la collection numérique

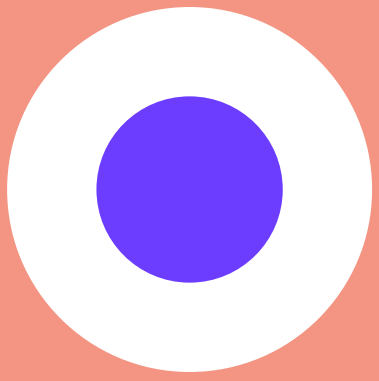
de l'Agence de mutualisation des universités et établissements d'enseignement supérieur ou de recherche et de support à l'enseignement supérieur ou à la recherche

février 2024

Sécurité des SI : saison 2
La cybersécurité au cœur de la stratégie de l'ESRI

amue
MUTUALISATION + SOLUTIONS

#31



Directeur général de la publication • Simon Larger

Rédacteurs en chef • Marion Lehmans – ANSSI - Bertrand Mocquet, David Rongeat – Amue

Secrétaire de rédaction • La com'

Graphisme & mise en page • @yay.graphisme

Photographie couverture • #31 février 2024.
Hacker éthique illustration issue de la campagne demainspecialistecyber.fr

ISSN 2650-8494 • La collection numérique est sous Licence Creative Commons CC BY-NC-SA 4.0

Ont collaboré comme auteur(e) à ce numéro • Vincent Strubel et les Sous-Directions Expertise, Opérations et Stratégie de l'ANSSI, Nicolas Eslous, Nicolas Babut, Jérôme Notin, Guy Duplaquet, Louis Di Benedetto, Florent Kirchner, Clara Bertolissi, la DGSI, Florent Della Valle, Philippe Bader, Bruno Chabal, Cédric Servaes, Simon Larger, Gilles Roussel, Pierre Boulet, Damien Berjoan, Brigitte Sor, Raymond Sclison, Guillaume Pourquié, Sarah Pauloin, Eric Fouré, Robert Malek, Julien Breyault, Philippe Werle, Olivier Perrot, Bruno Urbero, Frédéric Culie, Bastien Guerry, Cedric Foll, Mathieu Thuaire, Joffrey Célestin-Urbain, Véronique Gauthier, Aude Houdan-Fourmont, Jean Langlois-Berthelot, Marc-Olivier Boisset, Vincent Neuville, Sara Sellos, Nicolas Fouville, Florence Sèdes, Harry Claisse, Julien Valiente, Eric Berton, Dominique Launay, Guy Brand, Jacques Hertzberg, Michel Chabanne, Baptiste Robert, Viviane Delattre, Nicolas Schmitz, Claude-Isabelle Roux, Mejdi Bouchlaghem, Thierry Oger, Philippe Gaborit, Cristina Onete, Théophile Mandon, Delphine Chevallier, Alice Crelier, Bertrand Mocquet, David Rongeat

Remerciements et réseautage
Remerciements pour les Ministères et services de l'Etat, les associations et les établissements et l'ensemble des auteur.e.s, décideur.e.s et expert.e.s de la cyber qui se sont mobilisés pour ce numéro spécial. Pour gilles Missud pour la mise en relation.

Un remerciement particulier à Marion Lehmans coordinatrice sectorielle Enseignement Recherche de l'ANSSI pour son active disponibilité, son expertise dans la production de ce numéro.

Un remerciement chaleureux aux collègues de l'ANSSI qui ont permis la réalisation des articles ANSSI.

Un remerciement ému à Sylvie Barthel notre chère dir' com qui a soutenu dès le début la Collection Numérique. Bonne route Sylvie vers tes nouvelles aventures.

Editeur • Amue • 2 rue Albert Einstein • 75013 Paris

Fabriqué en France

tous les numéros de la collection sont en téléchargement Amue.
la collection numérique, ici →

à télécharger !

prochain numéro de la collection numérique (avril 2024) : Regards sur les stratégies numériques.

Vos propositions de témoignages et retours d'expériences dès maintenant à numerique@amue.fr

Édito

En cette année 2024, nous sommes plus que jamais convaincus que les établissements de l'enseignement supérieur, de la recherche et de l'innovation (ESRI) ont **un rôle majeur à jouer dans la lutte contre la menace cyber** : à la fois en tant que contributeurs à la connaissance et à la réponse aux enjeux de sécurisation des systèmes d'information (SI), et en tant que cibles potentielles de par les activités stratégiques qu'ils recoupent pour notre pays.

Lorsque le niveau de cybersécurité d'un ESRI est insuffisant, une attaque d'origine cyber peut atteindre durablement la continuité d'activité de l'établissement et la confiance de ses parties prenantes. Elle peut aussi se traduire par des situations encore plus graves, les plus extrêmes d'entre elles étant la propagation de l'attaque sur l'ensemble des établissements et entités partenaires, et l'utilisation des données de l'enseignement et de la recherche ou des équipements scientifiques à des fins militaires, de déstabilisation sociétale et politique ou d'atteinte aux droits fondamentaux. **Les attaques affectant les ESRI peuvent donc avoir des conséquences socio-économiques importantes et porter atteinte aux intérêts fondamentaux de la Nation. Ces risques, dans la conjoncture internationale actuelle, ne peuvent pas être ignorés.**

Dans ce contexte, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a voulu mettre en lumière les travaux engagés par les ESRI dans le domaine de la cybersécurité, afin de donner à voir les orientations poursuivies, illustrer ce qui a déjà été rendu possible et montrer que la cybersécurité est loin d'être antinomique avec les missions « cœur de métier » de ces établissements. **La cybersécurité constitue un levier essentiel** pour leur résilience et donc pour leur activité.

Ce numéro spécial est inspirant et chaque sujet développé gagne à être connu des gouvernances, des experts cyber, des enseignants, des enseignants-chercheurs et des étudiants. Tous construisent et participent à ce grand chantier d'intérêt général que nous menons ensemble, avec les ministères, les fédérations et associations sectorielles, les services de mutualisation du numérique, les éditeurs de logiciel et les autorités indépendantes. C'est ensemble que nous construisons un cadre de gouvernance de la cybersécurité plus fort et plus clair pour les établissements mais aussi un environnement numérique pour les populations académiques gagnant chaque jour un peu plus en sécurité et donc en confiance. L'ANSSI travaille au développement de son offre de services et de l'écosystème afin de répondre aux besoins des ESRI. Cela passe également par un soutien au développement du nombre d'experts et des compétences cyber disponibles sur le marché du travail.

A la veille de la transposition de la directive NIS 2 en droit français qui oblige les Etats membres à adopter une stratégie nationale concernant l'éducation et la formation, la recherche et le développement en matière de cybersécurité[1], nous encourageons les ESRI à se mobiliser afin qu'ils développent une plus grande **culture de la gestion du risque cyber et s'approprient les objectifs de cybersécurité** à atteindre. La France a besoin de s'appuyer sur des générations diplômées et acculturées au risque cyber.

La construction d'un modèle de gouvernance adapté, le renforcement des moyens alloués à la sécurité numérique, la formation régulière des experts cyber et la coordination de ces experts sont les clés de leur réussite. Il en va de même de la stratégie de mutualisation de leurs ressources qui pourrait faciliter la rénovation et la sécurisation de leurs environnements SI. L'intégration par défaut et dès la conception des SI des mesures de protection, est également un facteur de réduction des risques et est donc essentielle à leur stratégie. Tout comme l'implication des forces enseignantes et étudiantes et les exercices à la gestion de crise que nous espérons voir se multiplier afin que les ESRI soient mieux armés.

Le défi pour les ESRI est donc de **passer à un mode collectif de défense en profondeur de leurs SI** et de se saisir de cet enjeu sociétal crucial pour nos générations futures afin de construire un environnement numérique de confiance.

Sur tous ces enjeux, les ESRI ont définitivement un rôle à jouer et leur stratégie en matière de cybersécurité est et continuera d'être déterminante pour les secteurs d'activité les plus critiques autant que pour les missions d'intérêt public qu'ils servent avec passion.

Vincent Strubel, Directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

1 | Article 7.2.f et g de la directive NIS2 : *« la promotion et le développement de l'éducation et de la formation en matière de cybersécurité, des compétences en matière de cybersécurité, des initiatives de sensibilisation et de recherche et développement en matière de cybersécurité ».*

→ Photo © Patrick Gaillardin

enjeux et stratégie

auteur
ANSSI

Comprendre les menaces cyber d'aujourd'hui et de demain et s'armer pour y faire face

Une stratégie d'établissement solide s'appuie sur la connaissance des menaces cyber actuelles et futures

↘ DÉVELOPPER UNE STRATÉGIE DE CYBERSÉCURITÉ ADAPTÉE À LA CYBERMENACE

CERT-FR Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques

L'ANSSI publie chaque année un panorama de la cybermenace dans lequel il est fait état des grandes tendances de la menace cyber afin d'accompagner les entités. Des états de la menace sectoriels ou thématiques viennent compléter ce partage d'informations destiné à améliorer le niveau de connaissance des entités. Ces documents sont publiés sur le site du CERT-FR (https://www.cert.ssi.gouv.fr/cti/).

La prise en compte de la connaissance sur les menaces dans les stratégies de cybersécurité et dans les choix numériques et les pratiques du quotidien de chacun dans les établissements de l'enseignement supérieur, de la recherche et de l'innovation (ESRI), est un préalable à leur réussite. Il est aussi incontournable que les populations académiques spécialisées dans telle ou telle discipline liée aux thématiques ou secteurs particulièrement analysés, les consultent également.

↘ A PROPOS DE LA MENACE, AUJOURD'HUI

Parmi les menaces susceptibles de cibler les ESRI, **les menaces à but d'espionnage sont potentiellement les plus à même de porter atteinte au potentiel scientifique de la Nation**. Les attaquants liés à des États en compétition stratégique et industrielle avec la France ou l'Union européenne ciblent de façon répétée les institutions de recherche et certains chercheurs de façon individuelle. Ce ciblage peut avoir pour objectif de collecter des informations sur les recherches et positions stratégiques d'un État, mais également de dérober des données de

recherche scientifiques ou médicales utilisables dans le cadre de leur développement industriel. **Les établissements français de l'ESRI sont fréquemment ciblés par de tels attaquants.**

Outre l'espionnage, les établissements de l'ESRI sont également ciblés de façon plus opportuniste par des attaques à but de déstabilisation, souvent corrélées au contexte géopolitique. Ils sont aussi ciblés de façon récurrente par des acteurs cybercriminels qui cherchent à tirer profit des données personnelles massivement traitées par ces institutions, en pratiquant notamment de l'extorsion au moyen de rançongiciels.

↘ LES ÉVOLUTIONS TECHNOLOGIQUES : DES MENACES EN GESTATION ?

L'histoire du numérique a démontré une amélioration permanente des capacités des technologies numériques, en termes de changement d'échelle et de performance. Les stratégies des cyber attaquants utilisent toujours mieux ces nouvelles possibilités. Ainsi, la communauté académique s'interroge très régulièrement sur les enjeux générés par le potentiel des évolutions technologiques qui sont autant une menace qu'une opportunité. **Pour ne plus subir les évolutions technologiques utilisées au profit de la cybermenace, les stratégies de cybersécurité des ESRI doivent elles aussi évoluer symétriquement.**

analyste des cybermenaces illustration issue de la campagne https://demains-pecialistecyber.fr/

A suivre
Un état de la menace spécifique à la recherche sera prochainement publié par l'ANSSI

Ainsi, certaines évolutions technologiques de rupture en cours pourront constituer de nouvelles opportunités d'attaques. Parmi celles-ci, deux d'entre elles méritent d'être prises en compte dès aujourd'hui par les établissements.

→ Les risques cyber liés au potentiel de l'ordinateur quantique

Dans le cas où un ordinateur quantique suffisamment puissant pour mettre en œuvre les cryptanalyses quantiques serait construit, les mécanismes de cryptographie à clé publique tels que RSA, Diffie-Hellman ou ECDSA actuellement utilisés pour sécuriser notre vie numérique ne seraient plus sûrs. **Son avènement constituerait une innovation de rupture majeure pour la sécurité des données et communications.**

La menace pour les ESRI est sérieuse dès lors qu'ils utilisent les mécanismes de cryptographie à clé publique : la perte de confidentialité des données de recherche aboutirait en effet à la captation des résultats de la recherche au profit d'intérêts tiers et aurait des conséquences sur toutes les parties (chercheurs, ESRI, partenaires, industriels). Côté innovation, elle aboutirait à des pertes de chance et de marché (perte de brevets, droits de propriété, ressources rares). La conjoncture actuelle peut faire craindre de surcroît l'utilisation des données à des fins militaires et de déstabilisation.

La menace quantique devient de plus en plus une réalité. En témoigne les efforts de recherche et de développement sur la conception et l'analyse des algorithmes post-quantiques (sécurité théorique et implémentations sécurisées) et le nombre croissant de projets de collaboration et de publications scientifiques sur le sujet.

Au-delà de la sécurisation immédiate de ses SI et de sa résilience collective (cf. conseils de l'ANSSI ci-dessous), il convient pour l'ESRI de prendre en compte cet enjeu dans les cursus de formation et activités de recherche : le développement des compétences dans la conception, l'analyse et l'implémentation de la PQC nécessite d'être plus que jamais soutenu par les établissements.

Conseils de l'ANSSI

- → **1** Identifier ses SI et usages critiques
- → **2** Identifier pour chacun les mécanismes cryptographiques utilisés
- → **3** Evaluer son exposition au risque
- → **4** Définir son plan de transition au regard des risques : Prioriser les SI les plus critiques en implémentant une hybridation des mécanismes (combiner les calculs des algorithmes à clé publique pré-quantiques reconnus avec un algorithme PQC)
- → **5** Parallèlement, maintenir à l'état de l'art les compétences des personnels de recherche et experts cyber, et le niveau des enseignements délivrés sur la cryptographie et son usage dans les cursus de formation en cybersécurité.

Retrouvez l'avis de l'ANSSI et ses recommandations sur la page Avis de l'ANSSI sur la migration vers la cryptographie post-quantique | ANSSI (cyber.gouv.fr)

→ Les risques cyber liés au potentiel de l'IA

L'IA est entrée dans une nouvelle ère avec le développement de nouvelles méthodes statistiques et la mise en donnée du monde contemporain, qui permet un accès à un grand volume de données nécessaires pour l'entraînement de ces systèmes. Ces **nouvelles générations de systèmes d'IA soulèvent de nombreux enjeux en matière de cybersécurité.** En particulier, **les progrès de l'IA générative pourraient avoir un réel impact, par exemple en facilitant le développement de code malveillant.**

Face au déploiement massif de systèmes d'IA, leur cybersécurité constitue un enjeu prioritaire pour la communauté cyber aujourd'hui. L'ANSSI effectue des recherches sur l'utilisation de l'IA pour la détection d'intrusion. L'utilisation de méthodes d'apprentissage statistique est prometteuse pour étendre les capacités de détection, en complément de systèmes classiques mais de nombreux défis persistent.

« Retour sur.... »
N30 – « IA et Enseignement Supérieur : quels enjeux et impacts ? », décembre 2023
Pour aller plus loin avec la Collection numérique spécial IA → **ici**

enjeux et stratégie

auteur
ANSSI

Directive NIS 2 : ce qui va changer pour les entreprises et l'administration française

En France, de nombreuses entreprises et administrations seront soumises à cette nouvelle règlementation. Décryptage de l'ANSSI.

Le Parlement européen et le Conseil de l'Union européenne ont adopté, en juillet 2016, la directive « Network and Information Security » (NIS). Transposée au niveau national en 2018, cette directive avait pour objectif d'augmenter le niveau de cybersécurité des acteurs majeurs de dix secteurs d'activité stratégiques (ce qui représente quelques centaines d'entités en France) dans le contexte d'une augmentation de la menace cyber.

Face à des acteurs malveillants toujours plus performants et mieux outillés, touchant de plus en plus d'entités trop souvent mal protégées, la directive NIS 2, adoptée en 2022, élargit les objectifs et le périmètre d'application pour apporter davantage de protection.

Sa mise en application va permettre à des milliers d'entités de mieux se protéger. Elle va être l'occasion de mobiliser largement le tissu économique national et le secteur public. Elle amène aussi les Etats membres à renforcer leur coopération en matière de ges-

tion de crise cyber, en donnant notamment un cadre formel au réseau CyCLONe qui rassemble l'ANSSI et ses homologues européens, et à développer, au niveau de chaque Etat membre, une capacité de régulation pouvant amener à des injonctions en cas de non-conformité identifiée.

Selon le « Panorama de la cybermenace 2022 » de l'ANSSI, plus de 60 % des attaques qui sont remontées à l'ANSSI concernent des petites structures (PME/TPE/ETI et collectivités territoriales). L'agence observe également une évolution des attaques qui ciblent désormais les chaînes de sous-traitance pour se rapprocher de leurs clients finaux. Promouvoir la sécurité numérique auprès d'entités ne disposant pas d'expertise en la matière et leur permettre de mettre en place les mesures de protection de base face à la cybercriminalité sont donc des enjeux essentiels du dispositif NIS 2.

A ce jour, la directive NIS 2 comprend des annexes 1 et 2 dans lesquelles il est indiqué les secteurs, sous-secteurs et les types d'entité concernés. A l'échelle nationale, NIS 2 s'appliquera à des milliers d'entités appartenant à plus de dix-huit secteurs qui seront désormais régulés. Les acteurs de la chaîne d'approvisionnement, dont les acteurs du numérique, seront soumis au dispositif. Ces acteurs sont en effet de plus en plus ciblés par des cyberattaques qui visent à atteindre, à travers eux, des clients finaux d'importance plus critiques. Ils verront donc également leur niveau de sécurité numérique renforcé. Les administrations centrales des Etats membres ainsi que certaines collectivités territoriales intègreront également le périmètre de NIS 2.

La règle de base impliquera une inclusion par défaut des entités en tant qu'entité essentielle (EE) ou entité importante (EI) via des critères tels que le secteur d'activité, le nombre d'employés et le chiffre d'affaires (liste non exhaustive). Pour les entités ne répondant pas aux critères précédents et aux seuils associés, la directive NIS 2 offre la possibilité aux autorités de désigner unitairement des entités supplémentaires.

NIS 2 apporte donc une évolution majeure, l'inclusion d'un mécanisme de proportionnalité, qui distingue deux catégories d'entités régulées en fonction de leur niveau de criticité : les entités essentielles (EE) et les entités importantes (EI) permettant de ne pas les soumettre aux mêmes exigences.

Des consultations ont été effectuées avec les fédérations sectorielles afin de préciser certaines définitions de la directive. A cette occasion, l'ANSSI a partagé un premier projet de référentiel rapportant le détail des objectifs de sécurité assorties des mesures de sécurité que les entités régulées devront mettre en place. Le projet définitif sera bien sûr diffusé sur le site de l'agence.

Afin d'encourager la transformation des entités, l'ANSSI accompagne les entités privées et publiques dans leur réflexion et propose des outils facilitateurs (Mon aidecyber, MonServiceSécurisé, etc.) et des parcours de sécurité pour qu'elles puissent augmenter rapidement et de manière efficace leur niveau de maturité cyber. L'agence travaille également à faciliter ses interactions avec les entités régulées notamment au travers d'un portail numérique qui permettra de mettre à disposition des solutions de sécurisation. En parallèle, il est envisagé un potentiel mécanisme de présomption de conformité que pourrait offrir le recours à des prestations qualifiées par l'ANSSI (Prestataires d'Audit de la Sécurité des Systèmes d'Information (PASSI), Prestataires de Détection d'Incidents de Sécurité (PDIS), Prestataires de Réponse aux Incidents de Sécurité (PRIS), etc.).

L'ANSSI conseille donc à chaque entité de se préparer dès aujourd'hui. Les entités de l'ESRI peuvent s'appuyer sur les guides disponibles sur le site de l'agence, notamment le guide des TPE/PME et le guide d'hygiène informatique qui précisent les premières mesures de sécurité à adopter pour commencer et construire une base solide de mesures concrètes et pérennes.

En savoir plus

Vous avez des questions concernant cette directive NIS 2 ? Découvrez notre FAQ en ligne sur La directive NIS 2 | ANSSI (cyber.gouv.fr). Cette dernière est évolutive, elle est complétée au fil des questions transmises à l'agence.

→ **Calendrier**
NIS 2 rentrera en vigueur en France au plus tard en octobre 2024. La date d'entrée en vigueur ne correspond pas à la date d'application des exigences réglementaires applicables pour les entités : certaines exigences seront d'application directe et d'autres seront soumises à un délai de mise en conformité.

→ **Les services**
Retrouvez la liste des solutions certifiées, qualifiées ou en cours de qualification sur la page Trouver un produit/service de sécurité évalué | ANSSI (cyber.gouv.fr)

enjeux et stratégie

auteur
Nicolas Eslous, Fonctionnaire de Sécurité des Systèmes d'Information (FSSI) des ministères MESR-MENJ-MSJOP.

MINISTÈRES ÉDUCATION JEUNESSE SPORTS ENSEIGNEMENT SUPÉRIEUR RECHERCHE
Liberté Égalité Fraternité

Retour sur une crise d'origine cyber : la crise « TORTILLA »

De l'automne 2022 au début de l'année 2023, les secteurs de l'enseignement supérieur et de la recherche et, dans une moindre mesure, de l'éducation nationale et de la jeunesse, ont subi une vague massive de cyberattaques, qui a nécessité l'activation du dispositif ministériel de gestion de crise cyber, créé début 2022. Le déroulement de cette crise, baptisée « TORTILLA » sera restitué dans cet article.

1ère phase → des fuites massives « à bas bruit » de mots de passe d'étudiants

Début septembre 2022, *le responsable de la sécurité des systèmes d'information (RSSI) de RENATER et le responsable du CERT-RENATER font part aux FSSI d'une* ***menace d'un nouveau type****, difficilement détectable au niveau des établissements et dont la diffusion semble amorcer une croissance importante.*

Cette menace est constituée par des logiciels malveillants, appelés « information stealer » ou ***« stealer », dont la finalité a pour objet de dérober et exfiltrer les mots de passe et secrets stockés sur un ordinateur. Implantés dans des logiciels contrefaits*** *(par ex.* ***logiciels*** *habituellement payant «* ***crackés*** *»), ils sont* ***diffusés*** *via les* ***réseaux sociaux****, des* ***forums*** *et même parfois via des* ***liens publicitaires sur des moteurs recherche*** *grand public. Cette menace mondiale et non spécifique au secteur.*

L'éclairage de Cybermalveillance.gouv.fr

QU'EST-CE QU'UN *STEALER* ?

Les virus informatiques de type stealer sont spécialisés dans le vol d'identifiants (mots de passe…), de portefeuilles, de cryptomonnaies, de cookies de session et autres données stockées notamment dans les navigateurs Internet. Une fois exfiltrées, des données sont utilisées par les cybercriminels à des fins frauduleuses ou malveillantes.

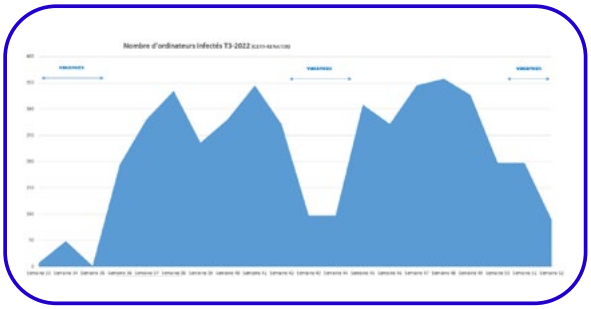
L'éclairage de Cybermalveillance.gouv.fr

De manière générale, les cybercriminels exploitent l'intérêt des internautes à obtenir des fichiers vidéo (films, séries), des logiciels piratés («crackés») ou encore des programmes permettant d'améliorer les performances dans les jeux vidéo, de l'ordinateur, etc.

1 | La Cellule Opérationnelle de Crise Cyber (COCC) est adossée au centre ministériel de veille et d'alerte (CMVA) et participe au centre ministériel de crise (CMC), pilotés par le Service de Défense et de Sécurité et communs aux trois ministères.

2 | CERT : Computer Emergency Response Team, qui peut se traduire en centre de détection et de réponse aux incidents de sécurité du numérique ou centre de cyberdéfense.

***Avec la rentrée universitaire 2022-2023**, le retour des **ordinateurs personnels des étudiants** sur les réseaux universitaires permet de détecter début septembre quelques dizaines d'ordinateurs infectés, évoluant rapidement ensuite à une moyenne de **300 ordinateurs infectés par semaine**, répartis dans l'ensemble des établissements. Le volume global sur le semestre s'établira à plus de **4200 signalisations**.*



***Chaque situation était signalée aux RSSI d'établissement, néanmoins la remédiation de ces incidents présentait plusieurs difficultés** :*

→ Les ordinateurs des étudiants ne relevant pas des parcs gérés par les établissements (informatique personnelle), les RSSI et correspondants SSI dans les composantes devaient réussir à convaincre l'usager de faire analyser son ordinateur.

→ Lorsqu'un étudiant acceptait de confier son ordinateur personnel, les anti-virus disponibles détectaient rarement ce nouveau type de menace. Il restait difficile d'apporter la preuve à l'étudiants que son ordinateur était compromis.

o Seuls de moyens avancés, disponibles uniquement sur certains équipements réseaux de nouvelle génération ou au niveau du CERT-RENATER, permettaient de détecter la compromission.

→ La volumétrie des signalisations dépassait souvent les capacités d'assistance informatique, en particulier dans les grands pôles universitaires.

2ème phase → l'exploitation par d'autres cybercriminels des mots de passe subtilisés

Ces dernières années, les groupes cybercriminels se sont organisés par spécialités. Certaines équipes sont dédiées au développement de logiciels malveillants (dont les « stealer »), puis s'appuient sur d'autres acteurs chargés de la diffusion en masse des logiciels corrompus. D'autres membres interviennent ensuite pour la revente des identifiants subtilisés.

Les groupes cybercriminels offensifs – ceux qui mènent les intrusions - disposent ainsi d'un véritable marché de comptes d'accès subtilisés prêts à l'emploi.

***Le 4 novembre 2022**, une première cyberattaque sur l'**université A**[3] est signalée par un partenaire du Centre Opérationnel de la Sécurité des SI Ministériels (DNE/COSSIM). L'information est immédiatement partagée avec les FSSI, le CERT-RENATER et les RSSI de l'université. L'ANSSI est avisée.*

→ L'attaque a pu être stoppée en début de phase de déploiement d'un rançongiciel, qui aurait pu détruire l'ensemble du SI de l'université.

→ Malgré tout, huit serveurs ont été chiffrés par le rançongiciel et l'annuaire électronique est compromis.

→ Face à l'importance de l'incident, l'université fait appel à un prestataire de réponse à incident de sécurité (PRIS)[4] afin de disposer d'expertises spécialisées pour l'analyse de la situation et la remédiation après incident.

***Le 14 novembre 2022**, une seconde cyberattaque en cours est signalée par le partenaire du COSSIM touchant une **université B**. Les intrusions sont identifiées sur des serveurs web d'accès distant (un socle technologique nommée « Guacamole ») utilisés par les étudiants pour leurs TP et accès pédagogiques.*

*→ Les analyses menées par les RSSI permettent d'identifier et de partager au CERT-Renater et au COSSIM des premiers marqueurs techniques d'identification des attaquants. **Ce partage sera très important dans la suite des évènements**.*

→ Ces marqueurs d'identification des attaquants sont placés en surveillance sur le réseau RENATER.

***Le 24 novembre 2022**, les marqueurs mis en surveillance par le CERT-RENATER permettent d'identifier une nouvelle intrusion en cours dans un autre serveur d'accès à distants d'une **école d'ingénieur C**.*

→ Le mode opératoire d'attaque est le même que celui de l'université B et s'appuie à nouveau sur le socle technologique « Guacamole », ce qui inspirera plus tard le nom de la crise ;

→ L'école d'ingénieur C déconnecte le campus concerné et réalise les analyses et la remédiation de son SI ;

3 | Les noms de établissements sont remplacés par un lettrage, sans lien avec le nom réel.

4 | Il s'agit de prestataires spécialisés disposant d'une certification attribuée par l'ANSSI. La liste des prestataires de réponse à incident de sécurité numérique est disponible sur le site de l'ANSSI : https://cyber.gouv.fr/prestataires-de-reponse-aux-incidents-de-securite-pris

Les 29 et 30 novembre 2022*, toujours grâce aux éléments issus de l'université B,* ***deux nouvelles intrusions*** *sont détectées dans* ***l'université D et une école d'ingénieur E*** *qui mettent immédiatement leurs SI en arrêt et initient les opérations de remédiation, avec appui d'un prestataire de réponse à incident pour l'école d'ingénieur E.*

Le lundi 5 décembre 2022*, alors que pendant le week-end la presse a fait état de cyberattaques importantes sur une collectivité territoriale et un hôpital (hors secteur ESR), nous apprenons que l'IUT E a subi massivement un rançongiciel, qui a détruit la totalité du SI, mais aussi les sauvegardes. L'activité est totalement arrêtée et la reconstruction va nécessairement repartir d'un système d'information vide.*

→ *Du fait de l'indisponibilité des journaux techniques, il ne sera pas possible de réaliser une analyse détaillée de l'attaque.*

→ *Seule certitude, les traces au niveau du réseau RENATER montrent qu'il s'agit d'une cyberattaque différente des situations surveillées via les marqueurs techniques connus.*

→ *Il semble s'agir d'un autre groupe d'attaquants s'appuyant sur des chemins d'attaques différents.*

Du fait du caractère systémique des cyberattaques et de l'impact majeur subi pour l'IUT F, le FSSI, en lien avec le Haut Fonctionnaire de Défense et de Sécurité, décide le 5 décembre 2022 de l'activation formelle de la Cellule Opérationnelle de Crise Cyber (COCC) *qui mobilise 12 agents :*

→ *L'ensemble des acteurs SSI du Service Défense et de Sécurité (FSSI et FSSI adj.)*

→ *L'ensemble des membres du COSSIM (4 membres en 2022)*

→ *L'ensemble des membres du CERT-RENATER (4 membres en 2022)*

→ *Les RSSI ministériels de la DNE (2 membres)*

*L'****objectif de la COCC*** *est de* ***coordonner*** *le dispositif d'urgence cyber,* ***d'analyser les situations et leurs évolutions possibles****, d'****élaborer des plans de réponse*** *cyber et de produire des* ***synthèses exécutives et opérationnelles*** *pour le centre de veille et d'alerte ministériel (CMVA), le HFDS et les cabinets ministériels.*


MINISTÈRES ÉDUCATION JEUNESSE SPORTS ENSEIGNEMENT SUPÉRIEUR RECHERCHE
DIFFUSION LIMITÉE
Cellule Opérationnelle de Crise Cyber (COCC)
FSSI, COSSIM, CERT-RENATER
Cellule Opérationnelle de Crise Cyber (COCC)
Incident « TORTILLA »
Fiche de situation #1 au 6 décembre 2022

Des situations d'urgences continuent à être détectées, puis signalées aux RSSI et à l'ANSSI :

→ ***Le 5 décembre*** *: intrusion détectée en phase initiale dans l'****université G***

→ ***Le 8 décembre*** *: intrusion détectée en phase initiale dans l'****IUT H***

Le ***plan de réponse global*** *est élaboré pendant la semaine et fait l'objet d'une communication urgente, avec mentions de limitation de rediffusion,* ***vers l'ensemble des 420 RSSI titulaires et suppléants désignés dans l'enseignement supérieur et la recherche****. Le plan de réponse comporte* ***16 mesures majeures*** *pour la détection d'évènements et la protection à prendre en compte dans chaque établissement.*


Objet: [rssi] [TLP AMBER] Message important : multiples incidents en cours et cellule de crise cyber ministérielle activée
TLP-AMBER - ne partager qu'au sein de votre établissement
Bonjour à toutes et à tous,
Nous souhaitons vous informer et attirer votre attention sur des incidents et menaces multiples portant sur le secteur.
La cellule opérationnelle de crise cyber (COCC) est en activée depuis ce lundi 5/12 et réunit plusieurs fois par jour les FSSI, le CERT-Renater et le COSSIM.
Contexte global

Le samedi 10 décembre *: une intrusion est détectée en phase initiale dans* ***une école privé d'ingénieur I****. Le déploiement du rançongiciel était imminent mais, avec le* ***week-end****, aucun contact n'était joignable. Le DSI pourra finalement être contacté juste à temps pour déconnecter l'ensemble du SI.*

Le 12 décembre *:* ***deux intrusions*** *en phase initiale sont détectées dans* ***l'université J et dans un rectorat d'académie K****.*

Les 13 et 14 décembre *:* ***deux intrusions*** *détectées dans une* ***école d'ingénieur L*** *et dans un* ***centre de recherche de l'EPST M.***

L'éclairage du FSSI

Les FSSI, COSSIM et CERT-RENATER ont désormais la certitude qu'un même groupe d'attaquants mène une campagne de diffusion de rançongiciel sur des établissements français d'enseignement supérieur et de recherche. L'ANSSI est informé de chaque situation.

Les connaissances acquises de leur mode opératoire permettent désormais de mener une « chasse » et de prévenir les établissements ciblés dès la phase initiale d'intrusion.

Ces marqueurs techniques doivent être maintenus sous embargo, sinon les attaquants pourraient se rendre compte qu'ils sont repérés et feraient évoluer leur mode opératoire d'attaque, ce qui ne permettrait plus de les détecter.

Ces « chasses » et la veille renforcée cyber sont désormais menés aussi en heures non ouvrables et week-end par les deux centres de cyberdéfense (CERT-RENATER et DNE/COSSIM) en coordination permanente avec les FSSI via un forum « Tchap » sécurisé, défini dans la procédure de gestion de crise d'origine cyber.

A l'approche des congés de noël, il est décidé en complément de mobiliser les gouvernances afin que les acteurs SI et SSI disposent de soutiens au plus haut niveau. Un message d'urgence SG/HFDS est transmis le 14 décembre à l'ensemble des dirigeants.


La Secrétaire générale du MENJ - MESR - MSJOP

Le 15 décembre : ***des demandes de levées de doutes pour de possibles intrusions sont transmises par le CERT-RENATER vers 128 établissements distincts. Les acteurs SI et SSI sont à pied d'œuvre pour mettre en œuvre les mesures de protection, avant les congés.***

Le 21 décembre : *trois intrusions sont détectées dans l'**école d'ingénieur N**, une **filiale privée d'un EPST O** et un **laboratoire mixte de recherche P**.*

Enfin, à partir du 22 décembre, des levées de doutes complémentaires seront réalisées mais plus aucune intrusion ne sera constatée.

Lors d'un point de coordination avec l'ANSSI début janvier 2023, il nous sera confirmé qu'au moins deux groupes distincts étaient en œuvre sur ces cyberattaques (et possiblement un troisième).

En l'absence de nouvelles situations au 13 janvier 2023, le FSSI établira la synthèse opérationnelle finale et proposera la clôture de la cellule de crise cyber « Tortilla », ce qui sera accepté par la Secrétaire Générale et HFDS des ministères.

L'éclairage conclusif du FSSI

Les mesures et le plan de réponse cyber ainsi que les communications vers les gouvernances et les acteurs de la sécurité des systèmes d'information ont permis une forte mobilisation de toute la communauté. Des impacts encore plus sévères et nombreux ont pu être évités.

Les partages des éléments techniques par les RSSI vers le CERT-RENATER et le COSSIM ont été très important pour être en mesure de détecter et anticiper les actions des cybercriminels.

Le déploiement des mesures de protection a rendu la progression des cyberattaquants de plus en plus difficile. **Cela a probablement provoqué l'usure des attaquants, qui ont ensuite changé de cibles**.

Cette hypothèse sera ensuite confirmée avec la survenance d'incidents similaires dans un autre pays européen en janvier 2023.

Recommandations principales en lien avec cette crise :

Pour les gouvernances :

→ S'assurer de la désignation effective d'au moins un Responsable de la Sécurité des Systèmes d'Information (RSSI), disposant des moyens nécessaires pour mener des actions sur l'ensemble du périmètre de l'établissement ;

→ Compléter autant que possible la désignation du RSSI titulaire par un à plusieurs RSSI suppléants, afin de contribuer à la continuité des missions de RSSI et d'être en mesure de suivre tous les périmètres et campus (dont les composantes et les laboratoires hébergés);

→ Élaborer une trajectoire de renforcement des moyens pour la sécurité du numérique en visant au moins un RSSI à temps plein et disposant d'un budget dédié aux projets de sécurité du numérique ;

→ Identifier les risques numériques principaux pour le périmètre et, en lien avec le RSSI et le DSI, lister les systèmes d'informations cruciaux à protéger et à garantir impérativement en cas d'incident cyber grave ;

→ Définir une organisation locale de crise cyber et s'entrainer par des exercices, en s'appuyant notamment sur les guides et kits de gestion de crise publiées par l'ANSSI.

Pour les acteurs techniques (DSI, RSSI et responsables d'infrastructures numériques) :

→ Renforcer les cloisonnements des réseaux afin de séparer les zones à faible maitrise (usagers avec ordinateurs personnels ou personnels externes) et celles à plus forte confiance ;

→ Vérifier et actualiser les politiques d'attribution de comptes et de gestion de mots de passe, en particulier pour les services exposés sur Internet (accès distant, vpn, applications web) ;

→ Mener des vérifications régulières des services numériques exposés sur Internet, en s'appuyant par exemple sur le service SILENE de l'ANSSI et le service « Scan'ER» de RENATER ;

→ Réaliser un plan de sécurisation des annuaires électroniques principaux en s'appuyant sur le service Oradad/ADS de l'ANSSI en obtenant le score d'au moins 3 ;

→ Vérifier les politiques de sauvegarde en s'appuyant par exemple sur le guide « Sauvegarde des systèmes d'informations » de l'ANSSI et tester régulièrement les capacités à restaurer.

enjeux et stratégie

auteur
Nicolas Babut,
conseiller stratégie numérique auprès du secrétaire général des ministères chargés de l'éducation nationale, de la jeunesse et des sports, et de l'enseignement supérieur et de la recherche

La mue du Responsable de la sécurité des systèmes d'information

C'est le nouvel enjeu de la gouvernance du numérique en établissement

La menace cyber continue à progresser de façon exponentielle et n'épargne pas les établissements d'enseignement supérieur et de recherche qui constituent désormais des cibles de choix. Les motivations des attaquants sont diverses : politiques, lucratives, économiques, ludiques. La surface d'attaque est particulièrement élevée du fait notamment de l'utilisation par les étudiants, enseignants et chercheurs de leurs ordinateurs ou équipements personnels. Les dérobeurs de mots de passe (*stealers*) et les rançongiciels (*ransomware*) constituent en effet l'essentiel des modalités d'attaque.

Face à cette menace, l'Etat fait évoluer sa gouvernance de la sécurité numérique et s'apprête à mettre en œuvre en octobre la directive européenne *Network and Information Security* (NIS 2). Pour les établissements d'enseignement supérieur et les organismes de recherche, l'application de la directive constitue l'opportunité de réévaluer leur gouvernance du numérique en y intégrant davantage la sécurité numérique, encore trop souvent sous-budgétée et considérée comme un domaine réservé aux spécialistes.

Si les schémas directeurs ou feuilles de route numériques se sont construits ces dernières années autour du développement des usages pour répondre aux nombreux besoins de dématérialisation et d'appui au métier, la sécurité numérique n'a parfois été traitée que sous l'angle des mesures techniques.

Au-delà de la mise en conformité avec les objectifs de la directive européenne, un rééquilibrage des questions de sécurité au niveau de la gouvernance du numérique de chaque établissement serait bénéfique, à l'heure où les risques, notamment sur la continuité d'activité mais aussi « réputationnels », sont avérés.

Le Responsable de la sécurité des systèmes d'information (RSSI) devrait se voir confier un mandat à plein temps et des moyens appropriés aux enjeux, sur la base d'une évaluation des risques portant sur les activités et les processus métiers les plus sensibles.

Compte tenu de la nature transversale de sa fonction, le RSSI gagnerait à être positionné auprès d'une direction générale des services, au même titre par exemple, que le Délégué à la protection des données (DPD) avec lequel il est amené à collaborer étroitement.

Il assurerait, en lien avec ses homologues des organismes de recherche et les correspondants SSI (notamment des unités mixtes), la bonne coordination de la mise en œuvre des politiques de sécurité numérique concourant à la protection du patrimoine scientifique et technique (PPST) dans une logique de site.

Il prendrait également l'animation d'une communauté d'ambassadeurs métier au sein de chaque direction ou entité, de sorte à intensifier les actions de sensibilisation et de formation permettant la diffusion large d'une culture de la sécurité numérique.

MINISTÈRES
ÉDUCATION
JEUNESSE
SPORTS
ENSEIGNEMENT
SUPÉRIEUR
RECHERCHE

Liberté
Égalité
Fraternité

Véritable pédagogue et bon communiquant, à l'aise avec les sujets techniques et focalisé en priorité sur l'activité métier, le RSSI est désormais amené à opérer sa mue stratégique comme ont eu à le faire les directeurs informatiques devenus directeurs du numérique ces dernières années. Les gouvernances des établissements sont appelées à porter et à soutenir cette transformation.

enjeux et stratégie

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

auteur
Jérôme Notin, directeur général du GIP ACYMA/ Cybermalveillance.gouv.fr

Cybermalveillance.gouv.fr : une coopération active avec le monde de l'éducation

Lancée en 2017, Cybermalveillance.gouv.fr est la plateforme du dispositif national de prévention et d'assistance aux victimes. Elle est opérée par le groupement d'intérêt public Action contre la cybermalveillance (GIP ACYMA) regroupant plus de 60 membres des secteurs public et privé qui contribuent à sa mission et son développement.

Les missions de ce dispositif qui sont principalement délivrées au travers de la plateforme couvrent trois domaines principaux :

→ la **prévention** avec la mise à disposition de plus de 500 contenus à vocation pédagogique (articles, vidéos, fiches, guides…), librement accessibles et diffusables, sur les cybermenaces et les bonnes pratiques de cybersécurité utiles pour y faire face ;

→ l'**assistance** aux victimes avec notamment un service en ligne qui permet aux victimes de diagnostiquer leur problème, d'obtenir les conseils et orientations nécessaires pour y remédier, et même de pouvoir être mises en relation si besoin avec un réseau de plus de 1200 prestataires référencés sur le territoire national en capacité de leur apporter une assistance technique de proximité ;

→ l'**observation** de la menace par ses différents capteurs qui lui permet de développer de manière opérationnelle ses missions de prévention et d'assistance et d'anticiper les risques.

Cybermalveillance.gouv.fr s'adresse à tous les publics qui ne sont pas couverts par d'autres dispositifs de l'État, et plus particulièrement à ceux qui ne disposent pas ou peu de compétences en informatique et en cybersécurité, qu'il s'agisse de particuliers, d'entreprises, d'associations ou de collectivités.

En 2023, la plateforme a accueilli plus de 3,7 millions de visiteurs et plus de 280 000 personnes sont venues y chercher une assistance spécialisée.

Les ressources mises à disposition par Cybermalveillance.gouv.fr sont déjà largement utilisées par les enseignants et servent même de références dans de nombreuses formations scolaires et universitaires.

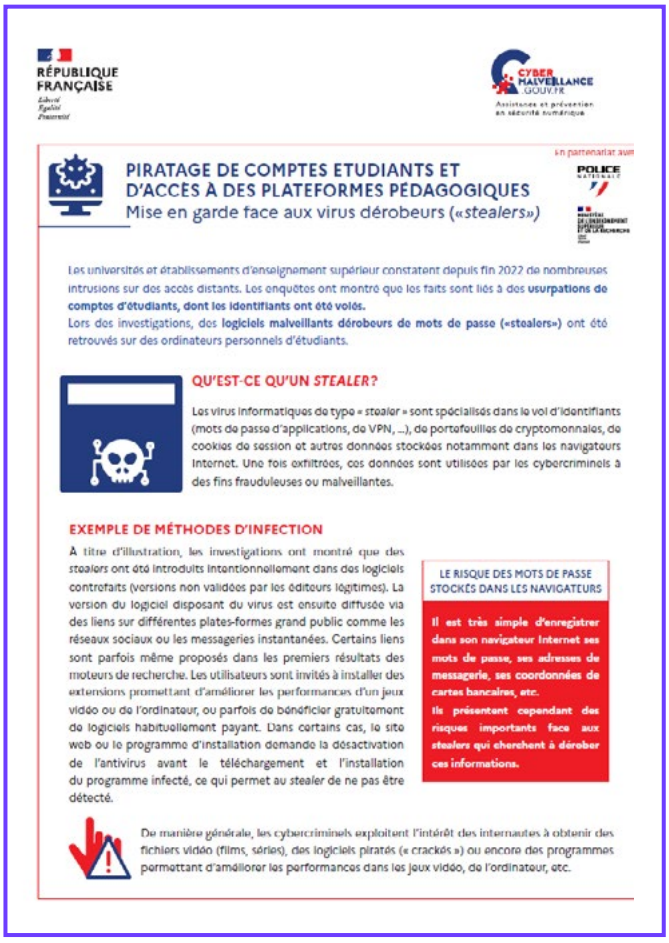
Le Ministère de l'Éducation nationale, de la Jeunesse et des Sports a rejoint le GIP Acyma en 2021. Depuis lors, plusieurs actions ont été réalisées en coopération parmi lesquelles on peut citer :

→ la contribution de Cybermalveillance.gouv.fr à l'élaboration des modules et contenus liés à la cybersécurité du programme Pix de développement et de certification des compétences numériques ;

→ la mise à disposition par Cybermalveillance.gouv.fr de son module de sensibilisation aux menaces et bonnes pratique de cybersécurité SensCyber pour l'ensemble du personnel du ministère sur sa plateforme de formation en ligne M@gistère.

Enfin, en 2023, la section spécialisée en cybercriminalité parquet de Paris (J3), la direction nationale de la police judiciaire et Cybermalveillance.gouv.fr ont proposé au MENJ et au MESR une action commune de prévention pour sensibiliser les personnels et usagers aux risques des virus voleurs de mots de passe (Infostealer).

Une fiche synthétique décrivant la menace, ses modes d'infection et bonnes pratiques à mettre en œuvre pour s'en prémunir a donc été réalisée conjointement avec le HFDS et la Direction du Numérique pour l'éducation du ministère, puis mise à disposition de l'ensemble des établissements d'enseignement supérieur et de la recherche via leurs responsables de la sécurité des systèmes d'information.


RÉPUBLIQUE FRANÇAISE

CYBER MALVEILLANCE .GOUV.FR

En partenariat avec POLICE NATIONALE

PIRATAGE DE COMPTES ETUDIANTS ET D'ACCÈS À DES PLATEFORMES PÉDAGOGIQUES

Mise en garde face aux virus dérobeurs («*stealers*»)

Les universités et établissements d'enseignement supérieur constatent depuis fin 2022 de nombreuses intrusions sur des accès distants. Les enquêtes ont montré que les faits sont liés à des **usurpations de comptes d'étudiants, dont les identifiants ont été volés.**
Lors des investigations, des **logiciels malveillants dérobeurs de mots de passe («stealers»)** ont été retrouvés sur des ordinateurs personnels d'étudiants.

QU'EST-CE QU'UN *STEALER* ?

Les virus informatiques de type « *stealer* » sont spécialisés dans le vol d'identifiants (mots de passe d'applications, de VPN, ...), de portefeuilles de cryptomonnaies, de cookies de session et autres données stockées notamment dans les navigateurs Internet. Une fois exfiltrées, ces données sont utilisées par les cybercriminels à des fins frauduleuses ou malveillantes.

EXEMPLE DE MÉTHODES D'INFECTION

A titre d'illustration, les investigations ont montré que des *stealers* ont été introduits intentionnellement dans des logiciels contrefaits (versions non validées par les éditeurs légitimes). La version du logiciel disposant du virus est ensuite diffusée via des liens sur différentes plates-formes grand public comme les réseaux sociaux ou les messageries instantanées. Certains liens sont parfois même proposés dans les premiers résultats des moteurs de recherche. Les utilisateurs sont invités à installer des extensions promettant d'améliorer les performances d'un jeux vidéo ou de l'ordinateur, ou parfois de bénéficier gratuitement de logiciels habituellement payant. Dans certains cas, le site web ou le programme d'installation demande la désactivation de l'antivirus avant le téléchargement et l'installation du programme infecté, ce qui permet au *stealer* de ne pas être détecté.

LE RISQUE DES MOTS DE PASSE STOCKÉS DANS LES NAVIGATEURS

Il est très simple d'enregistrer dans son navigateur Internet ses mots de passe, ses adresses de messagerie, ses coordonnées de cartes bancaires, etc.
Ils présentant cependant des risques importants face aux *stealers* qui cherchent à dérober ces informations.

De manière générale, les cybercriminels exploitent l'intérêt des internautes à obtenir des fichiers vidéo (films, séries), des logiciels piratés (« crackés ») ou encore des programmes permettant d'améliorer les performances dans les jeux vidéo, de l'ordinateur, etc.

***NDLR* : Sensibilisation partout pour toutes et tous :**
La sensibilisation des personnels aux risques cyber et aux bonnes pratiques est un élément clé de la sécurité numérique.
Cet exemple, une photo prise à la cafet' de l'Amue Montpellier, du bon sens pour toucher tous les agents, juste devant la machine à café, en est une illustration. La version numérique de cette affiche coproduite par cybermalveillance.gouv.fr et la CNIL peut être téléchargée → ici

enjeux et stratégie

Guy Duplaquet, chef du département Infrastructures et services opérés (ISO) de la direction interministérielle du numérique lors des 10 ans du Réseau interministériel de l'État le 07/12/23 à Paris. Crédit : A.PAPAÏS

auteurs
Guy Duplaquet, responsable du département Infrastructures et services opérés (ISO)
Louis Di Benedetto, adjoint au responsable du département des infrastructures et services opérés (ISO), Direction interministérielle du numérique (DINUM)

Cybersécurité et stratégie numérique de l'État

Le réseau interministériel de l'État (RIE) illustre parfaitement les défis à relever en matière de sécurisation des infrastructures numériques critiques. La DINUM les met en lumière.

La sécurité des infrastructures numériques critiques constitue une préoccupation essentielle pour le fonctionnement – évidemment souhaité efficace, résilient, sûr et économe en moyens – du système d'information et de communication de l'État. Au sein d'une organisation complexe, la définition et la mise en place d'une stratégie cohérente et partagée de cybersécurité s'avère un succès, peu connu mais très réel, pour l'État.

↘ LE RÉSEAU INTERMINISTÉRIEL DE L'ÉTAT (RIE)

Le système d'information et de communication de l'État est un ensemble complexe, constitué de plusieurs milliers d'applications et systèmes très variés, allant des services de base (messagerie électronique, annuaires techniques) aux systèmes les plus lourds (par exemple Chorus pour la gestion financière) en passant par des applications métier parfois très spécifiques, couvrant l'ensemble des missions de l'État. Applications et services peuvent être hébergés dans des centres de production infogérés (par exemple des services commerciaux en nuage, dans le cadre de la doctrine *Cloud au centre*[1]) ou au sein de centres de production informatiques (*DataCenters* ou DC) étatiques, sur des architectures techniques classiques ou, de plus en plus fréquemment, sur des services en nuage opérés en propre. L'État opère une dizaine de DC dis-

1 | Voir https://www.numerique.gouv.fr/services/cloud/doctrine/

2 | Hors du territoire national, c'est le ministère de l'Europe et des affaires étrangères qui assume la responsabilité des communications étatiques

posant d'une capacité interministérielle, répartis sur le territoire hexagonal. Pour les relier entre eux et mettre ces applications à disposition des agents de l'État sur l'ensemble du territoire national (outremer inclus)[2], le RIE aujourd'hui géré par la direction interministérielle du numérique (DINUM), depuis 2013, dessert environ 14 000 sites très variés – du phare de Port-Vendres à la place Beauvau en passant par la brigade territoriale de gendarmerie de Loures-Barousse, l'abattoir de Blancafort ou le centre de production informatique Justice de Nantes – pour environ un million d'utilisateurs internes.

↘ UNE APPROCHE INDUSTRIELLE DÉLIBÉRÉMENT SEGMENTÉE

Le RIE peut être vu comme décomposable en :

→ Un volet **Collecte**, le plus visible, construit sur la base des services professionnels de réseau privé offerts par les opérateurs commerciaux (Orange, SFR et Bouygues dans l'Hexagone, Orange en DROM, Can'L en Nouvelle-Calédonie, Onati en Polynésie Française), destiné à recueillir les flux issus des sites utilisateurs et à les déverser sur…

→ Une **épine dorsale** du réseau, se présentant sous la forme d'une double boucle optique très haut débit (100 Gbps) partiellement maillée, exposant un point de présence au sein de chaque grand DC interministériel sous la forme d'équipements actifs (routeurs) de classe opérateur, acquis par l'Etat et exploités sous sa responsabilité directe, reliés entre eux par des liens loués à deux opérateurs de confiance, **Renater** et **Terralpha**, et…

→ Une **plateforme d'accès à internet (PFAI)** sécurisée, se présentant sous la forme de 4 ensembles d'équipements de sécurité, acquis par l'Etat et exploités sous son contrôle direct, présents dans 4 des 10 points de présence de la dorsale RIE, et raccordés à internet par des liens de transit relevant de 2 opérateurs distincts (SFR et Free Pro) – une mutualisation partielle avec **Renater** étant, en complément, à l'étude.

Cette approche segmentée présente, certes, des risques en termes d'intégration, mais matérialise de manière très concrète l'idée que le RIE est construit avec les opérateurs. Depuis sa mise en service en 2013, le RIE a ainsi pu constituer une démonstration très visible d'interopérabilité et de coopération (parfois rude, il faut le dire) entre acteurs par ailleurs essentiellement concurrents.

↘ CYBERSÉCURITÉ : DÉFENSE EN PROFONDEUR

La pandémie COVID a mis en évidence le fait que les fonctions essentielles de l'État – et notamment l'accès à son système d'information – devait pouvoir être assurées en toutes circonstances et, en fin de compte, depuis tous lieux et en tout temps. En mobilité/télétravail, les agents s'appuient sur les services internet standards, en montant des tunnels sécurisés vers des points de terminaison opérés par leur ministère de rattachement, points se situant typiquement dans un DC étatique hébergeant un point de présence de la dorsale RIE. La chaîne de sécurité reliant un agent en mobilité (ou un internaute accédant à une application hébergée par un DC étatique) est longue :

→ En amont de l'entrée sur Internet, la DINUM mobilise les capacités de filtrage (lire : défense anti-DDoS) proposées par les **opérateurs de transit**

→ À l'entrée du RIE, sur la PFAI, la **DINUM** filtre les menaces sur la base des IOCs (indicateurs de compromission) communiqués par ses partenaires, en particulier l'**ANSSI**. En parallèle, cette dernière dispose de sondes permettant d'assurer une surveillance anti-menaces des flux circulant entre RIE et Internet.

→ À l'entrée des DC ministériels, c'est, cette fois, les **ministères** eux-mêmes qui assurent un contrôle de conformité des flux entrants.

Ce sont donc au total 4 acteurs qui, de manière autonome, chacun dans son domaine de responsabilité – domaines recouvrants, au moins partiellement – qui contribuent à la sécurité des flux. Cette profondeur, associée à la diversité des moyens mis en œuvre, complique de manière très importante les tentatives exogènes d'exfiltration ou de perturbation des services.

↘ L'HUMAIN RESTE INDISPENSABLE

Au-delà des moyens techniques, les **équipes opérationnelles** – SOC (Security Operation Center) – sont essentielles : les attaques, en nombre considérable, se diversifient et se sophistiquent avec le temps. Les contre-mesures mises en œuvre, sous forme de filtrages notamment, doivent en permanence être adaptées aux évolutions des attaques mais également des systèmes protégés. Deux points méritent d'être soulignés :

→ Les attaquants ne se limitent pas aux heures de bureau hexagonales : un SOC, pour être efficace, doit s'appuyer sur une **surveillance assurée en 24/7** (sur le RIE, c'est une brigade de 13 agents, à Rennes, qui assure cette fonction) et doit également fonctionner en astreinte 24/7 (pour la DINUM, ce sont donc 7 ingénieurs qui constituent l'équipe du SOC) ;

→ Les **échanges entre SOC sont fondamentaux**, tant en préparation (anticipation des contre-mesures, ce qui nécessite une compréhension des architectures techniques et métiers des systèmes protégés) qu'en opération (afin d'adapter en temps réel les contre-mesures et de s'assurer de leur efficacité, mais également, comme l'ont démontré des événements de sécurité, pour bien réagir en cas d'attaques simultanées sur plusieurs services).

La cybersécurité est l'affaire de tous, mais ce lieu commun ne signifie pas que les organisations soient dispensées de s'y intéresser, loin de là. Et pour être efficace, anticipation, profondeur et moyens doivent être harmonieusement conjugués par des équipes compétentes et motivées.

L'objet de cet article s'inscrit dans le cadre de nouvelle stratégie numérique de l'Etat produite par la DINUM intitulée « Une stratégie numérique au service de l'efficacité de l'action publique », en particulier la priorité relative à la préservation de la souveraineté numérique de l'État en investissant dans des outils numériques mutualisés. Pour consulter le document : https://www.numerique.gouv.fr/publications/feuille-de-route-dinum/

enjeux et stratégie

auteur
Florent Kirchner, Coordinateur de la stratégie nationale pour la cybersécurité- Secrétariat Général pour l'Investissement en charge de France 2030 , Service du Premier Ministre

PREMIER MINISTRE
Liberté
Égalité
Fraternité
Secrétariat général pour l'investissement en charge de France 2030

Innovation et passage à l'échelle

les deux mots clés de la stratégie nationale pour la cybersécurité

En exploitant le fort potentiel de recherche et de croissance de la filière française, la stratégie nationale pour la cybersécurité vise à accélérer l'innovation pour hisser l'offre française aux premiers rangs mondiaux, à maîtriser les technologies clés dans les applications critiques et à diffuser la cybersécurité au sein des entreprises et de la société. Pour cela, elle s'articule en 5 axes :

1. Développer des solutions souveraines et innovantes de cybersécurité ;

2. Renforcer les liens et synergies entre les acteurs de la filière ;

3. Soutenir la demande (individus, entreprises, collectivités et État), notamment en sensibilisant mieux tout en faisant la promotion des offres nationales ;

4. Former plus de jeunes et professionnels aux métiers de la cybersécurité, fortement en déséquilibre ;

5. Accélérer le développement des entreprises via des investissements en fonds propres.

Pour plus d'information :
https://www.gouvernement.fr/cybersecurite

FRANCE 2030

Les établissements d'enseignement supérieur et de recherche français (ESR) comptent parmi les meilleures équipes de la scène scientifique internationale. Des sciences sociales aux sciences de la nature, des sciences abstraites aux sciences de l'information, le niveau de leurs chercheurs doit – entre autres – à l'excellence des recrutements, à la qualité des environnements de travail et d'expérimentation, et à une culture reconnue de collaboration. Les laboratoires, comme lieux encourageant l'ouverture et le partage, contribuent ainsi à une recherche et un enseignement français de premier plan, au cœur d'une intense compétition mondiale.

Pourtant, ces établissements font depuis quelques années l'objet d'attaques informatiques fréquentes et soutenues. Entre 2019 et 2023, c'est plus de 250 attaques recensées publiquement sur les universités, soit une attaque tous les 6 jours, à travers le monde. Les enjeux sont, malheureusement, classiques dans le monde de la cybersécurité : blocage des systèmes informatiques contre paiement de rançon, vol de données et revente sur les marchés noirs, ou encore installation de logiciels espions, détournement de ressources de calcul… Dans un domaine dédié à la production de connaissance, et dans un monde où l'informatique est devenue, plus qu'un support, une clé indispensable de production de ces connaissances, ces cyberattaques ont des effets dévastateurs à court, moyen et long terme sur les équipes d'enseignants-chercheurs et de chercheurs.

La sécurité informatique se développe ainsi comme une mission « cœur » des établissements et organismes du monde de l'ESR. Dans la course internationale à la créativité et à l'inventivité, leurs capacités de cybersécurité constituent aujourd'hui un levier à part entière. L'enjeu est immense : pour maintenir, aujourd'hui, des capacités d'accueil des apprenants et des collaborateurs, et pour assurer la capitalisation des connaissances essentielle à une production de recherche au meilleur niveau mondial. Pour permettre, demain, d'accompagner par l'ingéniosité et le talent les mutations profondes de nos sociétés. De contribuer savoirs et apprentissages à l'accompagnement de nos concitoyens vers une vie meilleure.

La stratégie nationale cybersécurité, et le plan France 2030, sont pleinement en soutien à ces dynamiques de recherche et d'enseignement. Par l'intermédiaire de son Programme de Recherche et de son Programme de Transfert, c'est plusieurs centaines de chercheurs et d'enseignants-chercheurs qui se mobilisent sur quatorze projets clés. Et à travers les parcours de cybersécurité pilotés par l'ANSSI, près de 1000 entités, collectivités et établissements de santé, ont été accompagnées dans le renforcement de leurs systèmes informatiques, et la mise en œuvre de solutions de cyber-sécurisation. Dans la mise en œuvre de France 2030, l'Etat soutient les projets collaboratifs s'efforçant de respecter les meilleures pratiques et standards de cybersécurité, par exemple en matière des choix d'hébergement des données, d'architecture informatique ou de gestion des sous-traitances. Le soutien du Secrétariat général pour l'investissement en charge de France 2030 s'inscrit ainsi dans le développement des pratiques les plus vertueuses pour l'écosystème, à l'appui des travaux d'analyses de risque et d'homologation des systèmes informatiques réalisés par les entités.

L'enjeu pour l'ensemble de l'écosystème de l'enseignement supérieur et de la recherche est clairement d'échelle : celui d'assurer une confiance numérique indispensable au fonctionnement des établissements, des laboratoires, des projets, des échanges. Et de construire, en ouverture et en maîtrise, les acteurs de premier plan de demain.

enjeux et stratégie

© Adobe Stock

auteure
Clara Bertolissi,
Responsable d'action PEPR Cybersécurité, Direction des Grands Programmes d'Investissements de l'Etat, ANR

France 2030 et l'ANR

Un vaste programme de recherche rassemble les organismes de recherche, les universités et les opérateurs concernés pour accélérer la recherche sur la Cybersécurité

FRANCE 2030 — PROGRAMME DE RECHERCHE CYBERSÉCURITÉ

anr agence nationale de la recherche

Annoncé en 2021 par le Président de la République, le plan France 2030 poursuit les engagements des Programmes d'investissements d'avenirs créés en 2010 à travers le soutien à l'écosystème de la recherche et le financement dans la durée de projets structurants. France 2030 est doté d'un budget de 54 Mds€ dont 10 Mds€ sont gérés par l'ANR. L'agence est le principal opérateur du plan dans le champ de la recherche et de l'enseignement supérieur. A ce titre, elle est chargée d'organiser la gestion des programmes et équipements prioritaires de recherche (PEPR), de la contractualisation de leurs projets à leur évaluation in itinere et ex post.

Le programme de recherche (PEPR) Cybersécurité s'inscrit dans le cadre de la stratégie nationale pour la Cybersécurité (SNC) de France 2030, lancée en février 2021. Dotée de plus d'un milliard d'euros, cette stratégie a pour objectifs d'accompagner le développement d'une filière au potentiel économique important et de garantir in fine la maîtrise de technologies numériques souveraines et cyber-sûres.

La SNC aborde l'intégralité du cycle d'innovation, de l'idée à la mise en œuvre, de la recherche au marché, de la conception aux opérations. Le PEPR Cybersécurité en constitue le volet « recherche ». Lancé le 21 juin 2022, financé à hauteur de 65 M€ sur une durée de six ans, il a pour vocation de soutenir des activités de recherche au meilleur niveau mondial et ses résultats nourrissent les actions plus aval de la stratégie comme le Programme de Transfert au Campus Cyber, l'incubateur CyberBooster, le Grand Défi Automatisation de la Cybersécurité, les appels à projets Développement de Technologies Innovantes Critiques, entre autres. Le PEPR vise à obtenir des avancées scientifiques et faire émerger des technologies de ruptures bénéficiant à l'ensemble des acteurs français de la filière.

Le programme fait appel à plusieurs disciplines et implique 300 chercheurs et enseignants-chercheurs permanents issus du CEA, du CNRS, d'Inria, ainsi que de 23 universités et grandes écoles.

Sa direction scientifique est assurée par Bruno Charrat, Adjoint à la directrice de la recherche technologique du CEA, responsable de la coordination des actions cybersécurité ; Sonia Ben Mokhtar, directrice de recherche, CNRS et Hubert Duault, Responsable du Programme Cybersécurité, Inria. Les actions Cybersécurité sont coordonnées à l'ANR par Clara Bertolissi.

Sept premiers projets ont été lancés en 2022 pour un montant d'aide allouée compris entre 5,5 et 7,5M€ sur une durée de six ans. Ils portent sur :

→ La protection des données personnelles (IPOP – Inria) ;

→ La sécurité des protocoles et du vote électronique (SVP – CNRS) ;

→ La sécurité du traitement des données dans le cloud (Secure Compute - Université Paris Sciences et Lettres (PSL)) ;

→ La défense contre les programmes malveillants (Defmal - Université de Lorraine) ;

→ La Supervision et l'orchestration de la sécurité (Superviz - Inria et l'Institut Mines Telecom) ;

→ La sécurité matérielle et logicielle des systèmes embarqués (Arsene – CEA) ;

→ L'évaluation de la sécurité des logiciels (Secureval – CEA).

A la suite de l'appel à projets lancé en juin 2023 géré par l'ANR, trois nouveaux projets ont été sélectionnés pour cinq ans :

→ La résistance des systèmes cryptographiques (Cryptanalyse – INRIA) ;

→ L'exploitation de vulnérabilités en investigation numérique (REV – Eurecom) ;

→ La sécurité des données multimédia (COMPROMIS - CNRS).

Au-delà du programme de recherche (PEPR), l'ANR gère plusieurs autres actions clés de la stratégie Cybersécurité de France 2030, telles que l'Appel à Manifestations d'intérêt « Compétences et métiers d'avenir » ou encore le programme Transfert au Campus Cyber qui s'appuie sur la dynamique collective du Campus pour promouvoir des projets conjoints entre acteurs académiques, industriels, étatiques dans les domaines de la recherche, de l'innovation et de la formation.

En savoir plus :
→ Lien vers la stratégie nationale Cybersécurité : Cybersécurité | Gouvernement.fr
→ Lien vers le site du PEPR : Programme et équipements prioritaires de recherche pour la cybersécurité | PEPR - CyberSécurité (pepr-cybersecurite.fr)
→ Lien vers le site de l'ANR : Au service de la science | ANR
→ Page du PEPR sur le site de l'ANR : Cybersécurité | ANR

enjeux et stratégie

auteur
DGSI

La sécurité, c'est aussi acculturer

Le flash ingérence économique de la DGSI est un outil de sensibilisation des acteurs économiques et académiques aux ingérences étrangères

Depuis sa création en juillet 2012, le « flash ingérence économique » de la DGSI s'efforce d'acculturer les acteurs économiques et académiques publics et privés aux enjeux de sécurité et de les sensibiliser aux risques liés aux ingérences étrangères. Il s'est ainsi adapté aux mutations de l'économie afin d'alerter ses lecteurs quant aux nouveaux risques présentés par la dématérialisation accrue des échanges professionnels.

La DGSI publie dix « flash ingérence économique » par an, dont l'un est spécifiquement consacré aux enjeux propres au secteur de la recherche.

Les « flash ingérence économique » s'attachent, à travers la diversité des sujets traités, à illustrer la variété des modes opératoires qui ont été signalés au service et auxquels les acteurs étrangers offensifs ont recours afin de cibler les intérêts français et de tenter de déstabiliser des entreprises ou des structures de recherche françaises. Ils s'appuient ainsi sur des cas réels démarqués et veillent à formuler des préconisations accessibles au plus grand nombre et simples à mettre en œuvre visant à limiter les risques d'ingérence.

Depuis 2021, en association avec le ministère de l'Enseignement supérieur et de la Recherche, la DGSI a par ailleurs renforcé son suivi des structures de recherche. Cet effort vise à assurer une

meilleure sensibilisation de la communauté scientifique aux risques d'ingérence étrangère et à recueillir des informations plus précises, notamment en termes de projets de coopération scientifique internationale, de nature à favoriser les captations d'informations stratégiques. La mission de sécurité économique de la DGSI au profit de la recherche se décline en deux actions : des contacts auprès des acteurs de la recherche française pour détecter les tentatives d'ingérence et des prestations de conseil et de sensibilisation auprès de l'écosystème français de la recherche, auxquelles le « flash ingérence » économique contribue.

Le « flash ingérence économique » de la DGSI est disponible sur son site internet - www.dgsi.interieur.gouv.fr/la dgsi à vos côtés/contre-espionnage/conseils aux entreprises - où sont archivés les numéros des trois dernières années. Le flash peut également être consulté sur la page LinkedIn de la DGSI. Fin février 2024, la DGSI publiera le 100e numéro de son « flash ingérence économique ».

En 2023, ont ainsi été notamment traités les thématiques et risques suivants :

→ Comment se prémunir des risques associés aux captations de savoir-faire dans la recherche fondamentale ? ;

→ Risques d'accès aux appareils électroniques lors des contrôles aéroportuaires ;

→ Les risques liés aux visioconférences ;

→ Vol de données commis par des salariés en fin de contrat ;

→ Une société française innovante confrontée à des actions étrangères de captation technologique ;

→ Les salons professionnels, sources de vulnérabilités pour les entreprises.

enjeux et stratégie

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

auteur
Florent Della Valle, chef du service de l'expertise technologique au sein de la CNIL. Florent Della Valle a également occupé, entre 2019 et 2023, les fonctions de délégué régional à la recherche et à l'innovation (DRARI) en région Bretagne.

Mutualisation, la solution pour contrer les risques cyber ?

Enseignement supérieur et sécurité des données, les risques cyber sont réels mais ne sont pas une fatalité

Les établissements d'enseignement supérieur sont, comme tout organisme, exposés à une menace numérique omniprésente. L'été dernier, telle grande université du Sud de la France était touchée par un rançongiciel ; pendant la trêve des confiseurs, telle prestigieuse école proche de Paris était infiltrée via un hameçonnage. Ces incidents de sécurité frappent les établissements de tous types et de toutes tailles, universités, grandes écoles ou organismes de recherche. Sur les 17 500 violations de données notifiées à la CNIL depuis 2018, 380 (environ 2%) concernaient directement un établissement d'ESR. 40% de ces incidents avaient pour origine un piratage, 40% étaient dus à des accidents (erreur humaine ou dysfonctionnement) et 11% à des vols ou pertes d'équipements informatiques.

Cette réalité ne doit pas faire trembler les amphithéâtres, même connectés, mais il faut l'avoir à l'esprit. Les établissements d'enseignement supérieur sont singulièrement difficiles à prémunir contre la menace numérique. D'abord en raison du nombre et de la variété des éléments à protéger : inscriptions et scolarité, fonctionnement des cours et examens, accessibilité des ressources pédagogiques, laboratoires de recherche, données personnelles des élèves et des employés,

équipements informatiques (qui, pour partie, n'appartiennent pas à l'établissement), etc. Les risques sont à l'image de cette variété : de la simple attaque opportuniste avec demande de rançon au vol de résultats scientifiques, en passant par des perturbations motivées par des considérations militantes.

Un second défi est la diversité de la population qui fréquente les établissements : étudiants, enseignants, chercheurs, personnels administratifs et de soutien… Tous ne sont pas sensibilisés de la même manière à l'hygiène numérique, voire sont susceptibles de la négliger lorsque celle-ci apparaît comme une contrainte. Or c'est l'un des éléments sur lesquels la politique de l'établissement (ou du regroupement d'établissements) peut espérer agir efficacement. Vis-à-vis des étudiants et doctorants, en particulier, il est plus que souhaitable que la sensibilisation à la cybersécurité fasse partie de leur formation. S'agissant de la protection des données personnelles, le réseau dynamique SupDPO (*NDLR* : voir article du réseau SupDpo) peut également jouer un rôle moteur.

Il est évident que se pose une question de moyens et d'organisation. Certes, il faut que chaque établissement mette en œuvre des mesures minimales de sécurité, à l'image de ce que la CNIL préconise dans son guide sur la sécurité des données personnelles.[1] Mais cela entraîne, outre un problème de priorité et de budget, un besoin d'accès aux compétences en sécurité des systèmes d'information rares et onéreuses. Une plus grande mutualisation des compétences et des solutions entre établissements, voire au niveau national, peut-être une piste. Concernant l'organisation, la fragmentation en composantes et laboratoires, ainsi que, parfois, la multiplicité des tutelles, invitent à aborder explicitement la question du pilotage de la sécurité numérique dans les règlements intérieurs et conventions, comme c'est le cas pour la sécurité physique, avec la bonne dose de subsidiarité.

Enfin, c'est le propre des universités, écoles et organismes de recherche d'être les lieux d'usages numériques nouveaux. Ces usages, avec tout le bénéfice qu'ils apportent, peuvent ne pas être neutres en termes de sécurité ou de traitement de données personnelles : cours en ligne, examens télésurveillés, ces derniers ayant récemment fait l'objet d'une recommandation de la CNIL.[2] À ceux-ci s'ajoutent les traitements de grandes quantités de données par la recherche publique, en IA, en santé et ailleurs. Ici encore, les établissements n'ont pas nécessairement les moyens de tout contrôler. Il est donc important qu'ils puissent se reposer sur des infrastructures ou des solutions fiables, sécurisées et conformes à la règlementation, ainsi que sur des modalités de gouvernance adaptées aux enjeux. L'organisation autour de centres de données et de calcul régionaux pour la recherche offre, le cas échéant, l'occasion de mener une telle réflexion.

1 | https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles

2 | https://www.cnil.fr/fr/telesurveillance-des-examens-en-ligne-la-cnil-publie-une-recommandation

cryptologue, illustration issue de la campagne demainspecialistecyber.fr

auteur
Philippe Bader, RSSI, **Bruno Chabal**, responsable du pôle technique, **Cédric Servaes**, expert sécurité SI, **David Rongeat**, responsable numérique, **Simon Larger**, Directeur - Amue

Stratégie Cyber autour de l'offre Amue

Encore une fois la mutualisation fait son œuvre et prouve, par la diversité des partenaires, que l'Union fait la force.

↘ MUTUALITÉ, MUTUALISATION, SÉCURITÉS ET CONFIANCE

Commençons par l'histoire : depuis le XVII[ème] siècle, qui a vu l'émergence de la notion de « mutualité » en France , la mutualisation des risques visait à mettre en place et assurer la protection sociale. Concept ensuite remplacé par celui de sécurité sociale à compter de 1945, toujours, pour partager des risques et ainsi mieux y faire face. Retenons que la mutualisation est, par construction, un élément de sécurisation : sur les risques sociétaux au départ mais maintenant sur les risques cyber.

Par son rôle dans la co-construction (et plus encore avec l'exploitation en mode service) de solutions logicielles, l'Amue se doit d'offrir le meilleur niveau de sécurité pour ses adhérents, créer de fait une relation de confiance indispensable au partage et à des mises en commun.

L'activité de sécurisation de notre offre est historiquement assurée avec un haut niveau de professionnalisme et cela ne saurait changer, même si le niveau réglementaire est augmenté, notamment au vu du chantier de transposition de NIS2.

↘ SSI ET OFFRE AMUE

Pour son propre Système d'Information et pour les solutions qu'elle construit et déploie, l'Amue s'appuie sur le cadre de gouvernance de la sécurité numérique de l'État (PSSIE). Toutes les solutions logicielles Amue bénéficient d'une analyse de risques et d'un audit RGPD. Chaque solution est dotée de son dossier « sécurité » à destination des établissements qui les exploitent afin de parfaire la sécurisation du SI de nos adhérents.

Pour certaines solutions, des audits de code sont effectués : les améliorations recommandées par ces audits sont ensuite implémentées, progressivement, dans les solutions.

Plusieurs solutions exploitées sous forme de service (PMS, CAPLAB, SIFAC+) subissent des tests d'intrusion. Des homologations de sécurité de type RGS (voir le guide de l'ANSSI « L'homologation de sécurité en neuf étapes

simples ») sont ainsi obtenues par SIFAC+, SIFAC/ChaRM, SIHAM-PMS, Caplab, Pégase, le site web de l'Amue.

Un ensemble d'activité qui s'appuie sur une veille constante, la mutualisation et des échanges avec les RSSI des établissements, l'ANSSI et le partage autour des alertes CERT (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques).

L'Amue comme tous les établissements subit des attaques régulières, tentatives qui sont interceptées par nos équipements et procédures, puis analysées par les équipes dans une logique d'amélioration continue.

En établissement, ou dans les data-centres pour les exploitations mutualisées, les solutions Amue sont constamment attaquées. Sur toutes ces attaques via ces solutions logicielles, il n'y a pas eu de compromission de SI d'établissements, ni de compromission ou vol de données.

↘ LA CYBERSÉCURITÉ DANS LE FUTUR DE L'OFFRE AMUE

L'offre Amue vit une évolution importante puisqu'en plus de se charger de construire ou co-constuire les solutions logicielles, la partie co-exploitation va dorénavant devenir du ressort de l'Amue et de ses partenaires. Un changement majeur où les activités d'exploitation des solutions logicielles (et donc leur sécurisation) étaient menées par les établissements pour, à l'avenir, aller vers une exploitation commune sur des data-centres mutualisés de l'Enseignement Supérieur et Recherche.

Notre stratégie de développement d'une offre de service doit donc « muscler » sa sécurité par tous les moyens (mutualisation, meilleures pratiques de sécurité sur les data-centres, équipe plus forte et mutualisée, travail renforcé en lien avec l'expertise des RSSI, rapprochement fort de l'Agence, de Renater et de l'ANSSI, corrélations pour améliorer la prédiction d'attaques et s'en prémunir, mutualisation d'outils performants …).

L'appétit des malveillants sera aiguisé par cette exploitation centralisée, réunissant en quelques points un grand nombre d'instances des applications Amue pour beaucoup d'établissements.

Toutefois, ce regroupement d'exploitation bénéficiera de la force de frappe des équipes des data-centres, des équipes d'exploitation nouvellement créées, de la mutualisation d'outils de surveillance et de réponse à incidents performants, d'un travail conjoint avec des experts de la sécurité.

Donc en face, à nouveau, la mutualisation sera une force pour bénéficier d'un haut niveau de sécurité des data-centres et des équipes mutualisées.

↘ ANSSI ET AMUE, LE DÉBUT D'UNE HISTOIRE COMMUNE

L'ANSSI et l'Amue débutent une relation forte et structurée, dont le présent numéro n'est que la première pierre. Co-dirigé Amue-ANSSI, cet opus de la Collection Numérique préfigure d'autres articles de l'ANSSI dans les futurs numéros.

Une rencontre entre nos deux organisations s'est tenue fin janvier pour construire les contours d'un travail commun au bénéfice de nos adhérents et de la sécurisation des Systèmes d'Information. L'objectif est d'avancer sur des sujets comme par exemple la généralisation des formations, le partage d'expertises, la mise en place de solutions communes pour sécuriser les SI de l'ESR (accord cadre pour retenir des PRIS (Prestataires de Réponse aux Incidents de Sécurité), par ex), la mutualisation d'analyses de risques ou la recherche de simplification des homologations autour de l'offre Amue.

La sécurité des solutions de l'Amue, qui a toujours été au rendez-vous et constitue sans aucun doute un facteur de confiance de ses adhérents, doit être renforcée pour rester aux meilleurs niveaux d'exigence, à mesure que ces derniers sont réhaussés réglementairement. Il en va du maintien de cette confiance mutuelle au sein de la communauté et donc de son avenir dans son entier.

« Retour sur…. »
Un premier opus de la Collection Numérique sur la sécurité à lire ou relire N°17 Sécurité des systèmes d'information - Octobre 2021

Offre de service et plateforme mutualisée….

Dans le cadre du passage en mode service de son offre, l'Amue envisage la co-construction d'une plateforme et d'un centre de services mutualisés. Cet ensemble de ressources humaines et logicielles apporterait aux DSI concernées des facilités d'intégration de leur écosystème aux solutions de l'Amue. Pour l'Amue, c'est un levier incontournable pour relever le défi du mode service pour l'ensemble de son offre sans induire de discrimination vis-à-vis de la capacité technique de certains établissements. Pour tout le monde, les services proposés de contrôle d'accès, de médiation et de supervision participeront à renforcer le niveau de sécurité dans ce contexte plus exposé d'une offre en mode service.

enjeux et stratégie

France Universités

auteur
Gilles Roussel, référent Numérique de France Universités et président de l'Université Gustave Eiffel

La cybersécurité vue de l'Université

Formations des étudiants, sécurisation des SI, sensibilisation de la gouvernance, soutien de l'ANSSI. L'université se donne les moyens de sa sécurité.

Dans un monde toujours plus numérique, si les universités forment les experts de demain et explorent le sujet sous tous ses aspects, elles sont aussi confrontées à une recrudescence d'attaques cyber. Les attaquants se professionnalisant, il est crucial de renforcer les compétences de nos établissements en proposant davantage de formations en cybersécurité, et cela dans un délai contraint. Pour l'État, il s'agit également d'un enjeu pour l'ensemble de la population et les universités doivent s'adapter rapidement pour y répondre.

↘ L'IMPORTANCE DE FORMER ET D'INCLURE DAVANTAGE LES FEMMES

La filière cyber fait déjà face à un déficit de main d'œuvre alors que la stratégie nationale de l'État est de créer 37 000 emplois supplémentaires d'ici 2025[1]. L'adossement des formations à la recherche a permis aux universités d'identifier, en amont, la cybersécurité comme un enjeu essentiel, et des formations existent déjà dans de nombreux établissements. Comme à l'Université Bretagne Sud qui a fait de la cybersécurité une de ses spécialités et qui *« est fière de contribuer à la formation de jeunes diplômés en cyber du Bac+3 au doctorat. L'université se met en ordre de marche pour former encore plus de compétences en formation initiale ou continue »*, assure Virginie Dupont, vice-présidente de France Universités et présidente de l'Université Bretagne Sud.

Autre exemple du côté de l'Université de Poitiers, où a été mis en place une formation d'ingénieur visant à former des spécialistes. *« Elle est basée sur une longue expérience en termes de gestion des risques »*, souligne Virginie Laval, présidente du Conseil de la formation, de la vie

1 | Source : Stratégie nationale d'accélération pour la cybersécurité https://www.economie.gouv.fr/strategie-nationale-acceleration-cybersecurite

étudiante et de l'insertion professionnelle de France Universités et présidente de l'Université de Poitiers.

Afin d'identifier les formations de qualité, le label SecNumEdu de l'ANSSI a été lancé en 2017. Il regroupe une grande partie d'entre elles (dont celles présentes à l'Université Bretagne Sud et à l'Université de Poitiers) avec 47 formations initiales et 30 formations continues.

Mais une ombre au tableau persiste, dans l'ensemble des formations du territoire, les femmes représentent seulement 14 % des effectifs selon l'ANSSI, leur recrutement est donc une priorité pour les établissements qui adaptent leurs formations avec de nouvelles disciplines et compétences à acquérir par les étudiants.

↘ LES UNIVERSITÉS ET LES ÉCOLES VISÉES PAR LES CYBERATTAQUANTS

Le nombre d'attaques cyber est en augmentation notable ces dernières années (+37 % entre 2020 et 2021) et l'ANSSI considère que 15 % d'entre elles ciblent le milieu éducatif, dont les établissements d'enseignement supérieur et de recherche. Pour Gilles Roussel, référent numérique à France Universités et président de l'Université Gustave Eiffel, *« la menace principale identifiée est l'attaque par rançongiciel, mais nous pouvons aussi être victimes de vol de données (de recherche, mais aussi de sujets d'examens) ou de tentative de modification des données de scolarité. La compromission initiale peut cibler n'importe quel compte des usagers de nos systèmes d'information, la plupart du temps par un simple mail d'hameçonnage. »*

↘ FRANCE UNIVERSITÉS SE MOBILISE

France Universités s'est saisie de la question de la cybersécurité et en a fait une de ses priorités en 2023-2024, notamment avec de multiples actions de sensibilisation auprès de ses établissements membres, avec l'appui de l'ANSSI. Dans le cadre de son comité numérique, France Universités avait déjà formulé, en 2022, des recommandations pour sécuriser le système informatique des universités. *« L'une d'entre elle était de mobiliser les moyens nécessaires aux services de sécurité des systèmes d'informations des établissements. En d'autres termes, et selon les recommandations de l'ANSSI, il faudrait prévoir 10 % des budgets informatiques dans les outillages, mesures et personnels dédiés à la sécurité »*, précise Gilles Roussel. Aujourd'hui, France Universités poursuit ces travaux avec l'ANSSI. Elle a également dispensé (récemment) à ses membres une formation *« Enjeux de Cybersécurité pour nos établissements »*, dans le cadre de l'offre de formations proposée aux présidentes et présidents membres. L'objectif était *« de sensibiliser nos membres aux enjeux de la cybersécurité et aux lourdes conséquences en cas d'attaque, explique Johanne Ferry-Dély, directrice du développement de France Universités. Mais aussi de partager les expériences et bonnes pratiques à mettre en place, afin de penser ensemble l'accompagnement des établissements. »*

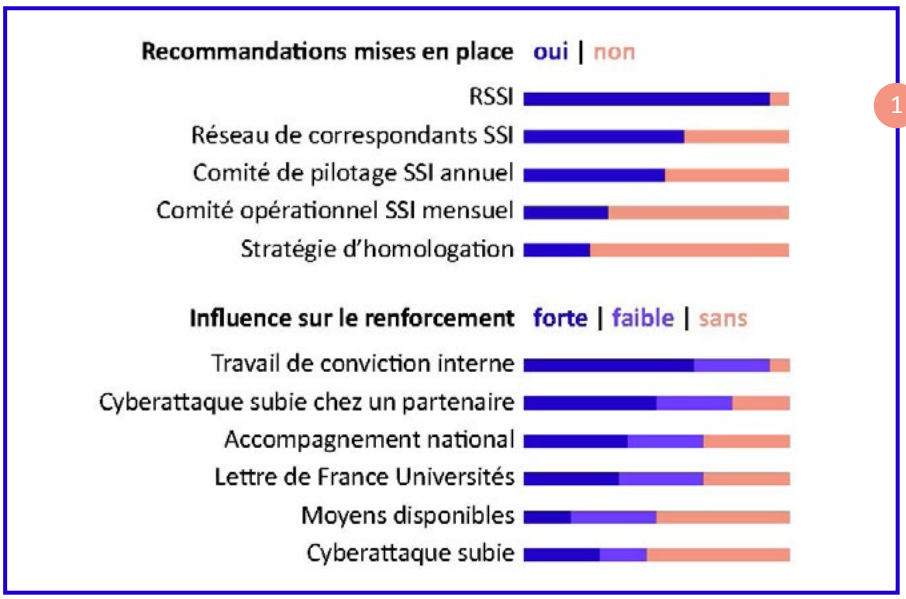
enjeux et stratégie

auteur
Pierre Boulet,
Président de l'Association VP-Num, pour le bureau de VP-Num

La sécurité des systèmes d'information se renforce dans les universités

L'an dernier, Vp-Num a coordonné l'écriture d'une lettre envoyée par France Universités aux gouvernances de ses établissements adhérents. Cette lettre insistait particulièrement sur l'augmentation des risques de cyberattaque et sur les bonnes pratiques à mettre en œuvre au niveau de la gouvernance de la sécurité des systèmes d'information (SSI). Un an après, nous avons interrogé nos adhérents pour essayer de mesurer la prise en compte de ces recommandations dans les universités françaises. Nous présentons ici les résultats de cette enquête qui a reçu 28 réponses, soit plus du tiers des universités françaises.

À la question sur la mise en place des recommandations émises par la lettre, celle qui est le plus suivie est la nomination d'un ou plusieurs responsables de la SSI pour la quasi-totalité (93 %) des établissements répondants. Plus de la moitié ont mis en place un réseau de correspondants SSI (61 %) et un comité de pilotage SSI annuel (54 %), mais moins d'un tiers ont un suivi opérationnel institutionnalisé par un comité opérationnel SSI mensuel (32 %) et une stratégie d'homologation, qui est une obligation récente (25 %). Il reste donc du chemin à parcourir puisque seules 2 universités ont déployé les 5 recommandations.



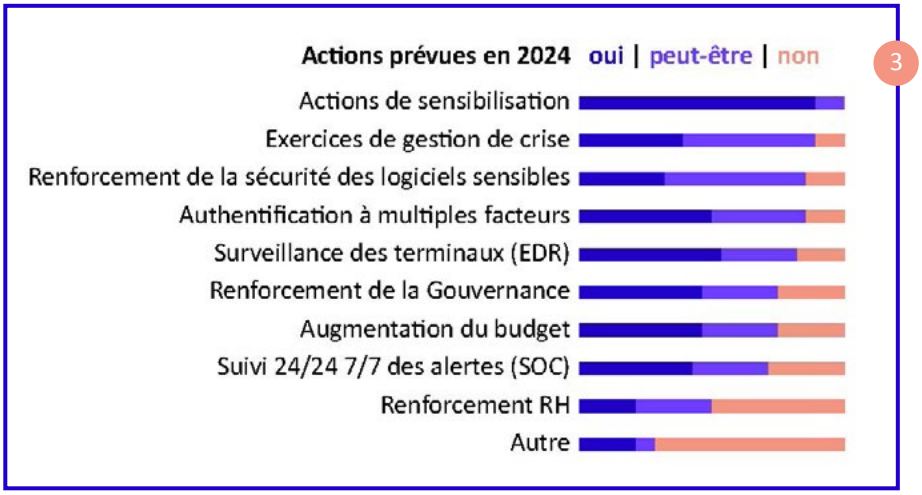
1

1 Nous notons cependant que tous les établissements ont maintenu ou renforcé la gouvernance et les moyens dédiés à la SSI. En effet, pour les années 2022 et 2023, 54 % des répondants ont déclaré un fort renforcement de la gouvernance de la SSI et 29 % son renforcement faible ; 29 % ont déclaré une augmentation forte des moyens humains et financiers dédiés à la SSI, et 29 % une augmentation faible de ces moyens. Aucun établissement répondant n'a déclaré d'affaiblissement de la gouvernance ou de diminution des moyens humains et financiers.

2

2 Nous avons ensuite interrogé les établissements sur les raisons de ce renforcement de la gouvernance et des moyens. Ces raisons sont multiples, la plus souvent citée est le travail de conviction interne (93 %), suivie par une cyberattaque subie chez un partenaire proche (79 %). L'accompagnement par les structures nationales (MESR, CERT-RENATER, ANSSI...) et la lettre de France Universités ont influencé chacun 68 % des établissements répondants. Viennent ensuite les moyens disponibles (50 %) et une cyberattaque subie (dans 46 % des établissements tout de même !).

3



3 Enfin, nous avons interrogé nos adhérents sur les actions qu'ils prévoient en 2024. Reconnaissant que chacun doit être acteur de la cybersécurité, 100 % des répondants ont déclaré vouloir travailler à des actions de sensibilisation. De nombreux autres sujets sont très présents : les exercices de gestion de crise (à ce propos, nous apprécions grandement les kits « clés en main » mis à disposition par l'ANSSI fin 2023), le renforcement de la sécurité des logiciels sensibles, le déploiement de l'authentification à multiples facteurs, la surveillance des terminaux (EDR), le renforcement de la gouvernance et le suivi 24 heures sur 24 et 7 jours sur 7 des alertes de sécurité informatique (SOC). Ces mesures sont supportées par des augmentations de budget chez 75 % des répondants et dans une moindre mesure (50 %) des renforts humains. Cette liste d'actions n'est bien sûr pas exhaustive et la mise en place de procédures d'homologation se poursuit chez ceux qui n'en ont pas déjà déployées.

En conclusion, nous pouvons affirmer que le travail de sécurisation est bien engagé dans les universités et va encore se renforcer dans les années qui viennent, mais que la situation est contrastée avec des établissements très engagés et d'autres chez qui le sujet n'est pas encore complètement d'actualité. Nous souhaitons souligner que toutes les mesures de sécurité nécessitent du personnel compétent mais que le renforcement des ressources humaines dédiées à la SSI est difficile dans le contexte actuel alors qu'il y a urgence. En effet, les jeux olympiques en France cet été vont attirer les cybercriminels. Il est donc particulièrement important de renforcer rapidement la sécurité de nos établissements. Le travail de conviction doit donc continuer pour mobiliser des moyens supplémentaires !

enjeux et stratégie

auteur·e·s
Damien Berjoan, DPD,
Brigitte Sor, Présidente,
Consortium Esup

ESUP & la sécurité

Comment est-t-elle traitée dans les services de ESUP ou ses incubations : applications à installer ou mis à disposition en tant que service ?

La gestion de la sécurité au sein des services de ESUP (en production ou en phase d'incubation), en mode installé sur les infrastructures des établissements « on premise » ou en mode hébergé (SaaS), se déploie à plusieurs niveaux via diverses actions menées par plusieurs structures transversales d'ESUP-Portail. Ce catalogue de services composé de ressources provenant d'établissements divers, intègre naturellement les principes fondamentaux de la sécurisation organisationnelle et des bonnes pratiques de l'ANSSI, diffusées entre autres par les RSSI des établissements affiliés.

↘ CELA PERMET DE CONSOLIDER LA SÉCURITÉ NUMÉRIQUE À TRAVERS :

• La coordination technique d'ESUP-Portail et les ateliers thématiques, en charge de formuler des recommandations techniques basées sur les retours d'expérience des établissements membres. Ces instances assurent une veille constante sur les technologies et services émergents, les travaux sont présentés lors des journées biannuelles ESUP-Days dont les enregistrements sont disponibles sur le portail ESUP[1] (prochaine édition en Avril 2024).

L'expertise de la coordination technique a permis d'émettre des avis de sécurité spécifiques pour la communauté, notamment sur des sujets tels que Log4J et Spring.

1 | https://www.esup-portail.org/wiki/display/COMM/Les+ESUP-Days

Dans le cadre des offres hébergées, ESUP-Portail a constitué un groupe de travail composé de membres de la coordination technique, du comité de direction et du Délégué à la Protection des Données (DPD). Ce groupe a défini l'organisation pour le cadrage, la définition du modèle économique et l'accompagnement à la formalisation des conventions avec les établissements proposant des services en mode hébergé.

Cette collaboration a permis de formuler des recommandations en matière de sécurité, issues des expériences des établissements, afin d'établir un cadre commun pour assurer la conformité en termes de protection des données personnelles et l'homologation de sécurité des services numériques par les établissements adhérents utilisateurs. Cette démarche s'accompagne de l'intervention du DPD d'ESUP-Portail auprès des établissements, sans se substituer à leurs propres procédures et structures de sécurité, notamment par la mise en place de conventions spécifiques formalisant les clauses de sous-traitance RGPD de l'offre de service numérique en mode hébergé.

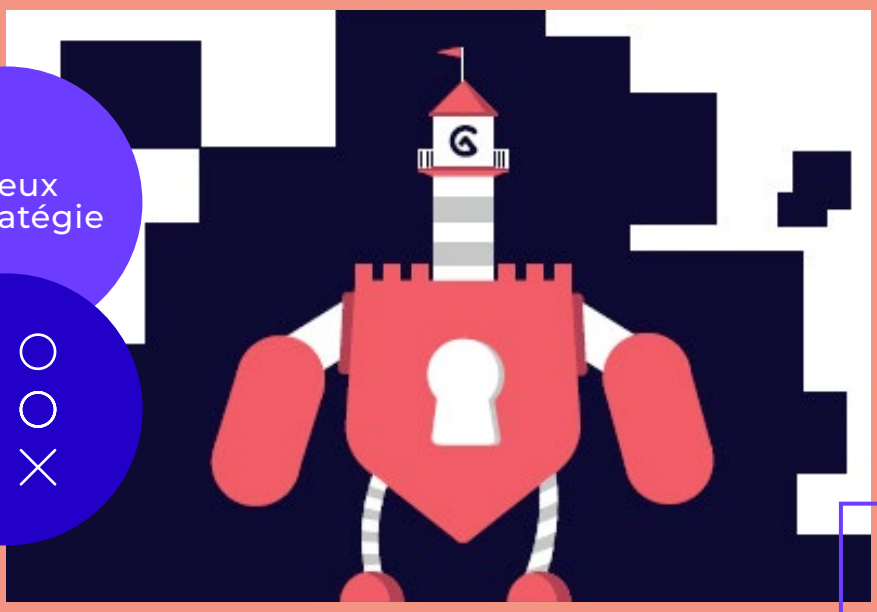
Les référentiels de cybersécurité utilisés pour formaliser ces éléments s'appuient sur la solution de cybersécurité "MonServiceSécurisé" proposée par l'ANSSI (*NDLR* : voir l'encart de l'article « L'homologation de sécurité RGS comme stratégie SécNum pour développer une culture de l'évaluation du risque à tous les niveaux de l'établissement »), destinée à aider les entités publiques à sécuriser et à homologuer leurs services numériques. Cela facilite le processus d'homologation des établissements fournisseurs ou utilisateurs de services en mode hébergé, assurant une vue homogène du niveau de sécurité des services numériques souverains fournis et utilisés par la communauté ESUP-Portail.

ESUP-Portail adapte ses services aux prérequis en matière de cybersécurité en fonction de la criticité de l'application et des priorités remontées par chaque comité de pilotage du service numérique concerné.

Pour toute information complémentaire ou pour échanger sur ces sujets de cybersécurité, protection des données, n'hésitez pas à revenir vers nous via nos différents canaux de d'échanges habituels[2].

2 | esup-utilisateurs@esup-portail.org – https://rocket.esup-portail.org – dpo@esup-portail.org

enjeux et stratégie



auteur
Raymond Sclison,
Directeur Technique, Association COCKTAIL

Et la sécurité dans l'offre Cocktail ?

Panorama des moyens mis en œuvre pour sécuriser l'offre.

Les applications COCKTAIL sont disponibles selon deux modes de déploiement, on-premise et cloud privé, qui est l'offre PHARE.

Pour le premier cas de déploiement COCKTAIL travaille avec les établissements pour prendre en compte les problématiques de sécurité dans la mesure du possible puisque la stratégie de sécurité est évidemment différente pour chaque établissement.

La plateforme PHARE est une plateforme SaaS multi-tenant qui héberge les applications COCKTAIL pour le compte d'établissements. Les applications manipulant aussi bien des données financières que personnelles.

Le projet a fait l'objet d'un financement France-Relance en accord avec la DINUM avec laquelle nous avons décidé de cibler un hébergement labellisé SecNumCloud. Le label SecNumCloud garantit un très haut niveau de sécurité de la plateforme. Il adresse aussi bien des critères liés au réseau, à l'organisation, à l'environnement. Très peu d'opérateurs dispose de la certification nécessaire au vu de ces exigences qui doivent être respectées.

Pour répondre aux défis soulevés par le niveau de risque croissant concernant la sécurité des données nous avons dû mettre en place des mesures complémentaires.

En premier lieu nous avons fait réaliser un audit par un cabinet spécialisé avant la mise en production officielle de la plateforme. Cet audit a consisté en une analyse avec la méthode EBIOS suivie de pen-tests pour identifier les risques d'intrusion ou de perte de données. Le niveau de sécurité a été jugé satisfaisant mais évidemment le travail de sécurisation est un travail permanent et des suites seront donc données pour ajuster en permanence les mesures et s'adapter à l'évolution des risques.

En second lieu, la plateforme étant multi-tenant c'est à dire qu'elle accueille de multiples adhérents, nous devons assurer une étanchéité totale entre les applications et les données des adhérents respectifs. C'est évidemment une condition essentielle pour la sécurité et également pour rassurer un adhérent qui passe d'une opération on-premise à un hébergement cloud. Cette étanchéité est assurée par construction de la plateforme en utilisant des techniques réseaux et les fonctionnalités du serveur de données Oracle.

Enfin nous avons dû adresser la problématique de la sécurisation des données. La plateforme met en place des stratégies de backup "classiques" basées sur la redondance (2 datacenters sont utilisés) et des backups à niveaux de fréquence et rétention multiples (quotidien, hebdomadaire, mensuel).

Il nous est apparu toutefois que le risque de ransomware, voire de malveillance d'une personne disposant d'accès suffisants n'était pas nécessairement couvert par ces différentes mesures et nous avons donc conçu un dispositif adressant spécifiquement ce risque. Les données de chaque adhérent sont extraites quotidiennement, elles sont ensuite cryptées avec un cryptage asymétrique fort puis la sauvegarde est envoyé chez un autre opérateur dans un stockage S3 immuable. Seul l'établissement adhérent possède la clé privée capable de décrypter les données. En cas d'attaque de la plateforme par un ransomware il nous est ainsi possible de reprendre cette sauvegarde et de reconstruire un environnement. Ceci est complété par le fait que la plateforme est construite "as-code" et qu'il est donc possible d'effacer entièrement les serveurs et de reconstruire automatiquement la plateforme.

COCKTAIL travaille en continu avec les établissements hébergés pour renforcer la sécurité.

enjeux et stratégie

auteur·e·s
Guillaume Pourquié, DPO de Grenoble Ecole de Management et Président de SupDPO, **Sarah Pauloin**, DPO d'Université Paris Cité, **Eric Fouré**, DPO Adjoint de l'Université de Lille et **Robert Malek**, DPO de l'Institut Mines-Telecom

RSSI et DPO : des intérêts convergents

SupDPO met en lumière les missions complémentaires de ces acteurs clés et l'articulation entre sécurité de l'établissement (RSSI) et celle des personnes (DPO)

L'utilisation croissante des applications numériques par les établissements de l'Enseignement Supérieur et de la Recherche (ESR) s'accompagne d'un renforcement des réglementations et normes européennes et françaises concernant la cybersécurité et la protection des données personnelles. Cette évolution implique que leurs dirigeants prennent en compte les risques juridiques associés et portent la conduite des changements organisationnels et techniques visant à renforcer la sécurité des systèmes d'information de leurs établissements et à assurer une meilleure maîtrise des données à caractère personnel des étudiants, des enseignants et des personnels administratifs.

Bien que leurs missions diffèrent, le rapprochement stratégique entre le Délégué à la Protection des Données (DPO) et le Responsable de la Sécurité des Systèmes d'Information (RSSI) est naturel et bénéfique par la convergence de leurs objectifs respectifs : allier protection des données personnelles d'une part, et sécurité du patrimoine informationnel et des infrastructures, d'autre part. De concert, ils accompagnent les directions des ESR dans un processus d'amélioration de la protection de la vie privée des personnes concernées.

La nécessaire collaboration entre le DPO et le RSSI est d'autant plus prégnante, dans le contexte actuel de cybermenaces auxquelles les ESR font face, que la transposition prochaine de la directive NIS 2 tend à encourager cette dynamique commune. Chaque direction d'établissement se doit donc de mettre en place les conditions favorables à cette coopération indispensable à la protection des données personnelles.

Sur un plan opérationnel, ils doivent impulser des actions d'audit et de conformité adaptées aux différents niveaux de risques en fonction de la sensibilité de la donnée, parmi lesquelles :

- assurer la sensibilisation de la communauté universitaire dans le but de diffuser une culture proactive en matière de cybersécurité et protection des données ;
- élaborer et promouvoir des politiques communes visant à encadrer l'ensemble des processus et des procédures et veiller à leur application par les directions métiers ;
- communiquer sur des procédures de signalement d'incidents de sécurité et de violation des données personnelles ;
- adopter une gestion de crise coordonnée permettant la mise en place rapide de mesures correctives appropriées et notifier aux autorités compétentes dans les temps impartis ;
- accompagner les différentes directions métiers lors de la conception de leurs traitements de données personnelles respectant les principes de privacy et security by design et intégrer ces principes dans la politique d'achat de solutions numériques et dans les projets de développements informatiques internes.

La mise en œuvre de ces différentes mesures techniques et organisationnelles facilitera les actions d'homologation des SI et la réalisation d'analyses d'impact sur la protection des données personnelles.

Pour conclure, la collaboration entre le RSSI et le DPO offre la synergie adéquate pour répondre aux défis complexes de la sécurité des données. Ensemble, ces acteurs clés permettent à l'établissement d'apporter les garanties nécessaires à la protection de la vie privée des personnes. Dans un contexte de cybervigilance accrue, ces deux fonctions pourraient idéalement coexister au sein d'un service dédié à la conformité des établissements.

enjeux et stratégie

CyberEdu
La sécurité par l'enseignement supérieur des NTIC

auteurs
Julien Breyault, Président de l'association CyberEdu et **Philippe Werle**, Premier Vice-président de CyberEdu

CyberEdu, la sécurité du numérique passe par tous !

Sensibiliser en phase d'apprentissage pour labelliser des adultes avertis et concernés

L'enseignement supérieur, une importante force de recherche et de formation en cybersécurité, doit soutenir notre tissu socio-économique et nos établissements. Entreprises, laboratoires, startups, administrations et directions des universités nécessitent une forte acculturation et de solides formations, de la gouvernance au légal, des organisations à la technique.

« […] la sécurité de l'écosystème numérique est une responsabilité partagée : responsabilité de l'État dans la protection des citoyens et des infrastructures critiques, dans l'organisation de la défense et de la sécurité des systèmes d'information ; responsabilité des acteurs économiques dans la sécurité des produits et services qu'ils proposent ; responsabilité des citoyens dans l'exercice de leur vie numérique. »[1]

La démarche **CyberEdu** a été initiée à la présentation en 2015 de la **stratégie nationale pour la sécurité du numérique**[2] **par le Premier ministre**, puis portée depuis 2016 par **France Universités**. « La France sensibilisera, dès l'école, à la sécurité numérique et aux comportements responsables dans le cyberespace. Les formations initiales supérieures et continues intégreront un volet consacré à la sécurité numérique adapté à la filière considérée. »

La sécurité du numérique ne peut pas reposer uniquement sur des experts. Pour CyberEdu, chaque acteur non expert cyber utilisant le système d'information doit se sentir concerné et être impliqué en améliorant sa vigilance, en prévenant l'apparition des vulnérabilités et en facilitant donc la coopération avec les spécialistes.

1 | https://cyber.gouv.fr/publications/strategie-nationale-pour-la-securite-du-numerique-dossier-de-presse

2 | www.cybermalveillance.gouv.fr/medias/2019/11/strategie_nationale_securite_numerique_fr.pdf

Le partenariat qui en a résulté avec l'**Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)** porte sur deux objectifs principaux[3] :

→ Intégrer la **sensibilisation à la cybersécurité** dans toute formation supérieure et dans les formations continues

→ Intégrer la **formation à la cybersécurité** dans toute **formation supérieure intégrant une part d'informatique**.

L' association[4] :

→ réunit des **enseignants**, spécialistes en sécurité et non spécialistes ;

→ **conseille et labellise les formations :**

- au niveau national aux côtés de GT nationaux pour les BTS (CIEL, SIO), les BUT (Informatique, R&T), AFPA, les AMI (CMA dernièrement), du GT Formation du Campus Cyber (matrice de compétences des métiers cyber, ...) ;
- et local (établissements) ;

→ **donne accès aux modules pédagogiques** de la « mallette CyberEdu » qui servent de « briques de base » à l'intégration dans les parcours (licence CC-BY-SA) ;

→ permet à l'adhérent de bénéficier d'un **accompagnement de la communauté** et de **contribuer à l' objectif commun** ;

→ organise des **colloques pour diffuser et alimenter le partage entre enseignants** intervenant dans des formations non dédiées à la cybersécurité (cf. Colloque du CUME de juin 2023 lors du BootCamp des VP-NUM[5] à Angers).

Le label CyberEdu[6], dont le référentiel **a été réalisé avec le centre de formation à la sécurité des systèmes d'information de l'ANSSI**, avec la contribution d'industriels, d'écoles, du Pôle d'Excellence Cyber et du ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche **apporte une assurance aux étudiants et employeurs que** :

→ la formation **intègre correctement et profondément les compétences de sécurité numérique, quels que soient les métiers visés** ;

→ la formation **répond à une charte** et des critères définis par CyberEdu, en collaboration avec les acteurs et professionnels du domaine.

Le label est attribué pour 3 ans renouvelable et permet à la formation :

→ d'être **publiée** sur la page[7] des formation **labellisées** ;

→ d'**utiliser son logo** dans les publications, supports et communications concernant cette **formation** ou dans le **CV du diplômé**.

Ce label s'adresse en priorité aux formations longues :

→ **reconnues par les ministères** de l'éducation nationale, de l'enseignement supérieur et de la recherche, du travail ;

→ **non spécialisées dans les aspects sécurité**, tissant tout au long de leur cursus des contenus en sécurité du numérique pertinents ;

→ dont une **part significative** des enseignements en sécurité repose sur des **intervenants internes à la structure**.

3 | https://cyber.gouv.fr/cyberedu-la-cybersecurite-pour-toutes-les-formations-en-informatique

4 | https://www.cyberedu.fr/pages/adhesions/

5 | https://vpnum.fr/bootcamps/

6 | https://www.cyberedu.fr/pages/labellisation/

7 | https://www.cyberedu.fr/pages/formations-labellisees/

A propos des co-auteurs *NDLR*

Julien BREYAULT

- Président de l'association CyberEdu
- Membre des GT formation du club EBIOS et du Campus Cyber
- Enseignant cyberdéfense
- Responsable pédagogique de la formation professionnelle cyberdéfense (alternance, FC/VAE Ecole Nationale Supérieure Bretagne Sud (ENSIBS)

Philippe WERLE

- Premier Vice-Président de CyberEdu
- Elu du Comité Scientifique et contributeur aux GT NIS2 et Panocrim du CLUSIF
- Expert au Club EBIOS - Membre de l'AFCDP
- Contributeur à PreDon MADICS CNRS
- Responsable Sécurité Système d'Information Gouvernance Risque et Conformité de l'Université Paris Dauphine PSL

Références complémentaire

www.cyberedu.fr
www.wiki.campuscyber.fr/Formation
www.clusif.fr
www.club-ebios.org
www.afcdp.net
www.madics.fr/actions/predon
www.univ-ubs.fr

enjeux et stratégie

auteur·e·s
La rédaction

Le cadre réglementaire de la sécurité du numérique englobe deux grands champs d'application :
La sécurité des systèmes d'information →

La confiance numérique →

Pour mieux comprendre ce cadre règlementaire, consulter la page : S'informer sur la réglementation | ANSSI (cyber.gouv.fr) →

Stratégie de renforcement des moyens alloués à la cybersécurité : comment s'y prendre ?

L'attractivité et la fidélisation des experts cyber est un réel défi. Le travail de fond pour développer les filières de formations à la cybersécurité et l'Appel à Manifestation d'Intérêt *Compétences et Métiers d'Avenir* devraient conduire, à terme, à soulager les tensions entre l'offre et la demande sur le marché du travail. D'ici là, sont présentées ci-dessous certaines solutions « RH » rapportées par les établissements :

→ Mieux comprendre les rémunérations des métiers du numérique grâce au référentiel de la fonction publique afin de mieux comprendre les grilles de rémunération acceptables et favoriser les chances de succès des recrutements d'un expert cyber – Cf. Le référentiel de rémunération des métiers du numérique est mis à jour | Le portail de la fonction publique (fonction-publique.gouv.fr)

→ Faire converger les besoins académiques (apprentissage / formation des étudiants) avec les besoins de l'établissement (sécurisation des SI), en s'appuyant sur la construction de partenariats entre les filières de formation d'ingénieurs et les experts cyber de l'administration et le développement du hacking éthique sur les environnements « bacs à sable » de l'établissement

→ Bien qu'il nécessite du temps de pilotage de la prestation, recourir à des prestataires spécialisés afin de compléter les compétences disponibles. L'allocation d'un budget annuel et le recours à des marchés dédiés permettent de faciliter l'action des experts cyber.

→ Mutualiser les compétences cyber au sein des regroupements universitaires (voire entre eux) et rationaliser les SI et leurs architectures sont des facteurs déterminant le dimensionnement des RH : plus de SI et une architecture non adaptée signifient plus de temps de maintenance cyber.

Plusieurs établissements expliquent aussi plus généralement que l'efficacité de la gouvernance cyber mise en place est un facteur favorisant la rétention des experts cyber.

Développer la stratégie de sensibilisation à la cybersécurité des populations académiques à l'aide des ressources clés en main proposées par les services de l'Etat, et notamment l'ANSSI (SecNumacadémie), la CNIL, Cybermalveillance, PIX, la DGSI).

Stratégie de mutualisation : Les outils juridiques existants pour les établissements publics

- L'article 201 - LOI n° 2022-217 du 21 février 2022 relative à la différenciation, la décentralisation, la déconcentration et portant diverses mesures de simplification de l'action publique locale (1) - Légifrance (legifrance.gouv.fr) et le Décret n° 2023-1019 du 3 novembre 2023 relatif à la mutualisation entre certains établissements publics de l'Etat des fonctions et moyens nécessaires à la réalisation de leurs missions (Légifrance - Publications officielles - Journal officiel - JORF n° 0257 du 05/11/2023 (legifrance.gouv.fr))
- Les solutions du droit de la commande publique tels que les centrales d'achat, les groupements de commande, les contrats public – public (articles L.2511-1 à L. 2511-5 du code de la commande publique pour les marchés publics et Art. L. 3211-1 à L.3211-5 du code de la commande publique pour les contrats de concession), et les outils de coopération prévus par ce code (notamment des articles L. 2511-6)
- Les Groupements d'Intérêt Public sectoriels : Renater, AMUE, France Université Numérique FUN-MOOC, etc.

Quels budgets allouer à la cyber (hors RH), pour quels retours sur investissement ?

Cinq questions à se poser pour déterminer la criticité et les mesures de sécurité du SI

1 · Quel serait le coût d'une attaque réussie sur les missions essentielles et importantes de l'entité ? (humain, financier, réputationnel, opérationnel, pour la Nation, pour les personnes concernées ou pour les partenaires)

2 · L'entité est-elle dépendante du SI : Qu'impliquerait pour l'entité la perte définitive des données ? Combien de temps l'entité peut-elle supporter une interruption du SI ?

3 · Quels sont les niveaux de risque et de la menace à laquelle l'entité doit faire face ?

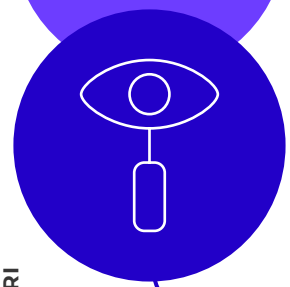
4 · Les mesures de sécurité que l'entité met en place permettent-elles de réduire la probabilité d'avènement d'une crise d'origine cyber ?

5 · Les projets numériques soutenus par l'entité contribuent-ils à :

a. la réduction des risques cyber et de la surface d'attaque ?

b. la conservation de la maîtrise technologique et des compétences au sein de l'entité ?

vue d'ensemble



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

les Crous

auteur
Olivier Perrot,
RSSI-N,
Les Crous

La sécurité au cœur : l'annuaire Active Directory

Mis à disposition par l'ANSSI, le service ADS s'intègre avec succès à la stratégie cybersécurité du CNOUS et des CROUS

Le réseau des Crous, qui a le rôle d'opérateur de la vie étudiante en France, est constitué des 26 Crous régionaux pilotés par le Cnous. Ces 27 établissements constituent un ensemble cohérent en matière de S.I qui mutualise beaucoup au travers de très nombreux outils et démarches communs (tutorat des nouveaux DSI/RSSI, partages de connaissances et expériences, séminaires et webinaires réguliers ...).

L'une des briques essentielles est la présence d'un annuaire pour chaque Crous, alimenté par notre SI RH commun à l'ensemble du réseau, et donc avec un niveau de maturité qui peut être différent d'un établissement à l'autre.

Tous nos établissements sont interconnectés et tous ces annuaires sont repris au sein d'un méta-annuaire commun qui est utilisé comme source d'authentification pour certaines applications.

Il est donc important d'avoir une démarche et niveau de sécurité homogène.

Il a donc été décidé, parallèlement à la mise en place d'une PSSI de cadrage pour le réseau des Crous, de publier une « circulaire SSI » à destination de l'ensemble du réseau qui définit de manière contraignante un plan d'action à suivre, avec des délais de réalisation. La mise à niveau globale de la sécurité de nos annuaires est l'un des points essentiels de ce plan d'actions.

L'ANSSI ayant mis à disposition l'usage d'un outil d'audit des annuaires Windows, nous nous sommes basés sur le résultat de ces audits comme indicateur pour nos annuaires. Même si depuis nous avons acquis divers outils on-premise complémentaires, ADS/Oradad (l'outil de l'ANSSI) reste à ce jour notre indicateur privilégié. L'ensemble des Crous ont donc pour obligation le fait d'atteindre, puis ensuite de maintenir, un indice minimum obtenu avec cet outil.

Aidé par des échanges réguliers avec l'ANSSI, nous avons ainsi réussi à améliorer le niveau de sécurité de nos établissements par des résultats ADS tangibles, allant jusqu'au niveau 5.

La création d'un groupe d'experts SSI issus des 27 établissements (COSSIC pour Comité Opérationnel SSI des Crous) et piloté par notre CSN, associée à une enquête envoyée chaque trimestre aux 27 RSSI régionaux complète le dispositif de pilotage et de partage de connaissance SSI au sein du réseau. Le résultat de l'enquête trimestrielle étant ensuite synthétisée puis partagée avec les RSSI du réseau qui peuvent ensuite voir où ils se situent et, le cas échéant, demander conseil à des collègues plus avancés.

Conscients que les annuaires Windows sont l'une des briques les plus sensibles du S.I commun des Crous, l'objectif avoué est que les 27 établissements atteignent et conservent le niveau le plus haut d'Oradad et se conforment autant que possible aux préconisations de l'ANSSI.

Références :

Pour les entités publiques et régulées :

- **Utiliser le service ADS *(Active Directory Security)***

→ Transmettre les nom, prénom, fonction, email et numéros de portable de deux référents à club@ssi.gouv.fr et au coordinateur sectoriel Enseignement Recherche de l'ANSSI et au FSSI ministériel

→ Télécharger la dernière version d'ORADAD sur GitHub

→ Extraire les fichiers exécutables (ORADAD.exe et fichier de configuration)

→ Ouvrir un terminal, exécuter l'outil avec un compte du domaine et depuis un poste membre du domaine

→ Positionner le fichier de configuration dans le dossier contenant l'exécutable ORADAD.exe

→ Téléverser les résultats sur le portail https://club.ssi.rie.gouv.fr/ après s'être authentifié en cliquant sur « Téléverser des captures d'ORADAD » depuis la page d'accueil

- **Travailler régulièrement sur la bonne progression des mesures de remédiation identifiées**

Pour toutes les entités :

- **Implémenter une architecture AD sécurisée et se former**

→ Consulter le guide Recommandations de sécurité relatives à Active Directory

vue d'ensemble

auteur
Bruno Urbero, directeur de la Cellule Nationale Logicielle / Groupe Logiciel, Ministère de l'Enseignement Supérieur et de la Recherche

Le marché Antivirus : un marché clé en main

Le groupe Logiciel protège les universités en leur proposant de s'appuyer sur le « marché Antivirus » négocié au niveau national pour se doter des services de protection du SI essentiels

Dans le secteur de l'ESR, le Groupe Logiciel porte ou est prescripteur des marchés logiciels du MESR dont bénéficient les 350 établissements adhérents du groupement de commandes. Les besoins communs des établissements en solutions logicielles sont satisfaits par les marchés en place. Ces derniers sont à renouveler tous les 4 ans et évoluent régulièrement. Les solutions de protections des systèmes d'information et de chiffrement entrent dans le cadre de ces marchés.

↘ LE MARCHÉ « ANTIVIRUS »

Le Groupe Logiciel vient de procéder au renouvellement de son marché antivirus pour 4 ans. Le portage de cette procédure a été piloté par Pierre Catala (Responsable cybersécurité-interconnexions de la DSI d'INRAE), Mejdi Bouchlaghem (Responsable des Infrastructures IT de Sorbonne-Université), Michel Chabanne (RSSI Responsable de la Sécurité des SI du CNRS) et Romain Gabeau (Coordinateur du Pôle Infrastructures numériques de l'ADEME) avec le support de la DNE et l'appui du RSSI du MENJ et le soutien logistique de la CNL du MESR.

Ce marché est le résultat d'un travail d'équipe, il se nomme marché antivirus, car le nom est d'usage depuis plus de 20 ans, mais va bien au-delà : il propose des outils de protection du système d'information (SI) qui ne sont pas que de simples antivirus.

Pour aller plus loin : le tout dernier opus de la lettre de la CNL (N°46) met en lumière le marché antivirus, via une interview de Pierre Catala, responsable cybersécurité-interconnexions de la DSI d'INRAE et pilote du marché antivirus.

Les menaces sont omniprésentes et sont sans commune mesure avec celles d'il y a 4 ans. Les vulnérabilités des SI sont liées à : 1) la complexité de leur maintien en condition de sécurité (MCS) par l'application récurrente de correctifs pour supprimer les failles sur tous les serveurs et postes de travail ; 2) un (trop) grand nombre de services exposés à tout Internet pour les rendre accessibles aux nombreux partenaires des établissements de l'ESR ; 3) la fragilité du contrôle d'accès sur simple mot de passe avec leur vol au moyen de phishings. Ceci permet aux cyberattaquants, au bout du compte, de compromettre tout ou partie des SI d'un établissement puis d'exfiltrer et de cryptolocker des données à des fins d'extorsion.

Lorsque les cybercriminels sont entrés au sein du SI, par exemple au moyen d'un compte volé sur un service exposé à tout Internet, leur connexion ressemble à celle de tout utilisateur. Il faut donc des outils capables de déceler et de remonter des activités anormales au sein de la connexion d'un utilisateur standard. Les EDR (Endpoint Detection and Response) sont des outils permettant ce type de détections. Un EDR signale des événements à analyser en indiquant leur niveau de criticité plus qu'il ne les bloque directement. Il faut donc impérativement qu'une équipe, appelée Centre opérationnel de Sécurité (COS ou SOC en anglais) assure l'analyse en continu des évènements de sécurité signalés par l'EDR. L'EDR doit couvrir tous les serveurs et postes de travail afin de bloquer au plus tôt une attaque avant qu'elle ne compromette plusieurs machines.

Ce marché a été prévu pour répondre aux besoins de tous les établissements à un niveau technologique d'une part et à un niveau financier d'autre part. Au niveau technologique, ce nouveau marché répond à la fois aux besoins de ceux qui souhaitaient : 1) continuer avec la protection de base déjà en place de type EPP (Endpoint Protection Platform – Mécanismes bloquant automatiquement par des règles préétablies par leur éditeur notamment des fichiers correspondant à des signatures virales ou des URL de sites Web) ; 2) étendre leurs moyens de détection des intrusions avec un EDR. Au niveau financier, les solutions ayant des fonctionnalités équivalentes au marché précédent s'inscrivent dans la continuité des prix, les solutions plus performantes étant plus onéreuses.

Le volet « services » du précédent marché a été enrichi : le support, la formation, le déploiement avec transfert de compétences s'enrichissent des prestations de services managés et d'appui technique pour conduire une analyse forensique en cas d'une cyberattaque grave nécessitant une gestion de crise. **Les services managés viennent pallier la difficulté à constituer un COS pour certains établissements, indispensable en cas de déploiement d'un EDR, et pour assurer une analyse 24/7 des événements remontés par l'EDR**.

Le marché présente un fonctionnement original sous forme de panier de solutions. Ces paniers permettent aux établissements d'accéder à plusieurs offres par typologie de protection. Ce dispositif permet une continuité d'offres de protection pour les établissements qui le souhaitent et également une variété de solutions pour mettre en place des alternatives.

Trois paniers sont disponibles dans le cadre du présent marché :

→ Les paniers des solutions EPP

→ Le panier des solutions EDR

→ Le panier des solutions antispam

Ces trois paniers s'accompagnent de services.

La liste exhaustive de ces solutions est disponible sur le site du Groupe Logiciel : www.glesr.fr

Une solution pour sécuriser le stockage dans le cloud

Le Groupe Logiciel dans son rôle d'accompagnement des usages a recherché une solution de chiffrement qui permette de stocker sur des espaces en mode nuagique (drive public) des données tout en assurant leur sécurité et leur confidentialité. Les solutions recherchées devaient répondre à plusieurs critères :

- Être open source pour que le coût ne soit pas un obstacle au déploiement
- Être ergonomique, voire transparent à l'utilisation
- Supporter les environnements Windows, MacOS, Linux, Android, iOS
- Offrir un haut niveau de sécurité
- Permettre d'accéder aux drives les plus utilisés : Dropbox, OneDrive, Box, AWS et Google.

Le Groupe Logiciel a initié une démarche pour faire entrer Cryptomator (Cryptomator - Free Cloud Encryption for Dropbox & Co) dans le circuit de certification de l'ANSSI car il correspond à l'ensemble des prérequis exprimés avec une ergonomie adaptée à des utilisateurs non spécialistes. Afin d'initier cette démarche, des échanges ont eu lieu entre l'éditeur du logiciel, l'ANSSI et le Groupe Logiciel. L'objectif est de faire évaluer la sécurité de ce logiciel open source. L'éditeur s'est engagé à apporter toutes les corrections qui lui seraient demandées dans la cadre de cette certification.
Si la certification est positive, la version qui sera diffusée auprès de la communauté ESR, au travers du portail du Groupe Logiciel, sera sans demande d'appel aux dons.

vue d'ensemble

auteurs
Frédéric Culie, responsable de la sécurité de systèmes d'information de la DINUM et **Bastien Guerry**, chef de la mission logiciels libres du département appui, conseil et expertise (ACE) de la DINUM

L'open source, l'atout de la cybersécurité

Ses nombreux avantages en font aujourd'hui des outils privilégiés par l'Etat, on les détaille.

Dans un monde où l'usage du numérique est en constante évolution, la cybersécurité est une préoccupation de tous les instants. Dans ce domaine où les solutions sont de plus en plus nombreuses, quels avantages présente l'utilisation de logiciels libres ? Une question à laquelle il est important de répondre lucidement, car force est de constater que les logiciels libres sont omniprésents dans nos systèmes d'information et que les solutions propriétaires restent une source de dépendance et de coûts importants.

La notion d'open source est associée à la publication de codes sources sous licence libre et à des pratiques de développement communautaires : des développeurs et des utilisateurs actifs partagent leurs connaissances sur la solution, proposent des corrections et des évolutions. C'est dans un tel contexte que les avantages de l'open source sont nombreux :

→ **Auditabilité :** Le code source étant accessible à tout le monde, tout acteur est libre de l'analyser en profondeur et de vérifier que ses fonctionnalités correspondent bien à celles qui sont attendues. Cette transparence permet de détecter plus facilement les éventuelles vulnérabilités ou portes dérobées, renforçant ainsi la confiance que l'on peut avoir dans le niveau de sécurité du logiciel.

Gestion des correctifs : Lorsqu'une vulnérabilité est découverte, les développeurs travaillent ensemble pour la corriger, minimisant ainsi les risques d'exploitation par des attaquants. Plus la communauté est active sur une solution et plus les correctifs de sécurité sont disponibles rapidement.

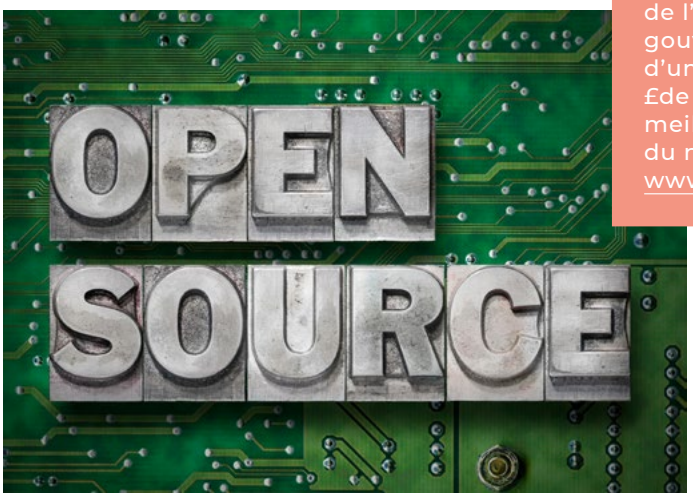
Adaptabilité et sécurité : Offrant une grande flexibilité, les solutions open source peuvent être personnalisées en fonction des besoins spécifiques d'une organisation, ajoutant ou supprimant des fonctionnalités selon leurs attentes.

Maîtrise budgétaire : L'utilisation de logiciels open source permet d'investir dans la cybersécurité les économies faites au niveau de l'achat de licences ; d'autres parts, dans un contexte de partage interministériel, les corrections et développements faits par une administration sont partagés avec les autres. On mutualise ainsi l'investissement dans des communs numériques là où l'achat de licences propriétaires fragmente en dépenses de fonctionnement pour l'avantage de quelques éditeurs.

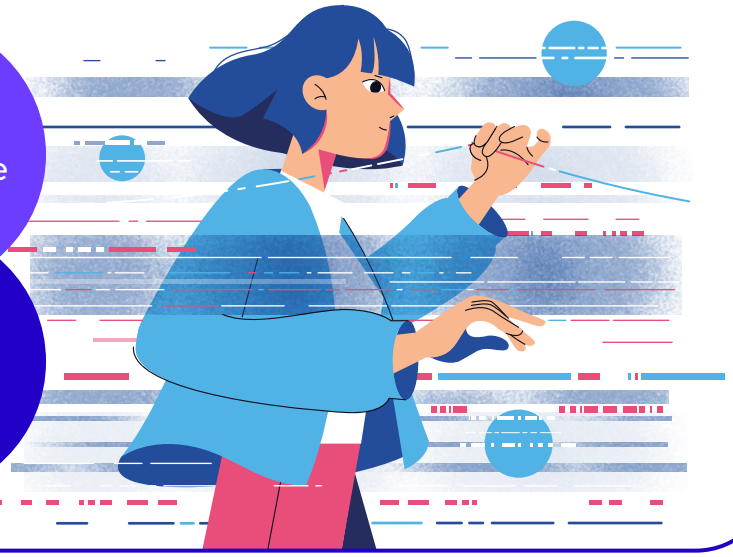
Ces incitations fortes à investir dans des logiciels libres, y compris pour des raisons de cybersécurité, demandent une bonne connaissance des acteurs de cet écosystème et une vigilance permanente : tel éditeur d'une solution open source va-t-il en préserver la licence à long terme ? Telle solution portée par une communauté va-t-elle continuer de recevoir activement des contributions ? Mes développements spécifiques m'obligent-ils à maintenir une version localement, et si tel est le cas, à quel coût ?

Solutions mêlant innovation, liberté, performance et maîtrise budgétaire, les logiciels open source sont des alternatives sérieuses aux solutions propriétaires dont la loi pour une République numérique de 2016 encourage l'utilisation pour la maîtrise, l'indépendance et la pérennité des systèmes d'information des administrations. La mission logiciels libres de la DINUM (https://code.gouv.fr) aide tous les organismes publics à découvrir et utiliser des logiciels libres existants ainsi qu'à publier des projets open source.

La DINUM
Service du Premier ministre, la direction interministérielle du numérique (DINUM) a pour mission d'élaborer la stratégie numérique de l'État et de piloter sa mise en œuvre. Elle accompagne et fait réussir les projets numériques de l'État, au service des priorités gouvernementales et dans un souci d'une amélioration de l'efficacité £de l'action publique tirant le meilleur parti des opportunités du numérique. En savoir plus : www.numerique.gouv.fr/



vue d'ensemble



Responsable cybersécurité, illustration issue de la campagne demainspecialistecyber.fr

auteure
Elina Machefer, cheffe de projet open source, **ANSSI**

Sécurité et open source, quel mix ?

L'ANSSI revient sur l'importance de la prise en compte de la sécurité pour les logiciels open source et continue de contribuer à leur sécurisation.

UNE UTILISATION RESPONSABLE DES SOLUTIONS OPEN SOURCE

Le choix d'une solution open source pour répondre à un besoin d'administration ou à un besoin métier peut présenter de nombreux avantages. Des outils open source sont d'ailleurs présents dans chaque système d'information et dans de nombreux produits propriétaires, qu'il s'agisse d'une démarche volontaire ou non. Le nombre et l'importance de ces produits – outils d'administration de systèmes d'information ou logiciels métiers – ne cesse de croître, ce qui les rend aussi critiques que les solutions propriétaires et les soumet aux mêmes risques de sécurité. Ils peuvent ainsi constituer une fragilité, voire même une porte d'entrée, que certains acteurs malveillants n'hésitent pas à exploiter. L'expérience de Log4j a permis de rappeler la nécessité d'augmenter le niveau de sécurité et de soutenir la maintenance de ces logiciels ouverts.

Le Cyber Resilience Act (CRA) apporte un nouvel éclairage couplé à des exigences pour la cybersécurité des objets connectés mis à disposition sur le marché européen. Si ces impératifs visent les produits commercialisés, la nécessité de la maîtrise de la chaîne d'approvisionnement et un suivi accru des vulnérabilités ont nécessairement un impact sur la maintenance des briques open source sous-jacentes.

Si les solutions open source peuvent faire l'objet de risques de cybersécurité, elles sont également porteuses d'opportunités en la matière.

La disponibilité du code permet, lorsque l'on détient les compétences et les moyens, de bien cerner le fonctionnement d'un outil ou d'un logiciel. Cela laisse aussi la possibilité d'étudier le code et de mener des audits de sécurité.

L'accès au code permet à un administrateur de déployer l'outil en le façonnant selon son infrastructure existante, en adéquation avec ses choix en termes de sécurité, voire même de développer des fonctionnalités *ad hoc*.

Enfin, le fonctionnement sans frontières des communautés open source rend possible la mutualisation d'expertises parfois rares – que ce soit dans des laboratoires de recherche, chez les particuliers, ou encore au sein d'agences étatiques, comme l'ANSSI.

De plus, de nombreux outils open source sont dédiés à la sécurisation de produits ou de systèmes d'information, comme des outils de cartographie, de recherche de compromission, ou encore de partage d'information sur la menace.

Plus largement, pour les solutions dites « métiers » ou les briques sous-jacentes aux infrastructures, la publication en open source des codes ou des packages peut constituer une occasion de renforcer la sécurité.

Ainsi, le choix d'une solution open source doit inclure une réflexion globale prenant en compte les aspects de sécurité et de maintenance du produit choisi. L'économie éventuellement réalisée sur les coûts de licence peut être investie sur du soutien à l'adaptation, à l'installation, au paramétrage et à la maintenance des logiciels. Si le choix de recourir à des solutions open source est encouragé, notamment par la stratégie de transformation numérique de l'Etat, ce choix doit se faire de manière éclairée au sein des organisations.

↘ LES ACTIONS DE L'ANSSI POUR ACCROÎTRE LA SÉCURITÉ DES LOGICIELS OPEN SOURCE

L'ANSSI mène depuis 5 ans des audits de sécurité de produits open source. Ces audits peuvent prendre plusieurs formes. L'une d'entre elle consiste à soumettre un logiciel open source au processus devant mener à l'obtention de la Certification de Sécurité de Premier Niveau (« CSPN »), schéma français faisant partie de la famille des Visas de sécurité de l'ANSSI. La CSPN est conditionnée à une série de tests en « boîte noire » visant à vérifier la robustesse d'un produit par rapport à une cible de sécurité donné. Des produits comme Suricata ou S2OPC ont ainsi pu obtenir un Visa de sécurité.

Lorsque la CSPN n'est pas la solution la plus pertinente pour un produit, d'autres types d'audits sont pilotés par l'Agence qui partage à la communauté les éléments techniques pertinents identifiés au cours des audits (vulnérabilités, recommandations de paramétrage, amélioration de la documentation par exemple). Cela fut notamment le cas pour le produit Sudo.

L'ANSSI a également soutenu financièrement, via le Plan de Relance, un projet du CoTer Numérique, faisant bénéficier d'une campagne de bug bounty 15 progiciels utilisés par les collectivités territoriales.

En complément, l'ANSSI mène différentes actions pour améliorer la sécurité des produits open source en contribuant à certains projets, en soutenant des fondations, en rédigeant des guides techniques disponibles pour tous (tel que celui dédié au développement sécurisé), ou encore en publiant sur son dépôt public des outils utilisés par ses laboratoires ou dans le cadre de ses opérations (tel que le logiciel DFIR ORC).

↘ L'INTÉRÊT D'AVANCER SUR LA MUTUALISATION DES EFFORTS D'AUDITS POUR LES ESRI

L'audit de sécurité de produit open source est un mécanisme accessible à chaque administration ou établissement public. Chacun peut envisager de financer un audit de sécurité sur un logiciel open source, en s'appuyant sur les laboratoires d'évaluation agréés par l'ANSSI (dits « CESTI ») si une CSPN est visée. Cet audit doit s'inscrire dans une démarche globale de gestion des risques et donner lieu à des actions concrètes, notamment pour corriger les vulnérabilités identifiées, en s'attachant à respecter les bonnes pratiques internationales du traitement coordonné de vulnérabilités.

Dans un même temps, force est de constater que la mutualisation des services et infrastructures du secteur de l'enseignement et de la recherche invite au développement d'une **stratégie collective** pour la prise en compte des questions de sécurité. Structurée pour conforter le niveau de sécurité des services « cœur de métier », la définition d'une trajectoire sectorielle de certification ou d'audits des produits les plus utilisés par les établissements apporterait un gage de confiance supplémentaire. Elle permettrait également de faciliter les choix numériques du plus grand nombre, en assurant un niveau de sécurité éprouvé pour l'ensemble des populations académiques utilisatrices.

En savoir plus :
Ces deux pages de références de l'ANSSI :
→ Comprendre la certification | ANSSI (cyber.gouv.fr)
→ Open-source à l'ANSSI | ANSSI (cyber.gouv.fr)

vue d'ensemble

Image générée pour cet article par DALL-E

auteur
Cedric Foll,
Directeur Général Délégué au Numérique, Université de Lille

L'art de rester maitre de son domaine

L'université de Lille développe des moyens stratégiques et techniques pour garantir la sécurité informatique de tous les usagers

L'Université de Lille, consciente des enjeux cruciaux de la cybersécurité, a placé ce domaine au cœur de sa stratégie depuis deux ans. De multiples chantiers ont été engagés pour améliorer la résilience de l'établissement face aux menaces croissantes de la cybercriminalité.

↘ DES TESTS D'INTRUSION

Depuis 2021, des tests d'intrusion annuels sont réalisés par des sociétés expertes en cybersécurité. Ces tests sont essentiels pour évaluer la solidité de notre architecture Active Directory face aux cyberattaques potentielles, notamment celles initiées depuis un poste de travail interne. Cette approche s'inscrit dans une stratégie de défense en profondeur, prenant en compte la possibilité de postes de travail compromis sur notre réseau interne. Un investissement significatif dans les ressources techniques et humaines a été consacré pour assurer une sécurité maximale de notre Active Directory. Cet effort a été reconnu et présenté lors des dernières assises du CSIER par les équipes en charge de ce dossier. Le niveau de sécurité de notre Active Directory a été jugé excellent par l'auditeur lors d'un dernier test d'intrusion, soulignant que c'était, depuis le début de sa carrière, seulement la seconde fois qu'il n'avait pas réussi à devenir administrateur du domaine après une semaine de tests.

↘ LA SÉCURISATION DES TERMINAUX DE L'UNIVERSITÉ

Le deuxième axe stratégique concerne la sécurisation des terminaux de l'université. La Direction Générale Déléguée au Numérique (DGDNum) gère environ 20.000 postes de travail sur les 25.000 terminaux de l'établissement. Il a également été observé plusieurs cas de compromissions ou de postes de travail ne respectant pas les standards de sécurité, tels que l'absence de chiffrement, dans plusieurs laboratoires. Afin d'augmenter le niveau de sécurité de l'ensemble des postes de l'établissement, une collaboration étroite a été établie avec les informaticiens des composantes et laboratoires non gérés directement par la DGDNum, ainsi qu'avec la délégation régionale du CNRS avec la constitution de groupes de travail sur le sujet. L'objectif était de définir des standards de sécurité communs, applicables à tous. Ces mesures comprennent un inventaire obligatoire des postes de travail pour une vision consolidée de leur niveau de sécurité, le chiffrement systématique des postes fixes et nomades, la mise à jour régulière des antivirus et pare-feu, ainsi que des systèmes d'exploitation et des logiciels. L'intégration aux outils de gestion centralisés, l'application du principe de moindres privilèges et l'obligation de sauvegarder les données sont également des éléments clés de cette stratégie. Ces objectifs de sécurité ont été validés par le Président et la Direction générale des services pour une application dans l'ensemble des périmètres de l'établissement avec le concours de la délégation régionale du CNRS.

↘ DES CHANTIERS À VENIR

En 2024, la DGDNum a initié des chantiers additionnels. Parmi ceux-ci, la souscription à un service de sensibilisation au phishing pour la réalisation de fausses campagnes de phishing et des capsules vidéo d'autoformation, ciblant les 130.000 boîtes mails de l'établissement plusieurs fois par an avec des indicateurs de pilotage quant aux taux de clics sur les messages. De plus, la mise en place d'EDR (Endpoint Detection and Response) sur l'ensemble des terminaux et serveurs est en cours, avec une souscription à un service de surveillance managée opérant en continu 24h/24 et 7j/7. Enfin, une étude approfondie est menée sur le déploiement d'une authentification forte à l'échelle de l'établissement, un défi complexe dans l'environnement de l'enseignement supérieur et de la recherche, compte tenu de la diversité des usagers et de l'utilisation potentielle de terminaux personnels pour le second facteur d'authentification.

En bref : la DGNUM de l'Université de Lille
La DGDNum de l'université de Lille opère le système d'information pour les 85.000 étudiants et 8.000 personnels de l'établissement. Elle assure la gestion et le support numérique pour les services centraux et la plupart des composantes de l'établissement. À ce titre, elle assure le maintien en conditions opérationnelles et de sécurité de 20.000 terminaux sur les 25.000 environ que compte l'établissement, ainsi que de 1.500 serveurs virtuels. https://www.univ-lille.fr/

vue d'ensemble

Université Paris Cité

auteur
Mathieu Thuaire, RSSI, Université Paris Cité

Mot de passe : « Bring Your Own Device »

Et si sa sécurisation était une affaire plus simple que ce que l'on pensait ? A l'université Paris Cité, la réflexion est engagée

En préambule rappelons que le RSSI, de par sa nature, a développé une aversion particulière au risque.

Par ailleurs, les universités sont intrinsèquement susceptibles de voir un grand nombre d'équipements hétérogènes et non maitrisés se connecter à leurs SI. La problématique du BYOD (*NDLR* : L'acronyme « BYOD » est l'abréviation de l'expression anglaise « Bring Your Own Device » soit en français : « Apportez Votre Equipement personnel de Communication ») est donc prégnante pour ces entités.

Dans ce cadre, plusieurs réflexions doivent être menées :

→ Tout premièrement, l'identification des besoins à couvrir. Il faudra bien évidemment prendre en compte le **niveau de service** que vous souhaitez fournir, notamment vis-à-vis de l'accès aux données, et de la capacité à extraire ces données sur des appareils non maitrisés ;

→ Une réflexion basée sur une **analyse de risque** qui permettra de définir les scénarios envisagés et les risques contre lesquels l'établissement souhaite se prémunir. Cela nécessite donc de travailler avec l'AQSSI (Autorité Qualifiée pour la Sécurité des Systèmes d'Information) en amont du projet ;

→ Les **moyens** mis à disposition. En effet, le niveau d'engagement technique, financier et RH sera dimensionnant pour le maintien de la solution dans le temps.

Il est bien évidemment possible de déterminer plusieurs mesures qui pourront aller du simple engagement de l'utilisateur, à des contraintes techniques fortes. Les architectures

retenues sont nombreuses et doivent être adaptées aux risques de l'entité. Dans cette réflexion, il ne faut pas oublier de garder la **proportionnalité** entre les solutions et le risque afin d'obtenir une solution adaptée à son environnement.

Quelle que soit la solution envisagée, il est indispensable de communiquer, notamment sur les limitations d'usage et cadre de mise en œuvre (ex : appareil sur lesquels vous pouvez refuser l'accès si les OS sont obsolètes, poste de travail de l'entreprise uniquement, imposer un VPN, …).

En effet, certaines solutions (ex : mise en place de DMZ[1], ZTNA[2], VPN, SASE[3] …) peuvent entraîner des limitations en fonction des besoins à couvrir.

Cependant, l'usage de ces outils ne doit remplacer les premières des précautions que l'on retrouve notamment au travers des guides de l'ANSSI[4], ou de la CNIL[5] sur l'usage de mot de passe fort, du cloisonnement, du chiffrement des flux, des politiques des antivirus, … Sans oublier les règles premières que sont le juste besoin et le principe des moindres privilèges.

Compte tenu de ce contexte, il apparaît que plusieurs solutions peuvent s'appliquer en parallèle, voir être utilisées complémentairement :

→ L'usage de solution du type VDI (Virtual Desktop Infrastructure). Cette solution permet de s'affranchir de tous les équipements, puisque vous hébergez ou faites héberger vos postes virtualisés directement dans vos infrastructures. L'inconvénient régulièrement rencontré dans ce type de solution est l'expérience utilisateur qui diffère d'un usage classique. Cette solution est toutefois très adaptée lorsqu'il est nécessaire de protéger les données de l'usager qui doit se connecter dans un environnement peu sécurisé (ex : données de recherche dans des pays dit de confiance réduite, télétravail …) ;

→ Une approche qui se veut plus circonscrite (notamment pour des accès applicatifs), vers des solutions orientée ZTNA. Cette solution peut être mise en place, notamment lors d'usage de solution cloud. Ce choix repose sur une identification fine des droits des usagers par applicatifs. Elle est complémentaire à la solution n°1

Quel que soit le choix, ce dernier ne doit se faire que lorsque les **cas d'usage** et les **moyens** pour atteindre les objectifs ont étés fixés en amont.

L'avantage de ce type de solutions reste la maîtrise de vos réseaux et systèmes. Coupler à un cloisonnement fort de vos droits d'administration, une telle architecture permettra une exposition aux risques réduite lorsque vous n'avez pas la capacité de maîtriser votre parc informatique. Cet enjeu étant d'autant plus important avec l'approche d'événements comme les JO 2024.

1 | Demilitarized zone

2 |Zero Trust Network Access

3 |Secure Access Service Edge

4 |https://cyber.gouv.fr/bonnes-pratiques-protegez-vous

5 |https://www.cnil.fr/fr/byod-quelles-sont-les-bonnes-pratiques

vue d'ensemble

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE

Liberté
Égalité
Fraternité

auteur
Joffrey Célestin-Urbain,
Directeur, Service de l'information stratégique et de la sécurité économiques, Ministère de l'économie, des finances et de la souveraineté industrielle et numérique

Lumière sur le SISSE

Sa place, et son rôle dans la protection de la recherche scientifique

Le Service de l'information stratégique et de la sécurité économiques (Sisse) a été créé en 2016. Ce service a une mission opérationnelle de ***protection des actifs stratégiques de l'économie française face aux menaces étrangères****.*

Rappelons que la sécurité économique et la cybersécurité sont des jumeaux. En sécurité économique comme en cybersécurité, il faut être très vigilant, y compris avec des partenaires de confiance. Une différence de taille, cependant, réside dans le fait qu'une menace de sécurité économique ne relève pas forcément, de la part des acteurs privés, d'une volonté de nuire. Nous devons, au quotidien, identifier ce qui, parmi les dizaines de partenariats étrangers noués par les entreprises et centre de recherche français, peut soulever des difficultés pour nos intérêts nationaux. En un mot, il s'agit de concilier les intérêts particuliers, souvent légitimes, d'opérateurs économiques avec l'intérêt général.

Les attaques croissantes qui ciblent la France n'épargnent bien évidemment pas le monde de la recherche. Depuis 2020, la menace globale a considérablement augmenté. En 2023, le SISSE a traité ainsi plus de 900 dossiers de sécurité économique, de nature très variée dont une part croissante étaient des attaques visant à la source les innovations portées par les centres de recherche (vol, intégrité, disponibilité visant l'atteinte réputationnelle, le débauchage de chercheurs de talents, l'espionnage, etc…). En lien avec nos partenaires au sein de l'administration, le Secrétariat général pour la défense et la sécurité nationale, et le Ministère de l'enseignement supérieur et de la recherche en premier lieu, nous avons bâti un dispositif complet de protection de la recherche sensible (aussi bien la recherche fondamentale qu'appliquée) -innovation-industrialisation.

Cette politique de protection de la recherche, très amont, a dû évoluer en fonction de la menace étrangère. Si l'espionnage scientifique et technologique n'est pas nouveau (cf. l'infiltration du projet Manhattan dès 1942 par le renseignement soviétique), la compétition économique accrue, la recherche par des puissances étrangères de la maîtrise de technologies disruptives donc d'avancées scientifiques (IA, quantique, biotechnologies, semi-conducteurs, etc.), nous imposent une extrême vigilance concernant les domaines sensibles de la recherche scientifique. A cet égard, le cyber est un vecteur majeur d'atteinte à nos intérêts scientifiques que ce soit à travers des attaques ciblées contre des laboratoires stratégiques pour perturber voire paralyser leur fonctionnement, obtenir un levier dans un rapport de forces (avec espérance de gains ou non), ou dérober des données à haute sensibilité, ou des attaques au sens large visant à fragiliser notre souveraineté.

C'est à travers un travail permanent de sensibilisation symétrique, à la fois aux risques de sécurité économique et aux risques cyber, en partenariat étroit avec l'ANSSI, les Services des haut-fonctionnaires de défense et de sécurité des ministères de tutelle et les Responsables pour la sécurité des systèmes d'information des établissements de recherche, mais aussi de prévention, et parfois d'entrave, que la sûreté des laboratoires sensibles monte insensiblement en gamme et en efficacité.

Avec un enjeu particulier, propre à la recherche, que constitue l'ouverture internationale de nos chercheurs. Protéger sans entraver la liberté académique de nos scientifiques, alerter sur les menaces sans remettre en cause le principe d'un espace mondialisé de la recherche scientifique, coopérer avec pragmatisme mais sans naïveté, c'est là l'équilibre constant que nous devons trouver.

vue d'ensemble

victeezy.com

auteures
Véronique Gauthier, RSSI, et **Aude Houdan-Fourmont,** FSD, Université de Caen-Normandie

Laboratoires sensibles et menace cyber

A l'université de Caen Normandie, on travaille sur les audits et retours d'expérience pour améliorer, toujours, les dispositifs de sécurité

La menace cyber n'a cessé d'augmenter ces dernières années, en témoignent les nombreuses attaques dont la presse se fait régulièrement écho. La recherche n'échappe pas à cette tendance, les laboratoires doivent donc être protégés. Si cette protection est encadrée par le dispositif de Protection du Patrimoine Scientifique et Technique (PPST), et la mise en place de Zones à Régime Restrictif (ZRR), comment agir concrètement au quotidien dans les laboratoires pour sécuriser les Données Sensibles (DS) ?

Données sensibles :
Les données sensibles sont en lien avec les activités de recherche dont le détournement ou la captation pourraient porter atteinte aux intérêts économiques de la nation, renforcer des arsenaux militaires étrangers ou affaiblir les capacités de défense françaises, contribuer à la prolifération des armes de destruction massive et de leurs vecteurs et/ou être utilisés à des fins terroristes sur le territoire national ou à l'étranger.

↘ IDENTIFIER LES DONNÉES SENSIBLES

En premier lieu, un recensement des DS est indispensable, sur support matériel dont les cahiers de laboratoire comme numérique. Cet inventaire doit être mis à jour régulièrement et transmis au Responsable de la Sécurité du Système d'Information (RSSI) et au Fonctionnaire Sécurité Défense (FSD) annuellement. Cette liste sera intégrée aux politiques sûreté et PSSI de l'établissement.

↘ SÉCURISER L'ACCÈS AUX DONNÉES

Ensuite, la sécurisation de l'accès aux DS s'appuie sur un management des accès physiques aux locaux (organigramme des clefs, gestion des droits, armoire à clef sécurisée...) dans un schéma directeur de sûreté intégrant également le déploiement des contrôles d'accès et d'une éventuelle vidéoprotection.

Concernant les accès au système d'information, une gestion des identités et des accès (IAM) est à mettre en place avec une revue annuelle des droits. Des outils de sécurisation des mots de passe comme des coffres forts de mots de passe et l'authentification multi-facteurs sont à privilégier.

L'architecture du stockage doit être pensée en fonction des DS et de l'IAM en intégrant des restrictions d'accès pour certaines données. Les supports amovibles sont à proscrire, au bénéfice de stockage et/ou clouds institutionnels. Si plusieurs solutions sont proposées, un choix unique de stockage est une solution intéressante, pour limiter les transferts de données d'un stockage à l'autre et les versions multiples.

Une attention particulière doit être portée sur la gestion des données et la protection du matériel en conditions de mobilité des personnels à l'étranger notamment, en proposant du matériel dédié à cet usage, ne contenant aucune DS.

Enfin, les ordinateurs et solutions de stockage doivent être chiffrés. Les transferts de données doivent se faire à l'aide d'outils sécurisés.

↘ RÉDUIRE LE RISQUE LIÉ À L'HUMAIN

Malgré toutes les mesures de prévention mises en place, le facteur humain reste difficile à maîtriser, entraînant des failles de sécurité comme le mot de passe collé sous le clavier, les sessions non fermées, les documents laissés sur le bureau ou les données sur un tableau...

Liens utiles :
→ PPST : https://www.sgdsn.gouv.fr/nos-missions/proteger/proteger-le-potentiel-scientifique-et-technique-de-la-nation
→ PSSIE : https://cyber.gouv.fr/cadre-de-gouvernance-de-la-securite-numerique-de-letat-pssie
→ Bonnes pratiques à l'usage des professionnels en déplacement : https://cyber.gouv.fr/publications/bonnes-pratiques-lusage-des-professionnels-en-deplacement
→ Se former à la sécurité du numérique : https://secnumacademie.gouv.fr/

Des correspondants internes au laboratoire prennent en charge la sensibilisation au quotidien, disposeront de fiches réflexes adaptées pour faire face aux incidents et pourront s'appuyer sur les ressources internes (RSSI et FSD).

En appui à la sensibilisation interne au laboratoire, une politique de formation des personnels des laboratoires est à déployer. Les acteurs locaux de l'ANSSI, DGSI ou la préfecture sont des interlocuteurs de choix pour porter une parole extérieure et des bonnes pratiques aux collaborateurs.

Si un système de management de la sécurité permet de réduire le risque, il ne permet pas de l'éliminer. Une analyse de tous les incidents (RETEX) ainsi qu'un audit régulier de ce dispositif permettra une amélioration continue de la sécurité, et la prise de conscience de chacun des enjeux de la sécurité reste un objectif essentiel.

vue d'ensemble

auteur
ANSSI,
Division de la coordination sectorielle

Conseils de cybersécurité aux chercheurs et aux opérateurs critiques[1]

Pour que la recherche fasse bon ménage avec ses partenaires sensibles

(1) Sont désignés dans l'article en tant qu'« Opérateur critique » :

•Les Opérateurs d'Importance Vitale soumis à la Loi de Programmation Militaire

•Les Opérateurs de Services Essentiels soumis à la directive NIS

•Les Entités Essentielles et les Entités Importantes entrant dans le champ d'application de la directive NIS2 (qui sera transposée en droit français en 2024)

•Les entités entrant dans le cadre du dispositif de Protection du Patrimoine Scientifique de la Nation

(2) Sont désignés dans l'article en tant que « Données protégées » les données entrant dans le cadre des données sensibles ou protégées au titre des différentes dispositions légales (secret de la défense nationale, secret des affaires, secret statistique, secret médical, secret des correspondances, secret des sources des journalistes, etc.)

(3) Sont désignés dans l'article en tant qu'« équipements » tout appareil technique pouvant entrer dans une des catégories suivantes :

•Ordinateurs, smartphones et équipements informatiques divers

•Equipements de laboratoire (oscillateur, laser, etc.) et systèmes industriels (automate, robots, etc.)

•Applications et services numériques utilisés pour la bureautique, la collaboration et / ou la recherche (y compris dans le Cloud)

↘ CONSEILS AUX CHERCHEURS MENANT DES PROJETS DE RECHERCHE EN PARTENARIAT AVEC DES OPÉRATEURS CRITIQUES

La violation des données protégées[2] ou l'accès non autorisé à un système d'information d'un opérateur critique peut engager votre responsabilité (administrative et/ou pénale) et celle de votre établissement d'affiliation, voire celle de l'opérateur critique.

→ 1 ● Pour mémoire, soyez vigilants, adoptez les bons réflexes dans votre quotidien numérique et respectez les règles d'hygiène informatique (à retrouver sur https://cyber.gouv.fr/bonnes-pratiques-protegez-vous) :

1 ● Maîtrisez vos mots de passe

2 ● Sauvegardez régulièrement vos données et renseignez-vous auprès des experts cyber, sur la politique de sauvegarde de vos données de recherche protégées ou sensibles mise en œuvre par votre établissement

3 ● Séparez votre environnement numérique professionnel de votre environnement numérique personnel

4 ● Mettez à jour régulièrement vos équipements[3]

5 ● Protégez vos équipements et vos communications des accès ou captations indésirables (utilisez un antivirus ou le VPN de votre établissement, évitez les réseaux Wi-Fi publics ou inconnus, etc.)

6 ● Protégez la confidentialité des données en accordant le juste niveau de privilèges

7 ● N'utilisez pas votre compte académique pour souscrire à des logiciels ou abonnement en ligne gratuit. En cas de besoin impératif, utilisez une adresse de messagerie temporaire et destinée à cet usage unique

8 ● Évitez les sites qui vous semblent douteux et effectuez vos téléchargements depuis des sources sûres

→ 2 ● Renseignez-vous sur l'état de la menace cyber et les enjeux du secteur et de l'opérateur sur https://www.cert.ssi.gouv.fr/cti/

→ 3 ● Déterminez les SI collaboratifs et de recherche et équipements informatiques nécessaires pour votre projet de recherche, en accord avec la chaîne SSI de son établissement et celle de l'opérateur critique

a. Intégrer les risques cyber à l'analyse de risque de son projet de recherche

b. S'assurer que les environnements numériques souhaités sont adaptés à l'analyse de risque de l'opérateur critique

c. Faire valider ces moyens par la chaîne SSI de l'opérateur critique ou privilégier son écosystème numérique dédié aux chercheurs

d. Ne partagez pas vos accès, les autorisations d'accès doivent rester personnelles et incessibles

→ 4 ● Convenir par voie contractuelle d'une convention-cadre entre votre établissement d'affiliation et l'opérateur critique validant l'écosystème numérique utilisable par les chercheurs participant au projet de recherche

→ 5 ● Tout au long du cycle de recherche :

a. Informez la chaîne SSI et l'opérateur critique de toute suspicion d'atteinte à votre environnement de travail associé à votre projet de recherche

b. Informez votre chaîne SSI et l'opérateur critique du bon respect du cycle de gestion des données (destruction, anonymisation, hébergement sur une plateforme sécurisée, etc.)

L'utilisation d'équipements informatiques personnels est prohibée. L'acquisition de matériels informatiques sur les fonds fléchés du projet de recherche doit respecter le cycle de gestion de votre établissement.

↘ CONSEILS AUX OPÉRATEURS CRITIQUES PARTICIPANT À UN PROJET DE RECHERCHE

1 ● Connaître l'état de la menace cyber et les enjeux pour votre secteur d'activité

2 ● Faire une analyse de risque cyber pour les projets de recherche et d'innovation impliquant votre organisation

3 ● Prévoyez la mise à disposition d'un SI et d'équipements numériques dédiés à la recherche idéalement cloisonnés du reste de votre SI et le proposer aux chercheurs impliqués ; Prévoyez la mise à disposition de comptes nominatifs avec une date de fin définie en amont du programme

4 ● Convenez par voie contractuelle d'une convention-cadre validant l'écosystème numérique utilisable dans le cadre du projet de recherche, et les mesures de sécurité à mettre en œuvre par les chercheurs participant au projet de recherche :

a. Y associer votre charte d'utilisation des systèmes d'information, annexé à votre règlement intérieur

b. Y définir impérativement et de manière proportionnée au projet :

i. la temporalité et le périmètre des accès aux données, au SI ou au site

ii. le cycle de vie des données transmises (y compris lors de la revue par les pairs et après la publication)

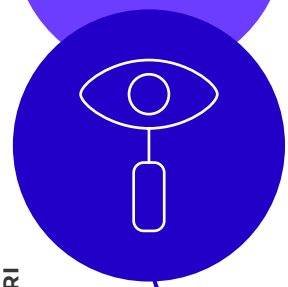
iii. les modalités d'hébergement des données strictement autorisées

NB : En cas de recherche interne à votre organisme, prévoir des dispositions écrites permettant d'engager les chercheurs sur la cybersécurité du projet (chartes, clauses dédiées dans les contrats de travail, etc.)

5 ● En cas de mise à disposition de données protégées, s'assurer de la sécurisation dans le temps des données et de leur bon hébergement ou destruction, conformément au cycle de vie validé

6 ● En cas d'entretiens de recherche réalisés avec les personnels de l'opérateur critique, rappeler les règles associées à la protection du secret

vue d'ensemble



auteurs
Jean Langlois-Berthelot, enseignant à Sciences Po, et **Marc-Olivier Boisset,** ancien enseignant à Sciences Po, enseignant en cybersécurité à l'école Hexagone et EPITA

Se former à la cyber. Quel choix ?

Cet article nous aide à comprendre les nuances de l'enseignement de la cybersécurité et ses trois approches essentielles

L'enseignement de la cybersécurité revêt diverses facettes, reflétant les besoins spécifiques des différents publics visés et des organisations publiques ou privées. Cependant, cette diversité peut parfois sembler confuse, notamment en raison de la variété des approches pédagogiques et des objectifs d'apprentissage.

→1● La Vulgarisation des Enjeux pour les Non-Techniciens

Pour les profils non-techniques, la cybersécurité nécessite une approche de vulgarisation. Il s'agit de comprendre et de sensibiliser aux risques dans le cyberespace pour les pays et les organisations. Des cours adoptant une perspective géopolitique, managériale ou juridique sont essentiels pour transmettre ces notions complexes de manière accessible.

→2●La Gestion de crise dans le cyberespace : Une Discipline en Management des Systèmes

Pour les profils techniques non spécialisés et certains non-techniques travaillant régulièrement avec des profils techniques, la gestion de crise dans le cyberespace est centrale. Elle s'intègre parfaitement dans les formations en management ou en école d'ingénieur, offrant une compréhension approfondie des aspects managériaux de la sécurité des systèmes et de la gestion des incidents.

→3● Approfondissement Technique : Informatique, Ingénierie et Mathématiques

Enfin, les formations techniques se concentrent sur les aspects hardware et software, plongeant dans les domaines de l'informatique, de l'ingénierie et parfois des mathématiques. Ces cursus visent à former des experts capables de manipuler les couches fondamentales des systèmes informatiques pour assurer leur sécurité.

↘ CONCLUSION : L'IMPORTANCE DE LA CLARTÉ DANS L'ENSEIGNEMENT.

Comprendre cette diversité d'approches est crucial pour éviter toute confusion chez les étudiants. Choisir le bon parcours éducatif dépend grandement de la clarté autour de ces différentes branches de la cybersécurité. Cette distinction permet d'orienter les étudiants vers les cursus qui correspondent le mieux à leurs aspirations et compétences.

vue d'ensemble

auteur
Vincent Neuville
est Officier Supérieur et Expert en Cybersécurité au sein de l'Armée de l'Air et de l'Espace, enseignant à EPITA et à l'Ecole Hexagone

Innovations dans l'enseignement de la Cybersécurité à Sciences Po ?

Quand le Ministère des Armées valorise les initiatives d'innovation pédagogique au service de l'intérêt commun.

Enseigner des sujets aussi pointus que l'innovation dans la cybersécurité à des profils non spécialistes est un défi majeur. C'est un défi qui va au-delà des enjeux liés à la simple transmission de connaissances, car il exige une approche pédagogique adaptée et équilibrée pour garantir une compréhension sans simplification excessive ni focalisation dans des détails techniques sans pertinence pour ces profils.

L'exemple marquant des enseignements proposés à Sciences Po (voir article précédent) dès 2018 par Marc-Olivier Boisset et Jean Langlois-Berthelot (sur l'identité digitale, les risques cybers émergents, le data mining pour l'analyse et la prévision en cybersécurité etc.) est un cas emblématique de cette démarche délicate. En choisissant cet établissement, ces enseignants venus de postes d'expertise au sein du Ministère des Armées avaient pour objectif, avec l'appui de leurs supérieurs, de sensibiliser les futurs décideurs, souvent issus des sphères administratives et politiques, à des enjeux technologiques complexes qui façonneront l'avenir de la cybersécurité.

Mettre en place une approche pédagogique singulière est fondamentale. Éviter la simplification excessive tout en rendant une compréhension suffisante accessible à un public non spécialiste est un équilibre difficile à atteindre. Il ne s'agit pas simplement de présenter des connaissances, mais de susciter la compréhension des enjeux, des implications et des aspects concrets de ces technologies. L'enseignement de l'innovation technologique et scientifique à des profils non spécialistes soulève plusieurs défis. Il faut créer une passerelle entre le monde complexe de la technologie et la réalité quotidienne de ces futurs décideurs. Cela nécessite une communication claire mais précise, en évitant le jargon sans pour autant tomber dans une simplification excessive qui réduirait la substance des sujets abordés. Un autre défi majeur réside dans le choix de la pertinence des connaissances transmises. Il est essentiel d'identifier les facteurs cruciaux des innovations technologiques qui impacteront directement ces profils, sans s'enliser dans des détails superflus pour leur domaine d'études et de carrière.

Enseigner ces sujets exige également une adaptation constante. Les technologies évoluent rapidement, et les enjeux de cybersécurité changent avec elles.

Malgré ces défis, la nécessité de cette démarche est indéniable et s'appuie sur une reformulation continue des contenus des enseignement. Préparer les futures élites administratives à comprendre ces technologies leur permet de prendre des décisions éclairées, de formuler des politiques adéquates et de favoriser l'innovation au sein des administrations. Cela peut également favoriser une culture d'adaptation et de compréhension des évolutions technologiques, permettant à ces profils non techniques de s'adapter efficacement à un monde en constante mutation.

Il est remarquable que ce soit de jeunes profils du Ministère des Armées qui, avec l'appui de leurs administrations, aient réussi à convaincre un lieu emblématique tel que Sciences Po de la nécessité de cette approche pédagogique innovante.

Les effets de cette initiative pédagogique se sont manifestés naturellement par les retours positifs des (anciens) étudiants désormais actifs dans diverses administrations (Economie, Intérieur et Affaires Etrangères en particulier). Ces élèves formés à la compréhension des enjeux technologiques ont su tirer parti de ces connaissances pour orienter des politiques, formuler des stratégies et favoriser l'innovation dans un secteur structurellement transversal: le Cyber.

Bibliographie

→ Boisset, M.O. and Langlois, J., 2021. An analysis of the Pegasus case: Rise of cyber threats.
→ Boisset, M.O. and Langlois-Berthelot, J., 2019. Conditions for the emergence of cyber-insurance
→ Boisset, M.O. and Langlois, J., 2021. Démocratisation des cyberarmes: Montée en puissance des cyber-menaces. CRSI.

vue d'ensemble

Généré par IA

auteur·e·s
Sara Sellos, Ingénieure Principale des Etudes et Techniques de l'Armement au Centre d'Analyse *technico-opérationnelle* de Défense de la Direction Générale de l'Armement;
Nicolas Fouville, Analyste SOC à la Direction Générale de l'Armement

Attaquer pour mieux se défendre

Tel est le leitmotiv de « Kids Can Hack », une plateforme éducative de « hacking éthique » qui développe la culture relative à la cybersécurité

Les enfants sont aujourd'hui confrontés de plus en plus tôt au « monde numérique ». Selon une étude menée en 2023 par Toluna-Harris Interactive pour l'association e-Enfance, les enfants commenceraient à utiliser Internet en autonomie avant l'âge de 7 ans. En outre, près de **46 %** d'entre eux seraient équipés d'un **smartphone avant l'âge de 10 ans**.

Malgré cette connectivité grandissante et de plus en plus précoce, le cyberespace reste en général largement méconnu du grand public et tout particulièrement des plus jeunes. Si la sensibilisation aux risques numériques s'est fortement accentuée dès l'école primaire, les approches visant à faire découvrir aux enfants la cybersécurité sont généralement de nature purement théorique. Pourtant, pour bien l'appréhender, cette discipline requière aussi une approche par la « pratique ».

Le hacking éthique permet clairement d'atteindre cet objectif car il consiste à « apprendre l'attaque pour mieux se défendre ». Il conduit à s'intéresser à des problématiques informatiques complexes tout en créant de nouvelles méthodes ou de nouvelles technologies pour les résoudre. Le hacking éthique est donc une excellente discipline pour mieux comprendre le cyberespace, le manipuler de façon concrète, et se protéger contre les risques qui le menacent.

Toutefois, les ressources de hacking éthique existantes ne sont pas particulièrement adaptées pour les enfants. Ces ressources sont majoritairement conçues pour un public plus âgé, déjà doté de prérequis techniques pointus dans le domaine informatique. Cette caractéristique conduit à faire du hacking une activité dite « underground », exclusivement réservée aux spécialistes « aguerris », la rendant quasi-inaccessible à un public néophyte.

Pour susciter l'intérêt des plus jeunes, nous avons développé une plateforme d'apprentissage spécialement dédiée aux apprenants. La plateforme « Kids Can Hack », accessible sur www.challenges-kids.fr, comprend une trentaine de challenges de cybersécurité permettant de découvrir diverses thématiques (web, cryptanalyse, stéganographie, réseaux informatiques) tout en développant sa culture générale. Les seules compétences requises pour résoudre les épreuves consistent à savoirs lire, écrire et compter. L'âge et le cursus de formation de l'apprenant ne sont donc pas une condition d'accès aux jeux-challenges proposés. Des fiches

pédagogiques seront publiées prochainement dans un ouvrage afin d'aider à l'animation des séances pédagogiques et à la résolution des challenges.

Chaque challenge a été conçu pour atteindre un ou plusieurs objectifs pédagogiques, tels que faire comprendre une notion technique essentielle (par exemple, le système hexadécimal) ou bien sensibiliser à un risque spécifique (par exemple, le quishing). Certains challenges sont reliés les uns aux autres, permettant aux apprenants de réinvestir leurs acquis vers de nouvelles compétences. Enfin, nous avons cherché à mettre en jeu des failles de cybersécurité réalistes et très répandues, en associant chaque challenge à des cas réels de cyberattaques, afin de marquer les esprits. Après avoir résolu l'ensemble des challenges disponibles sur la plateforme « Kids Can Hack », les apprenants sont capables de poursuivre leur initiation sur d'autres plateformes de hacking éthique, tel que PicoCTF (https://picoctf.org/). Ils peuvent aussi se lancer sans réserve ni appréhension dans des compétitions « Capture The Flags » organisés dans certains établissements.

Initialement, le projet a été développé à destination de l'enseignement primaire et du collège, mais l'acculturation de toutes les générations étant nécessaire, les entreprises, les associations, les grandes écoles et universités peuvent avantageusement utiliser « Kids Can Hack » pour promouvoir auprès de leurs publics une expérience plus pragmatique aux risques cyber. Nous encourageons les enseignants, associations d'étudiants, et RSSI et DPO à s'en saisir dans le cadre de leurs évènements, leurs actions de sensibilisations ou de découverte des métiers du numérique.

« Kids Can Hack » offre aux établissements une solution pour répondre au défi numérique qui s'impose à tous, à savoir augmenter la culture numérique des futurs décideurs et ouvrir « la boîte noire[1] », susciter des vocations pour la filière cybersécurité et permettre d'attirer davantage les jeunes filles. Dans un contexte où la cybermenace augmente constamment, face à une pénurie d'experts permettant de répondre à la dématérialisation généralisée des processus, et face à un taux de féminisation particulièrement faible, il est primordial de mieux valoriser les métiers de la cybersécurité auprès des plus jeunes et d'accroître le vivier de compétences sur le marché du travail.

1 | https://www.polytechnique-insights.com/tribunes/digital/inexplicabilite-de-lia-un-enjeu-organisationnel/

Demain Spécialiste Cyber :
une campagne pour augmenter le nombre d'experts cyber

Comme beaucoup d'entités, les ESRI pâtissent du manque de compétences cyber disponibles sur le marché du travail. Une des explications réside dans une orientation des élèves insuffisante vers les filières menant à la cyber. Ainsi, la découverte des métiers de la cyber et la connaissance des cursus de formation (y compris de formation continue) possibles sont cruciales. **Demain Spécialiste Cyber** est une campagne nationale co-construite par l'ANSSI et son laboratoire d'innovation, le MENJ et le Campus Cyber, proposant des contenus clés en main mis à la disposition des entités : vidéos, affiches et visuels pour réseaux sociaux (Zoom sur la campagne | DemainSpécialisteCyber (demainspecialistecyber.fr))

Tous les établissements d'enseignement (secondaire, supérieur et de formation continue) sont invités à s'en faire le relai !

vue d'ensemble

auteure
Florence Sèdes,
Professeure en Informatique, UT3 Paul Sabatier, chercheure IRIT

Les femmes dans la cyber : questions de genre ?

Focus sur la place des femmes dans le monde du numérique, et force est de constater que le chemin est encore long.

La demande actuelle en termes de main d'œuvre et de postes à pourvoir est exponentielle et pourtant les femmes restent très minoritaires dans les effectifs des équipes de cybersécurité.

Les stéréotypes et biais liés aux domaines scientifiques et à la technologie sont désormais clairement identifiés et les constats sont posés : au-delà des classiques problèmes de plafond de verre, plancher collant et syndrome de l'imposteur, qui se vérifient dans tous les secteurs, la cybersécurité souffre de manque de (role-)models féminins et d'accompagnement des carrières. On constate avec effroi que 50 % des femmes quittent les carrières de la tech après 35 ans, faute de se sentir intégrées, les biais bien connus agissant sur les opportunités de promotion et de leadership, et les écarts de rémunérations persistant. Le vivier initial étant limité, le nombre d'étudiantes conditionnant le potentiel de techniciennes, ingénieures et docteures, le mécanisme du « tuyau percé » est en route.

Améliorer l'employabilité des femmes dans la cybersécurité, les attirer et surtout les garder implique de compenser les biais en leur défaveur, qui les empêchent d'entrer et de réussir dans ce domaine. Valoriser les études et cursus en STIM, encourager les filles à briguer des formations sélectives ou au contraire pratiques et professionnalisantes, fournir un environnement de travail équitable et favorable pour les femmes qui choisissent de poursuivre une carrière dans ce secteur, en compliance avec les critères de diversité et d'inclusion qui font la réussite des équipes : la défiance des femmes n'est pas une fatalité mais relève de responsabilités diverses, à divers niveaux.

En complément à propos de Florence Sedes
L'auteure de cet article est également bénévole active pour ces deux associations : CEFSYS (Le cercle des femmes de la CyberSécurité) et CyberEdu (voir article « CyberEdu, la sécurité du numérique passe par tous ! » (quelques pages en amont.)

On évoque volontiers la cybersécurité du côté des « gentilles » mais quelle est la place des femmes du côté obscur de la force, i.e. dans la cybercriminalité ?

La société de cybersécurité Trend Micro a mené en 2023 une enquête portant sur le *« genre dans la cybercriminalité »*. Aucune statistique fiable sur le nombre de femmes cybercriminelles n'existe ; cependant, selon la chercheuse Mayra Rosario Fuentes, l'anonymat imposé par ce milieu le rend plutôt ouvert : *« Le cybercrime est l'une des communautés en ligne les plus méritocratiques, où les personnes ne sont appréciées qu'en fonction de leurs compétences et de leur expérience – et non de leur sexe […] ».*

Les remarques sexistes existent toujours dans les forums cybercriminels mais se retrouvent surtout chez les criminels de faible niveau. Plus le forum est *« professionnel »*, moins les questions de genre sont prégnantes.

En utilisant un analyseur de texte, Trend Micro a estimé à 30% environ la proportion de femmes dans les participant.e.s des forums cybercriminels XSS (russophone) et Hackforums (anglophone). Mayra Rosario Fuentes estime toutefois la présence féminine dans le cybercrime très largement sous-évaluée, encore un effet d'invisibilisation des femmes.

On retrouve ici un biais classique : estimer qu'un cybercriminel est par défaut un homme, compromettant inévitablement une enquête criminelle. *« […]. Dans de nombreux cas, l'enquête et l'interrogatoire d'un suspect de sexe féminin requièrent un état d'esprit différent »*.

Afin de compenser ce biais, Mayra Rosario Fuentes préconise l'inclusivité, comme il est dorénavant de mise dans beaucoup de pratiques, comme le recrutement : utiliser des pronoms pluriels neutres (*« them »* ou *« they »*), plutôt que des pronoms masculins (*« he »*, *« his »* ou *« him »*) sans a priori de genre du suspect dans le traitement des affaires cybercriminelles.

L'OSINT (Open Source Intelligence) est lié à **l'ingénierie sociale** car les techniques de manipulation psychologique nécessitent de collecter des éléments personnels et conjoncturels, facilement élicitables depuis les réseaux sociaux par exemple. Ces techniques se basent sur la fouille de données non protégées, publiques, sans piratage ni activités illégales ou utilisation de données classifiées ou confidentielles. Il s'agit d'un moyen légal et éthique de recueillir des renseignements à partir de la grande quantité d'informations disponibles sur l'Internet et d'autres sources publiques, sites web accessibles au public, publications officielles et gouvernementales, données géo-spatiales, renseignement humain,... L'aspect technique et informatique n'est en effet qu'une étape dans une cyberattaque : ce qui rend l'intrusion possible, c'est la porte d'entrée laissée ouverte ou rendue facile à ouvrir par un humain. Aujourd'hui, on peut dire que **90 % des attaques sont liées à un facteur humain**. Les cybercriminels et cybercriminelles travaillent sur les biais et les neurosciences, identifiant les stéréotypes de comportement pour inciter à cliquer, par exemple en usant de mécanismes d'ingénierie sociale pour le fishing, vishing, harpooning....

Un troisième point de vue sur les femmes dans la cyber est celui de l'ingénierie sociale qui désigne des activités malveillantes réalisées par le biais d'interactions humaines, utilisant la manipulation psychologique pour amener les utilisateurs à commettre des erreurs de sécurité ou à divulguer des informations sensibles : là encore, les biais et stéréotypes font des femmes des cibles moins techniques donc moins sensibilisées à la sécurité, et « socialement » plus accessibles car dans des positions en interface avec l'extérieur.

« Retour sur.... »
N°08 – La place des femmes dans le numérique, mars 2020. Sorti à l'occasion de la journée internationale des droits des femmes le 8 Mars 2020, ce numéro de la collection numérique est titré « Femmes, numérique et ESR ». Co-écrit uniquement par des femmes, il proposait un état de situation sur le sujet, mettait en avant des femmes et des « femmes numériques » et proposait des solutions pour améliorer la situation. Un sujet toujours d'actualité, à lire ou relire → **ici**

témoignage

auteur
Harry Claisse, DSI à l'Université de technologie de Compiègne

A l'UTC, tous concernés par la Cyber

Les ressources humaines et matérielles sont mobilisées dans le cadre d'une posture de défense proactive et plurielle

La cybersécurité émerge aujourd'hui comme un défi majeur et inévitable pour les établissements d'enseignement supérieur. Quelle université ou école n'est pas actuellement préoccupée par la sécurité numérique ? C'est le spectre obscur qui hante toutes les directions des systèmes d'information. La sécurisation des infrastructures numériques dans l'enseignement supérieur ne constitue pas seulement une nécessité, mais un impératif, afin d'instaurer un environnement fiable pour les enseignants, chercheurs, administratifs et étudiants.

↘ UN ENVIRONNEMENT HÉTÉROGÈNE

Dans cet environnement hétérogène qu'est un campus universitaire, une diversité tant humaine que systémique cohabite. La perception de la sécurité numérique diffère profondément entre un étudiant et un chercheur, entre un informaticien et un philosophe. Ainsi, l'acculturation des individus à la cybersécurité dès leur entrée dans l'établissement est fondamentale, un sujet que nous aborderons ultérieurement.

Au niveau des systèmes, cohabitent sur un campus des machines ne relevant pas du même niveau de sécurité. Les mises à jour sécuritaires ne sont pas appliquées de manière homogène, elles sont souvent gérées par des personnes surchargées ou d'autres pour qui ce n'est pas la priorité principale. Certaines machines se trouvent même contraintes par des logiciels ou matériels spécifiques, incapables d'évoluer. Au fil des années, le nombre de machines personnelles connectées au réseau interne, notamment celles des étudiants, n'a cessé de croître, représentant ainsi des menaces potentielles. Heureusement, elles sont confinées dans des réseaux segmentés, pierres angulaires de la sécurité réseau. Le premier niveau de sécurité que nous pourrions imposer concerne l'accès à ces différentes machines.

↘ LA GESTION DES IDENTITÉS ET DES ACCÈS

Une gestion efficace des identités et des accès seraient essentiels pour limiter les risques d'intrusions. Les établissements devraient mettre en œuvre des systèmes d'authentification à deux facteurs et des contrôles d'accès stricts. Bien que ces pratiques connaissent une montée en puissance, elles ne sont pas encore universalisées ; la complexité de leur implémentation ou les entraves qu'elles peuvent poser à l'utilisateur constituent des freins non négligeables à leur accroissement.

Dans le cadre d'une uniformisation numérique à l'échelle du campus, les établissements devraient élaborer et mettre en œuvre une politique de sécurité informatique (PPSI) claire et rigoureuse. Le ministère encourage vivement à la production de cette PSSI. De nombreux établissements l'ont élaborée, il est primordial qu'elle soit suivie pas tous les utilisateurs du système d'information et régulièrement actualisée par le RSSI (Responsable de la Sécurité des Systèmes d'Information).

↘ LE RSSI UN MAILLON ESSENTIEL

Le RSSI représente un élément vital dans la sécurisation informatique d'un établissement. Chargé de superviser et de mettre en œuvre les mesures de sécurité, il assure une surveillance quotidienne du réseau et doit être en mesure de détecter toute activité suspecte. Son rôle, bien que phénoménal, est parfois sous-estimé par les instances dirigeantes. Il est aidé par le CERT Renater qui opère une supervision en amont très efficiente. Le haut niveau de compétence technique requis pour occuper le poste de RSSI en fait un profil rare sur le marché du travail. Les établissements d'enseignements supérieur ont beaucoup de difficultés à recruter ce type de profil comme beaucoup d'autres par ailleurs. Le RSSI est amené quelque fois à tester la résilience des utilisateurs face aux attaques des pirates, pour cela il doit organiser des campagnes de tests.

↘ DES CAMPAGNES DE TESTS

Des campagnes de tests, telles que celles de phishing, ont été lancées par de nombreuses universités pour évaluer la vulnérabilité humaine ainsi que les réactions. Les résultats, souvent surprenants, mettent en lumière le manque de vigilance des utilisateurs et soulignent l'impérieuse nécessité d'actions de sensibilisation, voire de formation.

↘ LA FORMATION ET SENSIBILISATION DES UTILISATEURS

Au cœur des enjeux de sécurité informatique, l'élément prépondérant demeure l'utilisateur lui-même. L'ouverture aux cyberattaques trouve souvent son origine dans la négligence ou par manque de vigilance de l'utilisateur. Le piratage de ses codes d'accès au système est très fréquent d'où la nécessité de campagnes de sensibilisation.

Face à cette réalité, les institutions doivent impérativement déployer des programmes de sensibilisation à la cybersécurité pour éduquer les membres de la communauté universitaire sur les bonnes pratiques en matière de sécurité informatique. Ces programmes peuvent prendre la forme de sessions de formation, d'ateliers interactifs et de campagnes de sensibilisation régulières. Au cœur de ces initiatives, la communication occupe une place cruciale, car elle permet de transmettre efficacement les messages de prévention et d'alerte.

↘ EN CONCLUSION

La quête d'une sécurité absolue est illusoire dans le monde du numérique. La responsabilité de protéger nos systèmes requiert une sensibilisation constante pour tous, indépendamment du statut ou du niveau d'expertise numérique de chacun. La mise en place d'une politique de sécurité dépend largement de l'engagement financier et humain de l'établissement. Cela se traduit par l'allocation de ressources humaines dédiées à la sécurité et à la formation, ainsi que par un investissement financier conséquent.

Il est impératif d'investir dans des systèmes de défense avancés et de maintenir une mise à jour régulière des logiciels pour préserver l'intégrité de nos infrastructures face aux assauts perpétuels des cyberattaques. En effet, seule une posture de défense proactive et constamment actualisée peut garantir une protection efficace contre les menaces numériques émergentes

témoignage

Aix*Marseille université
Socialement engagée

auteurs
Julien Valiente, Responsable de la Sécurité des Systèmes d'Information / RSSI, Aix Marseille Université et **Eric Berton**, Président Aix Marseille Université

Plus fort ensemble !

Une alliance efficace entre Gouvernance et RSSI est non seulement une nécessité, mais surtout une force

A l'université d'Aix-Marseille depuis 2023 la fonction de RSSI est directement rattachée au Président. C'est une première reconnaissance de l'importance de la cybersécurité pour l'Université. L'articulation RSSI-Gouvernance se fait au travers de deux types de comités : un Comité Stratégique et des Comités de Pilotage.

↘ LE COMITÉ STRATÉGIQUE : UN TÊTE-À-TÊTE STRATÉGIQUE ENTRE AQSSI ET RSSI

Courts et réguliers, ils réunissent le Président en sa qualité d'Autorité Qualifiée de la SSI, et le RSSI. Sont abordés les sujets sensibles comme la protection des données de la recherche, la conformité avec la réglementation, et certains points de vigilance tels que la maîtrise des risques stratégiques, la résilience des activités essentielles, etc. L'objectif est de rendre compte de la situation, susciter des arbitrages au travers d'outils tels que des SWOT[1], et recueillir les orientations stratégiques.

↘ LES COMITÉS DE PILOTAGE : UN PILOTAGE TRANSVERSAL DE LA CYBERSÉCURITÉ

Animés par le RSSI avec les membres de la Gouvernance, selon les sujets à traiter, leur fréquence peut varier. La plupart du temps le VP au numérique, le DPO, la DSI et le FSD sont présents. Nous associons à ces comités d'autres Vice-Présidents, membres de la Direction Générale des Services, et autres contributeurs concernés. C'est une façon efficace d'impliquer les parties prenantes et d'intégrer la sécurité dans les projets.

1 | Outil d'analyse des forces (Strengths), faiblesses (Weaknesses), opportunités (Opportunities) et menaces (Threats)

Ces comités traitent opérationnellement de la gestion de crises d'origine cyber, de la mise en conformité, la conduite du changement, le contrôle d'accès, les moyens et ressources alloués etc.

↘ LA SÉCURITÉ C'EST COMME LES FREINS SUR UNE VOITURE : ÇA SERT À ALLER VITE

Nous mesurons chaque jour un très grand nombre de tentatives d'attaques, internes et externes, ciblant des comptes utilisateur, les messageries, les sites internet, les environnements numériques de travail. Certaines sont d'ailleurs conduites par vagues, organisées et particulièrement violentes. Les équipes, aguerries, savent faire face.

Mais la cybersécurité ne doit pas être perçue comme une contrainte supplémentaire. Prise en compte en amont, elle permet d'éviter la perte d'efforts et de moyens sur des solutions inadaptées ou d'éventuelles crises causées par un niveau de sécurité insuffisant. Elle diminue donc les risques, notamment celui d'interruption brutale et possiblement durable de l'activité académique quotidienne. La sécurité idéale est imperceptible, elle offre un bac à sable sûr dans lequel chaque acteur peut exercer pleinement ses missions.

↘ LA CYBERSÉCURITÉ, UN VECTEUR D'ATTRACTIVITÉ

Au delà de la protection, la culture de la cybersécurité devient un atout d'attractivité d'une université consciente des enjeux et des dangers. Ainsi, la compétition internationale académique rend obligatoire le développement d'environnements numériques sûrs pour les enseignants-chercheurs, les étudiants, et les personnels administratifs, mais aussi sûrs pour tous leurs partenaires.

La cybersécurité est une opportunité de rayonnement et de mobilisation.

Une organisation mature en protection de l'information est résiliente, agile, suscite de la confiance et de l'attractivité. Dans une période où l'actualité regorge d'incidents numériques, il est rassurant d'œuvrer dans une organisation qui a pris la mesure de l'importance des données et de leur protection. C'est un atout pour des projets d'envergure, les relations avec des parties prenantes attentives et exigeantes.

A l'Université d'Aix-Marseille l'acculturation aux fondamentaux de l'hygiène numérique est inscrite dans un processus de sensibilisation générale. Des programmes d'enseignement spécialisés répondent également au besoin croissant de formation de jeunes talents aux métiers de la sécurité numérique.

L'adoption de pratiques vertueuses concoure à protéger les pratiques métier, à préparer les jeunes générations aux défis numériques à venir, et à faire rayonner un savoir-faire collectif, que sont des valeurs chères aux ESRI.

témoignage

auteur
Dominique Launay,
responsable de la sécurité des systèmes d'information Fonctionnaire de sécurité et de défense adjoint, INRIA

Image by Azam Ishaq from Pixabay

Cybersécurité dans un EPST et articulation avec les EPSCP

Qu'il s'agisse de relations humaines ou d'infrastructures, les réseaux sont incontournables. Mais la confiance, l'échange et la communication restent les pierres angulaires du dispositif.

Pour un observateur venant de l'industrie ou du tertiaire, l'environnement d'un EPST pourrait être vu comme un OVNI : les partenariats et équipes multi-tutelles sont non seulement omniprésents, mais ils sont aussi multiples et différents selon le site (Université locale, industriel régional, autre EPST).

Leur teneur est très variée car ces partenaires peuvent aussi bien être publics, qu'industriels, liés à la défense ou académiques. Et il est parfois difficile d'identifier la limite entre le SI de l'EPST et celui du partenaire en fonction du lieu d'hébergement des travaux et du matériel utilisé.

Ajoutons que nos chercheurs sont très stimulants et ont sans cesse de nouvelles idées de partenariats ou d'expérimentations avec des montages innovants qui nous demandent fréquemment de nous adapter. On pourrait donc imaginer que l'environnement est ingérable et qu'aucune information sensible ne peut y être traitée.

Pourtant, un certain nombre d'outils organisationnels, réglementaires et techniques, permettent d'implémenter des bonnes pratiques de gestion de la sécurité de l'information.

Tout d'abord, la réaction aux incidents a été pensée dès la création de notre réseau, RENATER, en le dotant d'un CERT (Computer emergency response team). Le ministère, d'abord à travers l'UREC (Unité réseau du CNRS) et le CRU (Comité réseau des université), puis via RENATER, a organisé dès 1994 le réseau de ce qu'on appelait alors les correspondants sécurité. Ce réseau permet toujours aujourd'hui la mise en relation des RSSI (responsable sécurité des systèmes d'information) entre eux et avec les FSSI (fonctionnaire de la sécurité du système d'information) du ministère. Ces derniers sont chargés de la mise en musique de la réglementation dans les établissements sous-tutelle du ministère.

Cette réglementation a évolué pour donner des moyens d'action et une légitimité à celles et ceux qui gèrent la sécurité organisationnelle et opérationnelle dans leurs établissements. La PPST (protection du potentiel scientifique et technique de la nation) a incité plusieurs EPST (Inria, CNRS, INRAE) à adopter une échelle de sensibilité commune, afin de bien distinguer et marquer l'information à protéger. La mise en œuvre repose sur deux piliers : le producteur d'une information décide du niveau de sa sensibilité, l'établissement décide des mesures de sécurité adaptées

Le RGS, puis le cadre de gouvernance de la sécurité numérique de l'État ont introduit l'homologation de sécurité, la qualification de produits adaptés aux besoins de sécurité, et la PSSIE. Enfin l'IGI1337 définit l'organisation de la gouvernance de la sécurité numérique. Nous avons donc des référentiels, une organisation et des responsabilités équivalents.

Il reste que les établissements pourraient être très vulnérables sans une harmonisation des pratiques entre partenaires académiques et une communication sans filtre entre RSSI d'établissements partenaires. En effet, les adhérences entre les SI des établissements peuvent transformer chacun d'entre eux en vecteur d'une attaque, la propageant à un autre établissement. Une attaque sur un EPST ou un EPSCP pourrait se propager d'un établissement à d'autres, notamment en exploitant le fait que nombre d'EPST sont présents sur tout le territoire, et ont des partenaires académiques multiples.

C'est pourquoi une coopération permanente entre EPST et EPSCP est nécessaire pour compléter la chaîne de traitement traditionnelle. Elle n'est malheureusement pas encore systématique. Les incidents des deux dernières années nous ont montré que les établissements victimes s'isolent souvent pour ne pas aggraver l'attaque, ce qui est normal et louable. Mais le volet communication est malheureusement sous-évalué, les dégâts étant souvent appris par la rumeur, si ce n'est la presse.

L'annonce immédiate aux partenaires avec partage des indicateurs de compromission permettrait à chacun d'adapter sa posture probablement plus efficacement.

témoignage

auteur
Guy Brand, responsable de la sécurité des systèmes d'information RSSI/CISO, Université de Strasbourg - CERT OSIRIS

Protéger les usages et données numériques

Zoom sur la stratégie de cybersécurité de l'Université de Strasbourg dans un monde à haut risque

Dans un contexte global où le niveau de risque cyber est élevé, l'Université de Strasbourg accorde une priorité importante à la protection de ses systèmes d'information. Nous disposons d'un pilotage de la stratégie globale de sécurité numérique au niveau de la vice-présidence et de la direction générale des services de l'établissement. Notre stratégie vise à identifier et étudier les risques afin de protéger les biens numériques à un niveau suffisant pour nous prémunir des attaques auxquelles nous sommes exposés. Elle accompagne le développement du numérique dans l'établissement et s'articule avec le schéma directeur du numérique. Tout récemment, une démarche opportuniste d'homologation a été ajoutée à cette stratégie. Cette dernière doit prendre en compte notre périmètre large et varié qu'il est parfois difficile de couvrir dans son intégralité.

Sur un plan opérationnel, l'un des fondamentaux de notre ligne de conduite est de conserver la maîtrise des données essentielles en évitant les fuites de patrimoine via les plates-formes des clouds publics. Nos politiques techniques de sécurité bénéficient d'une forte implication de la Direction du numérique et des informaticiens de proximité ou de laboratoire dans leurs périmètres respectifs. Nous avons encore une exposition importante sur l'Internet, et la réduction de cette exposition est un objectif fort. En parallèle nous développons nos capacités de détection et de réaction. Ces objectifs progressent via un réseau de correspondants cybersécurité (plus d'une centaine de participants) maillant l'ensemble des campus strasbourgeois. La coordination de la cybersécurité se fait à la fois entre les structures au sein de l'université de Strasbourg et avec certains partenaires du site.

L'Université de Strasbourg partage un réseau métropolitain avec 17 partenaires historiques. Pour nombre d'entre eux, nous partageons, sur le domaine cyber, les mêmes chaînes fonctionnelles, les mêmes interlocuteurs nationaux (CERT-RENATER, FSSI, COSSIM, ANSSI) et des problématiques très proches, par exemple la compromission des fournisseurs, les dénis de service ou la captation des données de recherche. Sur ce dernier point, nous partageons nos

informations et nos actions avec nos homologues du CNRS. Les PSSI du CNRS et de l'Université de Strasbourg sont en phase. Nos socles d'hygiène informatique et nos recommandations de meilleures pratiques sont communs. Ceci nous permet souvent, s'agissant de sécurité numérique, de « parler d'une seule et même voix » et de passer les mêmes consignes. En parallèle, nous disposons depuis 2011 d'une équipe de réponse à incident de sécurité, le CERT OSIRIS, composée de personnels issus du CNRS et de l'université. Cette équipe a une vision sur l'ensemble des incidents affectant un partenaire connecté sur le réseau métropolitain commun. Elle assure le suivi de ces incidents, qui restent traités au niveau de chaque établissement concerné et s'appuie sur un réseau de correspondants cybersécurité mutualisé entre les partenaires du site. Enfin, des actions de sensibilisation ou de formation sont mutualisées autant que faire se peut entre le CNRS et l'Université de Strasbourg. Cette mutualisation avec nos partenaires de site n'offre que des avantages significatifs en termes d'efficacité opérationnelle, de lisibilité et de cohérence de nos politiques de sécurité numérique.

Description du CERT OSIRIS:
https://cert-osiris.unistra.fr
Le CERT OSIRIS est un centre d'alerte et de réaction aux attaques informatiques (computer security incident response team ou CSIRT), destiné aux partenaires du réseau métropolitain Osiris.

témoignage

auteur
Jacques Hertzberg,
RMSI, Université de Pau et des Pays de l'Adour

L'homologation de sécurité RGS comme stratégie SécNum

A l'université de Pau et des Pays de l'Adour, la culture de l'évaluation du risque se développe à tous les niveaux de l'établissement

La gouvernance Cyber, l'implication des acteurs du Numérique et l'acculturation des métiers sont ainsi les ingrédients indispensables pour la réduction des risques :

• la gouvernance exprime sa stratégie et impulse le mouvement. Elle soutient les chantiers SécNum intégrés au schéma directeur du Numérique ;

• les acteurs du Numérique font les choix technologiques adaptés, augmentent leurs compétences en se confrontant aux audits techniques. Ils participent activement à la procédure d'homologation ;

• les métiers prennent conscience des risques Cyber liés à leur activité et expriment les besoins de sécurité. Ils donnent à l'analyse de risque toute sa dimension protectrice.

Cette présentation fait le point sur l'organisation et les outils de la SécNum à l'Université de Pau et des Pays de l'Adour.

Organisation de la sécurité du numérique (SécNum) à l'Université de Pau et des Pays de l'Adour

Lexique :
AH : autorité d'homologation
ANSSI : agence nationale de la sécurité des systèmes d'information
APOS : assistance au pilotage par les objectifs de sécurité
AQSSI : autorité qualifiée
COMOP : comité opérationnel
COPIL : comité de pilotage
DGS : directeur général des services
DN : direction du Numérique
EBIOS : Expression des besoins et identification des objectifs de sécurité
ISP : intégration de la SécNum dans les projets
PASSI : prestataire d'audit de sécurité des systèmes d'information
RGS : référentiel général de sécurité
SécNum : sécurité du Numérique
Yogosha : défenseur (japonais)

Stratégie d'homologation et développement de la culture de la gestion des risques : Mon Service Sécurisé, la solution proposée par l'ANSSI pour faciliter le travail d'homologation

MonServiceSécurisé aide les entités publiques à sécuriser et homologuer rapidement leurs services publics numériques (site web, applications mobiles, API). Il est développé par l'ANSSI, en lien avec BetaGouv et la Direction interministérielle du numérique. Au-delà du service de conformité qu'il rend, ce service -gratuit- permet de faire collaborer toutes les parties prenantes (RSSI, DPO, DSI, directions métiers, chefs de projet, direction, etc.) et développe ainsi la culture de la gestion des risques cyber auprès des personnels participant à l'implémentation des SI.

En savoir plus : MonServiceSécurisé (ssi.gouv.fr)

témoignage

auteur
Michel Chabanne,
RSSI, CNRS

Une fédération Education-Recherche à confiance augmentée

Au cœur des failles les plus courantes, les accès et l'identité. Le projet NewConnect repense les essentiels avec un concept fondateur : la mutualisation.

La protection de nos données numériques repose depuis les origines de l'informatique sur le principe de la défense périmétrique. Depuis l'avènement du *cloud* sous toutes ses formes, la notion de périmètre est devenue floue, jusqu'à disparaître. Pour un attaquant, qui cherche comme nous à optimiser son retour sur investissement, quel est le meilleur vecteur à utiliser ? Tenter de percer une muraille consolidée et surveillée (même si elle peut avoir ses failles…) ou choisir une autre voie : obtenir puis abuser de l'identité d'un utilisateur légitime, si possible privilégié ?

Les incidents récents ayant conduit à des fuites des données ne laissent pas beaucoup de doutes sur les méthodes. Si l'exploitation de vulnérabilités[1] reste un sport de pratique courante (faille CitrixBleed touchant les serveurs Citrix, faille MOVEit touchant un logiciel de transfert de données, faille Cisco IOS XE, multiples failles Fortinet…), nombre de fuites de données ont eu pour origine **la compromission d'une identité** ayant permis l'intrusion dans le SI cible et la latéralisation de l'attaque par l'exploitation de failles. Cette identité peut appartenir à la structure visée, ou à l'un de ses fournisseurs (schéma d'attaque de type *supply chain*). Il peut s'agir d'une identité personnelle, ou d'un accès applicatif (de type *token*). Ces attaques visent le facteur humain, traditionnel maillon faible de la sécurité du SI, exploitant la crédulité, la maladresse de certains ou sont parfois si subtiles que des experts peuvent être dupés (« arnaque au président »). Elles utilisent encore des techniques anciennes mais toujours efficaces comme le *phishing*.

Dans notre communauté, sans stigmatiser certains établissements en particulier, les incidents à impact fort ont presque toujours eu pour origine la compromission d'identités numériques. Ceci nous alerte sur la **nécessité impérieuse de rendre plus robuste notre gestion des identités et des accès**, et également, remet sur le devant la scène les concepts de défense en profondeur et de maintien en conditions de sécurité des actifs, que nous n'aborderons pas ici.

↘ EVALUER OBJECTIVEMENT SA GESTION DES IDENTITÉS ET ACCÈS

Le NIST (*National Institute of Standards and Technology*) dans le guide « *800-63 Digital Identity Guidelines* »[2] qui en est à sa quatrième édition, introduit le concept de multiples **niveaux d'assurance** dans les identités (**LoA**), niveaux qu'il conseille de sélectionner en fonction d'une évaluation de risques des actifs associés à ces identités.

Ce LoA matérialise un niveau de **confiance** dans les identités numériques gérées par un fournisseur d'identité, **confiance qui doit être garantie sur l'ensemble des processus de gestion du cycle de vie, de contrôle a priori et de vérification a posteriori de ces identités**.

↘ S'ASSURER QUE JE SUIS BIEN CELUI QUE JE PRÉTENDS ÊTRE LORS DE MON ENRÔLEMENT ET PENDANT TOUTE MA VIE NUMÉRIQUE DANS LE SI

De la création de l'identité numérique d'un demandeur dans le SI, jusqu'à sa destruction au départ définitif du porteur, il faut

1 | https://www.cert.ssi.gouv.fr/alerte/

2| https://www.nist.gov/identity-access-management/nist-special-publication-800-63-digital-identity-guidelines

s'assurer que ces personnes physiques détiennent une identité prouvable à tout moment pendant toutes les phases du cycle de vie de cette identité.

Le processus de preuve et de vérification des preuves d'identité peut alors débuter. Il s'agit de collecter des données identifiantes et des preuves d'identité. La qualité, la quantité de données et le type de preuves fournies sont par essence variables. En fonction des choix de collecte, le **niveau de confiance résultant sera lui aussi variable**. Ce niveau de confiance est appelé ***Identity Assurance Level*** (**IAL**).

↘ S'ASSURER QUE JE SUIS BIEN CELUI QUE JE PRÉTENDS ÊTRE LORS DE L'ACCÈS AUX RESSOURCES (IDENTIFICATION ET AUTHENTIFICATION)

Une fois l'identité numérique créée dans un référentiel, elle est disponible au travers d'un fournisseur d'identités. Le porteur de cette identité se voit alors remettre un ou des *facteurs d'authentification* (le plus ancien et le plus classique : son mot de passe). Ces facteurs vont lui permettre de prouver son identité lors de ses accès au SI. Ici aussi, la qualité et la quantité de ces facteurs peut varier. Aujourd'hui, l'authentification à simple facteur (souvent le mot de passe) reste un standard *de facto*, mais les risques associés à son usage sont légion : perte, vol, divulgation, manque de robustesse… Certains de ces risques peuvent être mitigés par le recours à une authentification multi-facteurs (MFA) : associer (ou remplacer) le mot de passe par un ou plusieurs autre(s) secret(s), physique ou virtuel, que je détiens.

Le choix de ces facteurs, leur nombre, leur robustesse, leurs modalités de gestion permettent de définir un niveau de confiance appelé ***Authentication Assurance Level*** (**AAL**).

↘ NIVEAU D'ASSURANCE DANS L'IDENTITÉ NUMÉRIQUE (LOA)

L'Union Européenne s'est inspirée des travaux du NIST[3] dans la conception du règlement eIDAS[4], notamment dans la rédaction de son article 8. Le bloc de services « eID » impose la publication d'un LoA pour qu'un service d'identité soit conforme.

Trois niveaux d'assurance sont établis par le règlement :

→ **Niveau « Bas » (*Low*) :** la création d'une identité numérique ne nécessite pas de vérification de concordance avec l'identité physique du titulaire (IAL faible) et la vérification de l'identité peut reposer sur un simple facteur (AAL faible) ;

→ **Niveau « Substantiel » (*Substantial*) :** la création d'une identité numérique nécessite une vérification de concordance avec l'identité physique du titulaire (IAL substantiel), et l'authentification est elle-même renforcée (AAL substantiel) ;

→ **Niveau « Elevé » (*High*) :** la création de l'identité numérique est réalisée en face à face avec vérification fiable de pièces d'identité et l'authentification est « forte » (IAL et AAL élevés).

Des exemples opérationnels de conformité à ces niveaux sont détaillés dans le document « *eIDAS LoA guidance* »[5] qu'il est conseillé de lire.

↘ DES IDENTITÉS PLUS ROBUSTES DANS L'ESR : UN EFFORT COLLECTIF POUR UN BÉNÉFICE COLLECTIF

Lorsque chacun se sera auto-évalué sur la base des critères définis supra, et aura pu mesurer son niveau de confiance – et donc de maturité – dans la gestion de ses identités, il mesurera les efforts qu'il reste à faire pour atteindre le niveau supérieur.

L'ambition du projet « NewConnect » est de définir les niveaux de confiance devant être atteints en fonction des enjeux de sécurité, pour augmenter la confiance globale dans les identités de l'ESR, et d'aider les établissements à les atteindre en concevant des démarches opérationnelles de progrès.

Cette hausse de confiance globale doit nous amener à progresser dans les deux composantes du niveau de LoA : IAL et AAL. Il est inutile de cantonner la réflexion et le projet à un simple renforcement de l'AAL si les identités gérées restent peu fiables. Réciproquement, rien ne sert de gérer parfaitement l'enrôlement des personnels si leur manière de s'authentifier reste aussi fragile qu'aujourd'hui.

Il s'agit d'une refondation des concepts et des engagements qui sous-tendent la fédération Education Recherche telle que nous la connaissons, et opérée avec constance et efficacité par Renater depuis plus de 20 ans.

3 | https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL eIDAS+Levels+of+Assurance

4 | https://eur-lex.europa.eu/legal-content/EN TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

5 | https://ec.europa.eu/digital-building-blocks/wikis/download/attachments/40044784/Guidance%20on%20Levels%20of%20Assurance.docx?version=1&modificationDate=1488295895839&api=v2

Depuis mi 2023, un groupe de travail s'est constitué sous la tutelle de la DGRI avec des représentants d'EPSCP, EPST, de l'AMUE et de Renater, qui mène deux chantiers :

→ **Premier chantier** : Renforcement de l'authentification des utilisateurs

• WP n°1 : Recueil des besoins et définition des cibles technologiques MFA

• WP n°2 : Modalités d'implémentation locale dans un établissement

• WP n°3 : Opportunité et modalités d'une offre centralisée « MFA as a service »

→ **Second chantier** : Fiabilisation des identités et des (méta)données associées de nos fournisseurs d'identité

• WP n°3 : Définition des contraintes minimales à satisfaire

• WP n°5 : Feuille de route de mise à niveau d'un FI d'établissement vers le(s) niveau(x) d'IAL souhaités

Ces travaux s'inscrivent dans le respect des dispositions du règlement eIDAS, en tenant compte des pratiques existantes dans notre communauté française mais aussi européenne. De la même manière, la nécessaire interopérabilité d'une fédération ESR rénovée au plan sécurité avec les fédérations étatiques comme FranceConnect/AgentConnect est une nécessité.

Enfin, le groupe a toujours à l'esprit la définition de cibles atteignables dans notre contexte, la nécessaire adhésion des utilisateurs (commodité d'usage, compréhension des enjeux) et l'indispensable évangélisation puis le parangonnage du management de nos établissements.

L'urgence de ces travaux apparaît plus critique que jamais. **Par la fédération de nos identités, la faiblesse d'un seul met en danger l'ensemble de la communauté**. De plus, un nombre croissant de ressources scientifiques (calculateurs HPC…) nécessitent aujourd'hui la publication d'un LoA – voire un niveau minimal à atteindre ! – pour autoriser l'accès à un utilisateur. Il est grand temps d'unir nos actions.

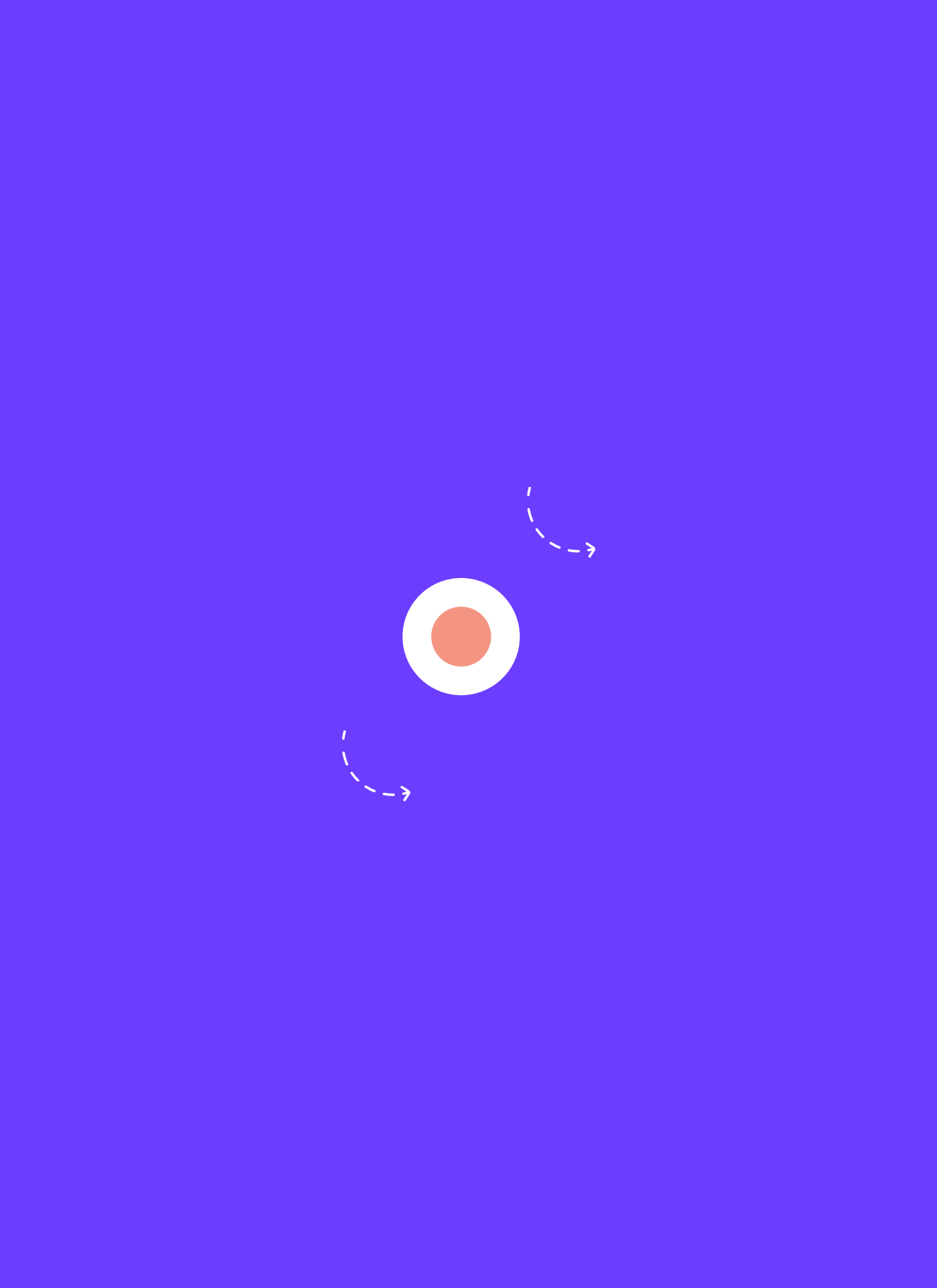
Déployons New Connect

L'Amue va se charger du déploiement de NewConnect, opération confiée par la DGRI/MESRI.

Aussi, nous renforçons nos équipes avec un 1er poste de « référent.e gestion des identités numériques » dont une des missions est de piloter l'accompagnement pour le déploiement de NewConnect, en lien avec les associations professionnelles, le ministère, la dinum et l'ANSSI.

Relayez ou candidatez à ce poste pour un projet nationale et d'importance pour la sécurité de nos établissements

amue
MUTUALISATION + SOLUTIONS



témoignage

auteur·e·s
Brigitte Sor, Directrice DSIN, INP Toulouse
Baptiste Robert, diplômé de l'INP-ENSEEIHT, hacker éthique, chercheur en cybersécurité et président de la société Predicta Lab

La résilience s'applique aussi au cyber

Retour sur l'attaque dont a été victime l'INPT et les actions qui s'en sont suivies

Dans le sillage d'une cyberattaque d'envergure de type ransomware (cybergang AvosLocker) qui a paralysé notre établissement Toulouse INP dans la nuit du 11 au 12 Septembre 2022, la maxime **"Ce qui ne tue pas rend plus fort"** prend tout son sens.

Face à cette crise, l'établissement est confronté à des défis complexes, allant de la restauration des systèmes informatiques et la révision de leurs usages à la préservation de la confidentialité des données sensibles. Par chance, dans notre cas, aucune donnée n'a pu être exfiltrée et nos sauvegardes n'ont pu être cryptées.

Cependant, au-delà des dommages immédiats, cette épreuve offre également une opportunité d'apprentissage et de renforcement. En effet, cette expérience douloureuse conduit à une prise de conscience accrue et mieux partagée des vulnérabilités potentielles et des lacunes dans les mesures de sécurité existantes. Elle incite à une réévaluation approfondie des pratiques de cybersécurité et à des investissements supplémentaires dans la prévention et la préparation aux attaques futures.

De plus, cette crise forge un esprit de résilience au sein de la communauté universitaire, renforçant la collaboration entre les acteurs internes et externes, ainsi que la sensibilisation à l'importance cruciale de la cybersécurité. Ainsi, bien que les conséquences d'une cyberattaque puissent être dévastatrices, elles peuvent également catalyser une transformation positive, faisant émerger une institution plus résiliente et mieux préparée à affronter les défis numériques de demain car

« Le pire est à venir » (la vision d'un pirate repenti et éthique, diplômé de l'INP-ENSEEIHT)

La (cyber) situation n'est pas bonne. Chaque jour, l'actualité est remplie de cas de sociétés victimes de cyberattaques. Grosses sociétés, PMEs, hôpitaux, établissements d'enseignement supérieur, personne n'est épargné. Et cela ne va pas s'arranger.

En effet, la multiplicité des services déployés, des appareils connectés sur les réseaux, et l'avènement du télétravail, augmentent de plus en plus la surface d'attaque des organisations, rendant ainsi la tâche des cyber défenseurs tous les jours un peu plus compliquée. Le besoin initial : déployer des nouveaux services, fait partie intégrante de la vie normale et

évolution de toute organisation. Le collaborateur doit pouvoir facilement déployer de nouveaux services. D'un autre côté, les responsables de la cybersécurité doivent s'assurer que les services soient déployés et configurés d'une manière sécurisée. Ils doivent ensuite veiller à son bon fonctionnement et mettre en place une veille en termes de sécurité sur le service en question. Malheureusement, faute de procédure adéquate, d'équipe dédiée ou même de volonté politique, la mise en place d'un nouveau service est rarement maitrisée faisant passer à la trappe des questions majeures telles que la souveraineté, la présence de vulnérabilité sur le service en question ou même le traitement des données par celle-ci.

Et le pire est encore à venir. L'arrivée de l'IA générative impose des challenges encore plus sophistiqués sur les organisations. Cette technologie, packagée dans des produits quasi exclusivement américains, faciles d'utilisation, et abordables voire même gratuits, rendent leurs adhésions dans le monde entier extrêmement rapide et non contrôlé. Exemple le plus illustrant, l'utilisation de ChatGPT au sein des sociétés du monde entier pose, notamment, des problèmes de confidentialité importante. Alors n'attendons pas.

La cybersécurité est une responsabilité collective. Il nous faut chaque jour et à tous les niveaux, sensibiliser sur ces questions afin de rendre la tâche des cyber attaquants plus compliqué.

Pour faire face à ces défis grandissants, il est crucial d'adopter une approche collective et proactive. Sensibiliser à la cybersécurité à tous les niveaux est essentiel pour rendre la vie plus difficile aux cybercriminels. Les établissements d'enseignement supérieur comme les entreprises doivent établir des procédures rigoureuses, former des équipes spécialisées pouvant être mutualisées pour répondre à la tension extrême du marché de l'emploi dans ce domaine, et investir dans des mesures de protection solides pour sécuriser systèmes et données.

La cybersécurité est une **responsabilité collective** qui requiert l'engagement et la collaboration de tous les acteurs concernés. C'est en sensibilisant, en éduquant et en prenant des **mesures proactives**, que nous renforçons notre capacité à faire face aux menaces numériques en constante évolution.

Vu aux assises du CSIESR :
Brigitte Sor co-auteure de cet article a partagé une présentation aux assises du CSIESR en mai dernier sur cette expérience . Intitulée « Retour sur l'attaque dont a été victime l'INPT », cette intervention peut être revue sur ce replay.

témoignage

UNIVERSITÉ DE LYON

ENS DE LYON

auteur·e·s
Viviane Delattre, DSI et **Nicolas Schmitz,** RSSI, Ecole Normale Supérieure de Lyon

Quand l'exercice devient projet

L'ENS Lyon a expérimenté le kit d'exercice à la gestion de crise d'origine cyber proposé par l'ANSSI

Fin 2022, face à la menace cyber grandissante, notre Direction a validé le lancement d'un projet « Gestion de crise ». Aux actions de fond que nous avons menées (voir encart), venait s'ajouter un point fondamental : organiser un exercice de crise pour mettre en musique ces éléments. Nous nous sommes donc portés volontaires à l'appel lancé par l'ANSSI pour tester le « kit d'exercice de gestion de crise dédié ESR ».

L'ANSSI nous a conseillé sur la composition finale de la cellule de crise, et nous a demandé de désigner un animateur de l'exercice. Cette fonction est clef car elle adapte le contenu du kit à l'établissement et est la seule à connaître le scénario avant qu'il ne soit joué !

Le jour J nous étions parvenus à mobiliser sur la demi-journée de l'exercice : vice-présidents, dircab, dircom, DPO et service juridique, DSI, RSSI et informaticiens de labo. Des profils informaticiens assuraient la rédaction des « points de situation » et de la main courante.

Pendant toute la demi-journée, l'animateur (assisté de deux personnes de l'ANSSI qui avaient fait le déplacement) nous envoyait des stimuli du type, « telle application ne fonctionne plus », « tel prestataire nous indique être victime d'une attaque par demande de rançon », « tel message a été publié sur les réseaux sociaux »… C'était donc intense (35 stimuli reçu en 2 heures 30), il fallait réagir en temps réel : assurer la communication interne/externe, prendre des mesures techniques, étudier les aspects réglementaires (RGPD, contrats..), gérer les demandes des VIP et des syndicats..

Pour aller plus loin :
Un exercice qui s'intègre dans un projet gestion de crise, comportant plusieurs volets :

- Composition cellule de crise : les rôles de chacun, les conditions de déclenchement…
- La stratégie de communication : messages types, canaux dédiés…
- Les outils pour l'équipe de crise : espaces collaboratifs, envoi de SMS en masse, recopie des documentations techniques… hébergés sur une plateforme externe décorrélée de notre SI.
- La cartographie avec les aspects sécurité : DICT, sauvegardes, logs, etc.
- La rédaction de fiches réflexes techniques
- La contractualisation avec un PRIS
- La sauvegarde déconnectée

Il s'agissait à chaque fois pour les experts de fournir très rapidement les clefs à la Direction pour qu'elle puisse prendre les bonnes décisions et ensuite solliciter les équipes techniques ou de communication pour leur mise en œuvre.

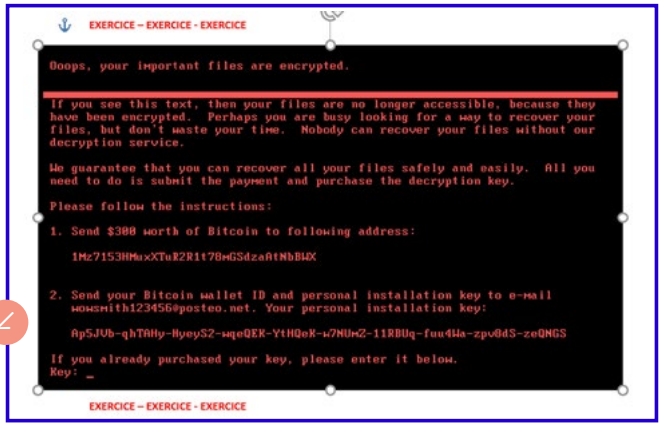
Le bilan est très positif : en premier lieu les 13 joueurs, issus de métiers très différents ont appris à travailler ensemble, et l'alchimie a fonctionné. Nous avons aussi pu apprécier l'importance des « points de situation », et de pouvoir compter sur la dircom. Plus globalement, cela nous a permis de valider le format de cette cellule de crise.

Le RETEX à froid organisé avec les participants, ainsi que le debrief de l'ANSSI, ont également permis d'identifier des axes d'amélioration : non praticité des échanges électroniques entre joueurs, format de la main courante à revoir, rôle des experts à affirmer, rôle des informaticiens de labo à ne pas négliger, etc. Ces axes font l'objet d'un plan d'actions suivi en interne.

Nous allons à présent organiser ce type d'exercice chaque année, dans une logique d'amélioration continue et pour maintenir le lien entre les participants. Après ce 1er exercice à un niveau stratégique, nous prévoyons pour 2024 un exercice plus opérationnel, avec une implication plus importante des équipes techniques.

A noter que le guide « Crise d'origine cyber – Les clés d'une gestion opérationnelle et stratégique », très structurant d'un point de vue méthodologique, nous a été très utile pour le projet et que l'ANSSI nous a beaucoup aidés dans l'organisation de l'exercice de crise : préparation, présence lors de l'exercice, et debrief post exercice … avec une approche structurante, facilitante et constructive

Nous sommes bien sûr à disposition des établissements de l'ESR pour un debrief plus détaillé sur cet exercice, ou plus globalement sur notre projet « gestion de crise ».



Exemple de stimuli
(stimuli n° 23 sur les 35 reçus en 2h30)

Retrouver les ressources de l'ANSSI pour faciliter l'organisation des exercices à la gestion de crise d'origine cyber :

Le guide dédié « Organiser un exercice de gestion de crise cyber »

L'outil d'autoévaluation de gestion de crise cyber

Le kit d'exercice avec le scénario dédié aux ESR

témoignage

L'accompagnement cyber, une priorité

Comment le CUME contribue pour la communauté, sur le sujet Cyber, retour sur les actions (webinaires, formations…) faites par l'association

auteur·e·s
Claude-Isabelle Roux, DSI du CROUS de Paris et présidente du CUME,
Mejdi Bouchlaghem, Responsable des Infrastructures de Sorbonne Université et Vice-président du CUME,
Thierry Oger, chargé de missions transitions écologique et numérique de l'université d'Angers et secrétaire du CUME

L'association professionnelle CUME (Comité des Usages Mutualisés du numérique pour l'Enseignement www.cume.fr) se veut une association qui a pour objectif la sensibilisation et la montée en compétences numériques de ses adhérents, c'est à dire les collègues des établissements de l'enseignement supérieur et la recherche. Dans un cadre financier contraint pour tous les établissements, le CUME réalise ses actions soit « gratuitement » pour ses adhérents, et ceci grâce à leurs cotisations, soit à un coût modique pour les stages.

Les actions phares du CUME sont les journées thématiques, les webinaires et les formations organisées et réalisées par les membres de l'ESR. Nous n'externalisons pas nos formations car nous laissons une large place durant leurs réalisations aux échanges entre collègues et souvent une ½ journée est réservée pour les réponses aux situations propres des collègues.

Ainsi, pour illustrer les propos, le stage Wifi et vulgarisation sur les réseaux, au-delà des éléments techniques, aborde les notions d'architecture de sécurité, d'authentification et de protocoles de sécurité comme le 802.1X/EAP TTLS pour le wifi et eduroam. Les architectures logiques et physiques qui sont souvent les premières briques de la sécurité sont présentées, avec certes de la vulgarisation, mais aussi en présentant la multitude de protocoles et d'applications ; d'où l'importance que ce soit un collègue de l'ESR, qui connait parfaitement l'environnement de nos établissements, qui réalise le stage.

L'année 2023 a permis d'organiser, en lien avec CyberEDU (*NDLR* : voir article «CyberEdu, la sécurité du numérique passe par tous ! ») , le 23 juin précisément, un webinaire cybersécurité, et, nous avions, en 2021, organisé un webinaire dédié sur la sécurité Active Directory. Le webinaire permet, en format court 45 minutes et 15 minutes de questions/réponses, de présenter un sujet sans contrainte de déplacement ni d'inscription. Il permet aux participants d'avoir une compréhension générale sur un sujet et les points d'entrée nécessaires pour approfondir le sujet traité. Dans ce contexte, le CUME fait appel à des spécialistes de l'ESR mais aussi des entreprises ou d'autres associations afin d'enrichir la présentation d'un sujet comme la sécurité. Nous sollicitons également les collègues sur des retours d'expériences via ce même format court.

Les journées thématiques sont privilégiées pour les échanges avec un format long, le plus souvent sur Paris. Une suite de présentations sur une journée permet d'offrir aux participants une vision claire d'un sujet. Elles sont centrées sur des sujets d'actualité, la sécurité sans être le cœur du sujet est traitée en filigrane.

Dès 2014, le CUME s'est intéressé à la sécurité, notamment lors de la journée « BYOD » du 9/10/2014, ou le 8/10/2015 sur « L'épreuve classante nationale (ECNi) et les examens sur tablette ». Ces deux journées ont permis notamment d'évoquer des architectures réseaux et logiciels pour sécuriser les flux.

Lors de la JT du 18/10/2017 « Les Examens et Certifications en ligne / à distance » nous avons abordé les aspects sur le règlement général sur la protection des données (RGPD).

Plus récemment le 22/11/2023, la journée thématique IA « Comment l'IA va-t-elle façonner notre environnement professionnel ? » pose la réflexion sur l'usage de l'IA mais également les notions de sécurité liées à cet usage.

L'association reste à l'écoute de ses adhérents et nous sommes tout disposés à accompagner ou à développer les idées de nos collègues de l'ESR. Nous pensons que l'année 2024 sera l'occasion de vous présenter de nouvelles idées, venez à notre rencontre aux prochaines manifestations CSIESR ou JRES.

recherche

auteur·e·s
Philippe Gaborit, Enseignant-Chercheur, Faculté des Sciences, Université de Limoges - Responsable du Master Cryptis en Informatique et **Cristina Onete**, Enseignante-Chercheuse, IUT du Limousin, Université de Limoges - Responsable du Département Informatique

Le tandem Formation / Recherche fait la preuve de l'excellence

À l'université de Limoges, on forme, on cherche, on cherche avant de former, on va plus loin, toujours, pour performer en matière de cyber

↘ FORMATION EN CYBERSÉCURITÉ/ CRYPTOGRAPHIE À L'UNIVERSITÉ DE LIMOGES

Le master CRYPTIS en cybersécurité de l'Université de Limoges remonte à 1986 (à l'époque DEA de Cryptographie), il a déjà formé plus de 1000 étudiants et est la plus ancienne formation universitaire de France sur la cryptographie et la cybersécurité. La formation se décline sous forme de 2 parcours: le parcours sécurité (qui permet d'obtenir un master en Informatique à destination d'étudiants avec une formation en informatique), et le parcours Mathématiques, Cryptographie, Codage, Arithmétique (qui permet d'obtenir un master en Mathématiques et applications à destination d'étudiants avec une formation en mathématiques). La formation s'appuie sur une très bonne équipe de recherche, très reconnue à l'international, ce qui garantit l'excellence des cours ainsi que sur un large réseau d'anciens élèves. Concrètement, les étudiants ont à choisir parmi un large éventail de cours dont une grande partie sous forme d'options sur des domaines variés en cryptographie et cybersécurité en passant par les applications sur la carte à puces. La pédagogie est très orientée sur la pratique de projets en groupe tout en restant très exigeante sur l'approche théorique. La formation accueille de l'ordre de 40 à 50 étudiants de M2 par an. Pour la deuxième année de M2, il y a un semestre de cours puis un semestre de stage en entreprise ou en laboratoire pour ceux qui souhaitent continuer en thèse. Le domaine de la cybersécurité étant un domaine très en tension, une grande majorité d'étudiants est embauchée directement suite au stage de M2 avec des salaires moyens en sortie de l'ordre de 41kE bruts par an. A noter qu'il existe une association étudiant très active, la TeamCryptis qui s'occupe de former et d'encourager les étudiants du master à participer à des challenges CTF (Capture The Flag). Enfin un des grands attrait de Limoges est le coût total des études moindre comparé à d'autres grandes villes.

↘ RECHERCHE

L'équipe de recherche CRYPTIS comporte une quinzaine de personnes s'organise en **5 thèmes principaux** qui interagissent entre eux:

1 → cryptographie et cryptographie post-quantique.

2 → mathématiques discrètes

3 → informatique quantique

4 → sécurité des protocoles et protection de la vie privée

5 → sécurité physique et des implémentations

L'équipe CRYPTIS est très reconnue au niveau international et publie dans les meilleures conférences internationales du domaine comme CRYPTO, EUROCRYPT, USENIX ou IEEE Security and Privacy et fait partie de trois programmes PEPR France 2030.L'équipe a également une bonne synergie avec l'écosystème socio-économique local (notamment NAQUIDIS en région Nouvelle Aquitaine), l'équipe co-porte une chaire d'excellence montée avec Limoges Métropole et la Fondation Partenariale de l'Université de Limoges, dont le sujet est : Cybersécurité, Vie Privée et Trust dans le domaine de la santé (CV-SAN-T).

• Cryptographie post-quantique: le but de la cryptographie post-quantique est de proposer des systèmes résistants à l'arrivée d'un ordinateur quantique, c'est une des spécialités de l'équipe avec notamment des systèmes basés sur la théorie des codes correcteurs en métrique de Hamming ou en métrique rang. L'équipe s'est particulièrement illustrée lors de la compétition internationale organisée sur le sujet par le NIST (l'institut des standards américain). L'équipe s'intéresse aussi à la protection physique de tels systèmes notamment aux attaques par canaux cachés.

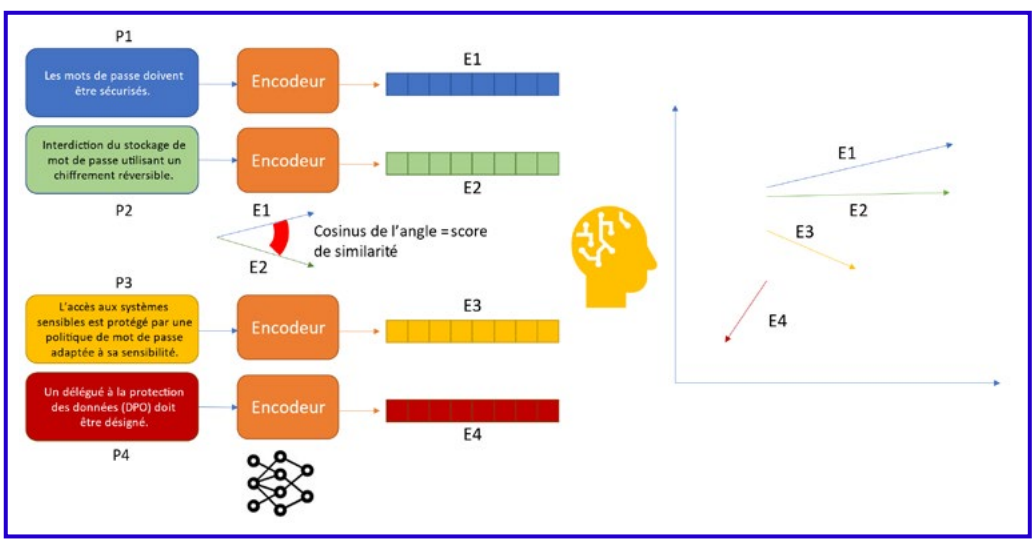
• Sécurité et protection de la vie privée : des protocoles cryptographiques potentiellement très complexes permettent aujourd'hui la communication et messagerie sécurisées, l'organisation des élections équitables à grande échelle, des transmissions entre des véhicules intelligents, les maisons et appareils intelligents et l'industrie 4.0. La sécurité prouvée des protocoles cryptographiques est une méthodologie moderne et très puissante, qui peut donner une preuve mathématique spécifiant sous quelles conditions un protocole est sécurisé ou, au contraire, pour démontrer qu'un certain protocole comporte des failles. L'équipe CRYPTIS a une expertise importante dans ce domaine et travaille sur des protocoles utilisés aujourd'hui : TLS 1.3, Signal, ou encore des protocoles utilisés dans le cadre des réseaux mobiles 5G.

recherche

auteur
Théophile Mandon,
Data scientist chez Acelys Services Numériques & doctorant avec le Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier (lirmm)

IA & cybersécurité

Reglys, l'outil de diagnostic sécurité enrichi avec l'IA, pour faciliter la conformité aux réglementations



↘ SAVOIR DÉMÊLER LA TECHNIQUE DU JURIDIQUE POUR ASSURER SA CYBERSÉCURITÉ

La sécurisation des systèmes d'information doit faire face à de nombreux défis. D'une part, il est nécessaire de mettre en place des solutions adaptées au contexte des entreprises et qui permettent notamment de résister à des attaques potentielles. D'autre part, ces systèmes doivent respecter les différents textes de lois existants (e.g. Le Règlement Général sur la Protection des Données personnelles - RGPD). Toutes les organisations, quelle que soit leur taille, doivent se conformer à ces exigences, ce qui représente une complexité relativement élevée pour les petites et moyennes entreprises qui disposent rarement à la fois de services informatiques et juridiques.

Les entreprises du secteur public sont, par exemple, régulièrement victimes d'attaques, malgré la mise en œuvre de solutions techniques de cybersécurité, en effet, ces solutions sont souvent mal adaptées au contexte métier de l'entreprise. Les PME sont également affectées par des attaques qui peuvent entraîner des interruptions d'activité de l'entreprise, malgré l'investissement dans des solutions techniques de sécurité coûteuses, si celles-ci ont été mises en place sans une réelle analyse des risques et de leur contexte.

Une solution automatisée permettant de mettre en évidence la bonne cohérence entre les exigences légales, réglementaires et normatives de l'organisation avec l'implémentation de mesures techniques, contribuerait à optimiser l'efficacité des mesures choisis et améliorer le niveau de sécurité réel. C'est l'objectif de la solution REGLYS proposée par Acelys Services Numériques, une ESN montpelliéraine indépendante qui mène des travaux dans ce sens en collaboration avec le LIRMM (Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier).

↘ CONFORMITÉ RÉGLEMENTAIRE ET REVUE D'IMPLÉMENTATION

La gouvernance et la cybersécurité des entreprises reposent sur des textes qui définissent les exigences ou les bonnes pratiques nécessaires pour assurer la sécurité des systèmes d'information. Ces réglementations établissent les exigences à respecter pour garantir la conformité et ainsi améliorer le niveau de cybersécurité et de gouvernance des données. Pour valider la conformité aux exigences, les experts en cybersécurité peuvent étudier les documents internes de l'organisation (Politiques de Sécurité des Systèmes d'Information-PSSI, chartes informatiques, etc…) afin de vérifier si l'organisation a décrit des mesures, une organisation ou des processus permettant de répondre aux exigences concernées. Cette activité, longue et fastidieuse, est connue sous le nom de revue d'implémentation de conformité. Un des objectifs de REGLYS est de semi-automatiser ce travail en utilisant une recherche automatique de passages similaires, suivie d'une classification permettant de déterminer si ces passages sont conformes ou non à l'exigence donnée. Les passages identifiés et les estimations de conformité devront, par la suite, être validés par un expert.

↘ L'INTELLIGENCE ARTIFICIELLE AU SERVICE DE LA REVUE D'IMPLÉMENTATION

Afin de mettre en lien les exigences avec les mesures décrites dans le corpus documentaire de l'entreprise, il est nécessaire de comparer ces textes. La sémantique et le style rédactionnel des réglementations peuvent être très différents de ceux utilisés dans les documents de l'entreprise, en effet, ces deux textes n'ont pas la même finalité et style varie d'un rédacteur à l'autre. De ce fait, nous utilisons une approche de type « plongements sémantiques de phrase » afin de pouvoir comparer le sens sémantique des phrases plutôt que le texte. Ces plongements représentent des phrases sous la forme de vecteurs de nombre réels. Cette représentation permet la comparaison, par exemple en calculant la similarité cosinus entre deux vecteurs.

Ces plongements sémantiques sont calculés grâce à des modèles d'intelligence artificielle entrainés et optimisés pour des bonnes performances en comparaison de textes. Ces modèles sont ensuite ré-entrainés sur un corpus de textes spécifiques à la cybersécurité et au vocabulaire juridique pour être mieux adaptés à l'utilisation dans le cadre de REGLYS.

Cette recherche augmentée par l'intelligence artificielle n'est pas la seule utilisation prévue de l'intelligence artificielle dans ce projet. Par exemple, il est aussi programmé d'utiliser de l'intelligence artificielle générative pour compléter et écrire automatiquement la documentation lorsque des modifications des mesures de sécurités sont envisagées et notées dans la revue d'implémentation. Il est aussi prévu d'utiliser l'apprentissage actif, une technique qui permet à l'utilisateur d'apprendre au modèle d'intelligence artificielle quasiment en temps réel pour permettre aux entreprises d'avoir des modèles d'intelligence artificielle plus performants et adaptés à leurs besoins.

recherche

auteur
Pôle Stratégie et Transformation Numérique, Amue

France 2030 soutient 17 projets pour la cybersécurité

Synthèse des lauréats !

Annoncée le 18 février 2021, la stratégie nationale d'accélération pour la cybersécurité a prévu d'allouer plus d'un milliard d'euros (dont 720 M€ de financements publics) afin de faire de la France une nation de rang mondial en cybersécurité.

D'ambition mondiale, cette stratégie s'articule autour de cinq axes :

→ **Développer des solutions souveraines** de cybersécurité ;

→ Renforcer **les liens et les synergies entre les acteurs** de la filière ;

→ Soutenir l'adoption de solutions cyber par les individus, les entreprises, les collectivités et l'Etat, notamment via **des actions de sensibilisation** tout en faisant la promotion des offres nationales ;

→ **Former plus de jeunes et professionnels aux métiers** de la cybersécurité, fortement en déséquilibre ;

→ **Soutenir en fonds propres** le développement des entreprises.

En octobre 2022, Jean-Noël Barrot, ministre délégué chargé de la Transition numérique et des Télécommunications présentait les 17 projets soutenus pour la stratégie nationale d'accélération pour la cybersécurité de France 2030.

Cet ensemble de projets est doté de 39 millions d'euros par France Relance. Ils visent, selon le ministre à :

→ Développer des solutions innovantes en cybersécurité ;

→ Renforcer les dynamiques collaboratives entre les acteurs de l'écosystème ;

→ Accroitre l'offre de formation.

Coordonné nationalement par Florent Kirchner, ce dispositif sera mené en lien avec Campus cyber (voir encart ci-contre) et fait partie de stratégie nationale d'accélération pour la cybersécurité de France 2030.

Plusieurs domaines sont couverts tels que le développement de technologies innovantes et critiques en cybersécurité, la mutualisation et valorisation des données d'intérêt Cyber et les compétences et métiers d'avenir.

Dans le domaine de l'Enseignement Supérieur et Recherche notons les projets de l'université de Montpellier, INSA Centre Val de Loire, Institut Mines-Télécom et Université Grenoble Alpes. Ces projets couvrent des sujets de formation, d'acculturation, de ressources pédagogiques et d'offre de formation.

Félicitations aux lauréats.

Pour aller plus loin :
Cet article synthétise les informations présentées sur cette page d'actualité → **ici**
La présentation rapide des 17 projets est à lire sur ce communiqué de presse → **ici**

Pour aller plus loin :
Campus Cyber est le lieu totem de la cybersécurité. Il vise à réunir les acteurs de la sécurité numérique pour protéger la société et faire rayonner l'excellence française du domaine. Cet écosystème cyber est le levier pour accélérer la création d'une société numérique de confiance.
Le site de Campus Cyber à consulter → **ici**

CAMPUS CYBER

témoignage société

auteur
Silvère Ruellan, Chef du bureau santé et affaires sociales à l'ANSSI

Secteur santé : point de situation sur les attaques touchant les établissements

→ Quelles sont les principales faiblesses des établissements ?

Les établissements de santé ne sont pas épargnés par la cybermenace. Le déploiement du numérique s'accélère dans tous leurs domaines d'activité (gestion administrative, urgences, imagerie, biologie, pharmacie, etc.), avec de multiples interconnexions avec des acteurs externes (patients, structures de ville, organismes d'enseignement et de recherche, fournisseurs de médicaments, prestataires informatiques, etc.), ce qui rend leur sécurisation particulièrement complexe.

A cela s'ajoute un historique de sous-investissement dans les infrastructures informatiques des établissements et dans leurs capacités de défense. Ce manque de moyens, couplé à une difficulté de recrutement de professionnels qualifiés, a conduit à la multiplication des brèches dans lesquelles s'engouffrent les attaquants, telles qu'une exposition sur Internet non maîtrisée, des annuaires vulnérables, des correctifs de sécurité non déployés, des méthodes d'authentification faibles, des sauvegardes mal protégées ou encore une supervision insuffisante.

Les dernières cyberattaques contre des établissements de grande taille ont servi d'électrochoc. L'ampleur de leurs conséquences ont donné lieu à une réelle prise de conscience des enjeux et à une forte mobilisation de l'écosystème. C'est dans ce contexte qu'a été lancé en 2023 le plan CaRE (Cybersécurité accélération et Résilience des Établissements). Piloté par le ministère de la Santé et l'Agence du Numérique en Santé, ce plan prévoit 750 M€ d'investissement d'ici 2027 pour mettre à niveau les systèmes d'information hospitaliers face à la menace et pour renforcer leur résilience.

Compte tenu de leurs écosystèmes « cousins », les secteurs de la santé et de l'ESRI partagent des enjeux similaires sur les questions numériques et les difficultés rencontrées au niveau cyber.

→ Observe-t-on une recrudescence des attaques contre les établissements de santé ces dernières années ?

Les établissements de santé ont une obligation de déclaration de leurs incidents de sécurité au CERT Santé prévue par le code de la santé publique. Ces déclarations donnent lieu à un rapport annuel. En 2022, le nombre total d'établissements ayant déclaré au moins un incident a augmenté de façon significative (+33 % par rapport à 2021). De manière générale, la menace se maintient à un niveau élevé, avec une industrialisation des capacités des attaquants.

→ Que sait-on des attaquants et de leur mode opératoire ?

La principale menace touchant les établissements de santé est d'origine criminelle. Elle est le fruit de groupes criminels qui opèrent dans le cyberespace. Ces groupes sont organisés comme de véritables entreprises, avec une répartition des rôles entre ceux qui fournissent l'infrastructure et les programmes malveillants, ceux qui les exploitent,

ceux qui commercialisent les données volées, etc. Leur motivation est l'argent et pour maximiser leurs gains, ils tendent à industrialiser leurs modes d'action. Aucun secteur n'est épargné.

Ces attaques se font en deux temps. L'attaquant trouve d'abord un moyen de s'infiltrer dans le système d'information de sa victime. Cela peut se faire en récupérant l'identifiant et le mot de passe d'utilisateurs légitimes par l'envoi de mails frauduleux (hameçonnage) ou encore via des virus spécialement conçus pour dérober ces informations sensibles (infostealers). L'attaquant peut même s'épargner cette étape en achetant directement une base d'identifiants et de mots de passe sur le dark web. Une autre façon de faire consiste à détecter une vulnérabilité sur un équipement de la victime accessible depuis Internet et à l'exploiter pour s'introduire dans le système d'information. De multiples outils permettent d'automatiser ces opérations.

Une fois l'attaquant entré, la seconde phase consiste à explorer le système d'information jusqu'à trouver quelque chose dont il va pouvoir tirer profit. Il peut s'agir d'obtenir des droits d'accès étendus sur le système d'information, lui permettant d'installer un rançongiciel qui va chiffrer les données de la victime (rendant son système inutilisable), le paiement d'une rançon étant exigé par l'attaquant en échange du déchiffrement des données. Les hôpitaux publics sont sujets aux attaques par rançongiciel quand bien même en France aucune rançon n'est jamais payée. Dans ce contexte, l'autre objectif visé par les attaquants est le vol de données personnelles, présentes en grande quantité dans les établissements de santé. Ces données sont ensuite mises en vente sur le dark web ou réutilisées pour commettre de nouvelles attaques.

Il est arrivé qu'un établissement de santé victime d'une attaque par rançongiciel soit finalement contacté par l'attaquant pour s'excuser (sic) et lui donner gratuitement la clé de déchiffrement, ce qui est une bonne illustration du caractère opportuniste de ce type d'attaque.

→ Vos conseils pour les établissements victimes ?

Les impacts d'une cyberattaque peuvent être découverts progressivement, avec des remontées d'information éparses, de la part du support utilisateurs ou des équipes techniques, et de la confusion avec des situations de panne « classiques ». La première étape consiste donc à bien qualifier l'incident à partir de ces informations. Dès l'incident de sécurité avéré, les décideurs doivent être informés, avec une synthèse de la situation et la proposition de premières actions de réponse à apporter et des impacts métier associés pour validation de leur part.

L'objectif est d'adopter rapidement des mesures de confinement pour empêcher la propagation de l'attaque. Cela passe par exemple par la déconnexion du réseau des machines compromises. Le cas échéant, il est recommandé de ne pas couper l'alimentation électrique de ces machines, de façon à préserver certaines traces de l'attaque qui pourront s'avérer utiles pour la suite des investigations. Dans les cas les plus graves, un établissement peut être amené à se déconnecter d'Internet, de manière à couper l'accès de l'attaquant au système d'information et aussi à éviter que l'infection ne se propage en dehors de l'établissement ; une décision lourde de conséquences au vu des nombreux acteurs qui interagissent avec un hôpital via Internet (patients, professionnels de ville, télé-experts, etc.).

Une autre priorité consiste à s'assurer de l'intégrité des sauvegardes, de façon à pouvoir restaurer les données perdues du fait de l'attaque.

Viennent ensuite les actions de remédiation, visant à rétablir le fonctionnement normal du système d'information, après s'être assuré que l'attaque a été éradiquée et que la sécurité a été suffisamment renforcée pour éviter qu'elle ne se reproduise. Ces actions peuvent s'étaler sur des jours, des semaines, voire des mois selon l'ampleur de l'incident – et coûter des millions d'euros.

Dès le début de l'incident, il est également important de respecter les obligations de déclaration d'incident vers les acteurs concernés (ANSSI, ANS, CNIL selon les cas). Il faut aussi déposer une plainte au commissariat ou à la gendarmerie la plus proche qui transmettra à un service enquêteur.

Dans le cas d'une attaque par rançongiciel, il est recommandé de ne jamais payer la rançon qui ne garantit en aucun cas la récupération des données et incite les cybercriminels à poursuivre leurs activités.

En savoir plus :

Les bons réflexes en cas d'intrusion sur un système d'information → **ici**

1 | https://www.cyberveille-sante.gouv.fr/lobservatoire-des-incidents#rapport-2022-1088

témoignage société

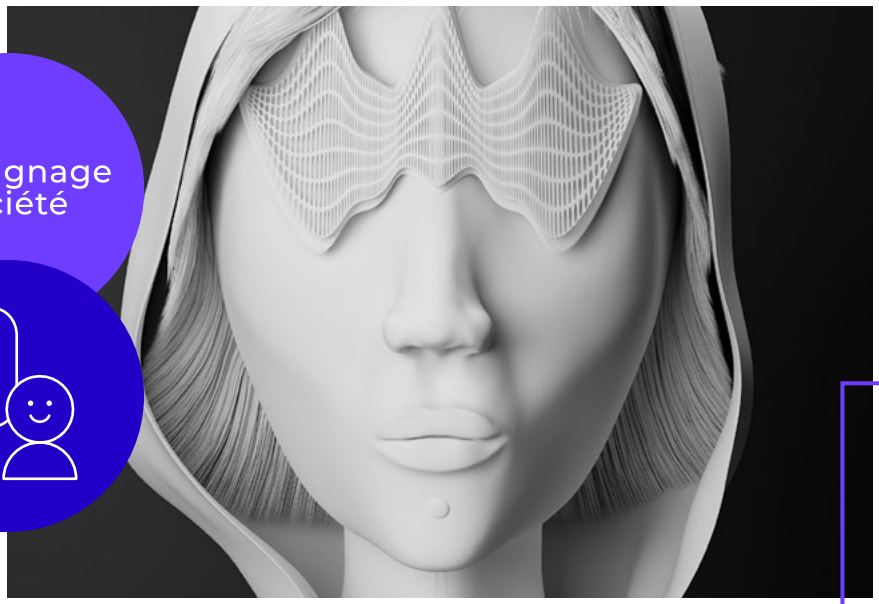


Photo de Hesam sur Unsplash

auteure
Delphine Chevallier, Présidente de l'ASSOVICA (Association de Soutien aux Victimes professionnelles de Cyberattaques)

Les femmes de la cyber : visibles ou invisibles ?

Dépassons encore une fois les statistiques et attachons-nous à mettre en lumière ces femmes, qui œuvrent à la sécurité au quotidien

Alors que l'histoire a longtemps masqué avec son manteau d'invisibilité les femmes pionnières de l'IT comme Grace Hopper l'inventrice du COBOL ou Joan Clarke, cryptanalyste, qu'en est-il dans le secteur émergent et en croissance rapide de la cybersécurité ?

L'ANSSI a dressé un profil très masculin du cyber expert type en 2021 : les professionnels de la cybersécurité sont à 89 % des hommes (source : résultat de l'enquête « les profils de la cybersécurité 2021 »). Cependant, des associations professionnelles comme le CEFCYS (Cercle des Femmes de la CyberSécurité) met en avant pas moins de 65 profils d'expertes cyber dans la dernière édition de son ouvrage « Je suis une femme et je travaille dans la cybersécurité ». Les femmes travaillant dans le secteur de la cyber seraient-elles donc condamnées à être une anomalie statistique ?

D'autant plus que du côté obscur de la cyber, on parle également toujours de hackeurs au masculin. Qui connait le nom de hackeuses ? Même si là encore, elles sont moins nombreuses que leurs homologues masculins, les femmes sont également de cette partie comme Maia Arson Crimew, Kristina Svechinskaya, Ying Cracker ou encore Xiao Tian.

Bref, surement moins nombreuses que leurs collègues masculins, les profils féminins existent bel et bien dans la cyber. Comme dans n'importe quel secteur en pénurie de talents, il serait stratégiquement contreproductif de se priver du gisement largement sous exploité de talents féminins.

Fille ou garçon, tous unis pour répondre aux enjeux de la cyber ! Polymorphes par nature, ces enjeux sont particulièrement complexes, reflets de la main mise grandissante des environnements digitaux sur nos vies personnelles et professionnelles. Et pour naviguer dans la complexité, la diversité est un facteur clé de succès.

Pour attirer les talents au féminin, continuons à

→ Déconstruire l'image d'Epinal du geek en sweat à capuches comme étant l'apanage du professionnel de la cyber,

→ Combattre la fausse croyance qui voudrait que les femmes soient moins naturellement attirées que les hommes pour les métiers dits 'techniques'

→ Promouvoir et mettre en avant à toutes occasions (conférences, tables rondes, présence dans les médias) les professionnelles de la cybersécurité, voire exigeons la présence d'au moins une d'entre elle lorsqu'il y a panel d'intervenants.

Pour aller plus loin :

L'auteure de cet article mène de nombreuses activités :

→ Dirigeante et fondatrice de Thalia NeoMedia, cabinet de conseil en cybersécurité
→ Présidente de l'ASSOVICA, Association de Soutien aux Victimes professionnelles de Cyberattaques
→ Référente cybersécurité TPE/PME
→ Experte en gestion de crise cyber
→ Editrice du magazine Kadna, Activer et manager la cybersécurité
→ Auteure, sous le nom de plume d'Angeline Vagabulle, de « Cyberattaque – Plongez au cœur du blackout ! », prix Cybersécurité du Forum InCyber 2023

L'association Assovica (Association de Soutien aux Victimes professionnelles de Cyberattaques) est un collectif composé d'experts techniques et non techniques qui visent à apporter de l'aide et du soutien aux victimes professionnelles des cyberattaques ciblant les organisations.
Toutes les informations sur le site de l'association →

« Retour sur.... »

N°08 – La place des femmes dans le numérique, mars 2020

Cet article fait écho au numéro au n°08 de la Collection Numérique. Sorti à l'occasion de la journée internationale des droits des femmes le 8 Mars 2020, cet opus de la collection numérique est titré « Femmes, numérique et ESR ». Co-écrit uniquement par des femmes, il proposait un état de situation sur le sujet, mettait en avant des femmes et des « femmes numériques » et proposait des solutions pour améliorer la situation. Un sujet toujours d'actualité, à lire ou relire → **ici**

témoignage société

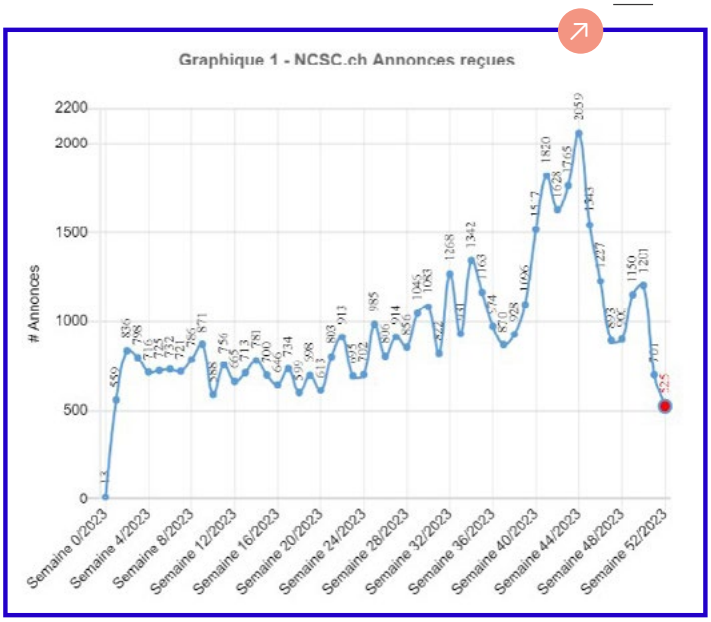
auteure
Alice Crelier, Chargée d'affaires politiques et internationales, Office fédéral de la cybersécurité suisse OFCS

Sensibiliser pour prévenir les attaques

On fait le point sur les chiffres actuels des cyberincidents signalés à l'Office fédéral de la cybersécurité (OFCS) par la population et les entreprises suisses

Le 1er janvier 2024, le Centre National pour la Cybersécurité (NCSC) est officiellement devenu un office fédéral intitulé Office fédéral de la cybersécurité (OFCS). Ce dernier est chargé de poursuivre les tâches principales jusqu'ici dévolues au NCSC, à savoir, être le premier interlocuteur des milieux économiques, de l'administration, des établissements d'enseignement et de la population pour toutes les questions portant sur cette thématique, assurer la mise en œuvre coordonnée de la Cyberstratégie Nationale (CSN) et rendre la Suisse plus sûre dans le cyberespace. Malgré ce renforcement institutionnel, la Suisse fait face, tout comme ses voisins, à des défis croissants en matière de cybersécurité, comme le reflètent les chiffres récents de l'OFCS concernant les signalements de cyberinicidents provenant de la population, des entreprises et des institutions suisses en 2023. Ces derniers mettent en exergue une hausse de 30 % par rapport à l'année précédente, soit du nombre total de signalements, atteignant près de 50 000 cas au 31 décembre 2023[1].

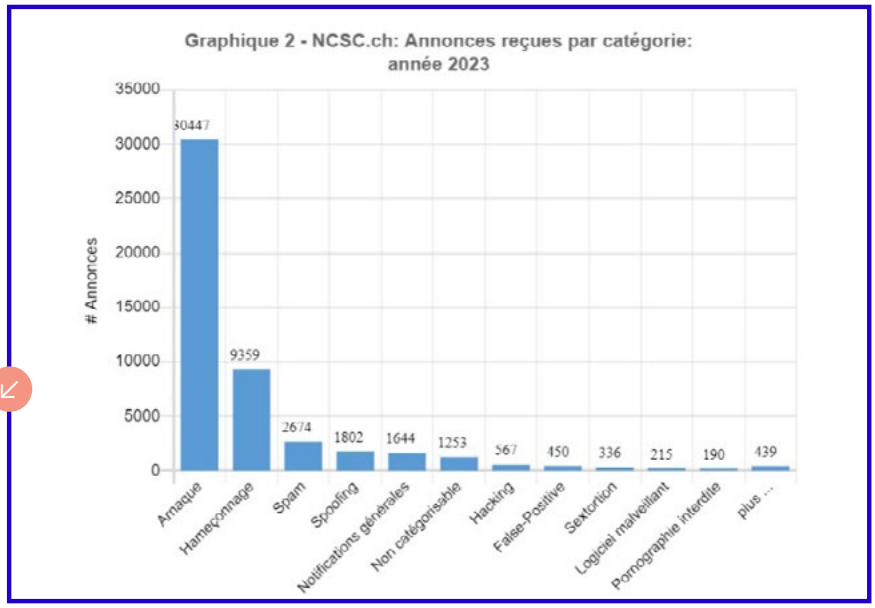
Source : OFCS



1 | Les chiffres proviennent des statistiques de l'OFCS basées, sur les cyberincidents signalés au cours de l'année 2023 par la population et les entreprises Suisses sur le territoire helvétique. Lien : Chiffres actuels (admin.ch)

↘ LES TENDANCES :

Les principales tendances comprennent une augmentation des fraudes liées à des offres d'emploi frauduleuses, des appels frauduleux au nom de la police, et une forte augmentation des arnaques au président et des fraudes à la facturation signalées par les entreprises.



https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/im-fokus/2023/wochenrueckblick_52.html#

→ Les attaques de déni de service distribué (DDoS) et les tentatives d'hameçonnage, notamment la technique de la "boule de neige", sont en augmentation. Les usurpations d'identité téléphoniques (spoofing) ont également doublé, atteignant près de 2000 cas, tandis que les attaques de rançongiciels contre les particuliers ont considérablement diminué.

→ En termes d'événements récents, plusieurs sites web de l'administration fédérale ont été temporairement inaccessibles en 2023 et en ce début 2024 en raison d'attaques DDoS revendiquées, pour des raisons politiques, par le groupe "NoName", proche de la Russie. Ces attaques visaient à attirer l'attention médiatique à des fins de diffusion idéologique, et n'ont pas entraîné de fuite de données. L'OFCS a anticipé ces menaces et mis en place des mesures de sécurité appropriées.

→ Les entreprises suisses font face à une menace croissante de piratage des données d'accès aux comptes de messagerie, en particulier les comptes Office365. Les attaques par rançongiciels contre les entreprises restent stables, mais maintenant presque toujours accompagnées d'une fuite de données, augmentant ainsi les dommages potentiels. Les attaques malveillantes de type "Lockbit" persistent, avec d'autres familles de rançongiciels signalées.

↘ RÉPONSES PROACTIVES ET MESURES D'ATTÉNUATION :

Le paysage de la cybersécurité est marqué par une diversification des attaques, avec une prédominance des fraudes ciblant les particuliers et les entreprises. Face à ces défis, la Suisse reste vigilante et apporte des réponses proactives permettant de renforcer sa résilience et sa cybersécurité, notamment au travers des programmes de sensibilisation et de soutien à la population, aux entreprises et à l'administration fédérale de l'OFCS pour se prémunir, faire face et atténuer les effets des cybermenaces et cyberincidents, tout en mettant en exergue l'importance des partenaires nationaux et internationaux.

retour sur...

auteur
Pôle Stratégie et Transformation Numérique, Amue

3 podcasts au Learning Planet Institute : L'université à l'ère de l'IA

Explorez l'impact de l'IA générative sur le monde universitaire en interrogeant ses implications pour la recherche, l'enseignement, l'éthique et la gouvernance. Voici le sujet traité par ces 3 podcast portés par le Learning Planet Institute.

Tout juste sortis, ces 3 temps d'écoute (environ 15' chaque) complètent la lecture du numéro N°30 - IA et Enseignement Supérieur : quels enjeux et impacts ? .

Ces podcasts portent sur 3 grands sujets : la recherche, la pédagogie et la gouvernance.

A écouter sur ce lien →

Les femmes à l'honneur dans la tech

Ada Lovelace a fait la 1ère page du numéro N°08 Femmes, numérique et ESR - Mars 2020 « Femmes, numérique et ESR" » car elle a été la première à produire un véritable programme informatique. C'était en 1842.

Quelques 66'000 jours plus tard, lancé en 2023, ce programme Tech pour toutes animé par la Fondation Inria, avec l'appui et l'expertise d'Inria et en partenariat étroit avec Femmes@Numérique, France Universités, la Conférence des directeurs des écoles françaises d'ingénieurs (Cdefi) et la Conférence des grandes écoles (CGE). Un programme qui vise à accompagner 10 000 jeunes femmes qui souhaitent commencer ou poursuivre des études supérieures dans le numérique.

Pour mémoire, seulement 23 % des emplois dans le numérique sont occupés par des femmes, un taux qui tombe à 15 % pour les métiers techniques (deux fois moins qu'il y a 30 ans). En 1842 100 % des développeurs étaient des développeuses.

Dinum & logiciel libre

Le Conseil national du numérique publie deux entretiens abordant le sujet des logiciels libres. Le sujet que vous pouvez lire ou relire dans le N°13 Vive le Numérique libre - Février 2021 « Vive le Numérique Libre !» de la collection numérique. Le 1er entretien donne la parole à Stéphanie Schaer, directrice de la direction interministérielle du numérique. Le second à Bastien Guerry, responsable de la mission logiciels libres et un des co-auteurs de ce numéro dédié au libre.

Le logiciel libre dans la stratégie de l'État. Entretien avec Stéphanie Schaer

Les logiciels libres comme espaces de collaboration. Échange avec Bastien Guerry

Une action pour soutenir les mainteneurs de logiciels libres critiques et fragiles : **4 prix de 10K€** récompensant le travail de mainteneurs de logiciels libres fortement utilisés dans l'administration, logiciels à la fois essentiels et peu soutenus. Pour tout savoir, une seule adresse → ici

grandes oreilles

auteur
Pôle Stratégie et Transformation Numérique, Amue

Au revoir, Au revoir, Sylvie…

Le moment est venu de dire au revoir à une collègue exceptionnelle, notre DirCom', Sylvie Barthel, une force motrice au sein de notre équipe de rédaction des Collections Numériques.

C'est avec une pointe de tristesse que nous bouclons ce (volumineux non ?) numéro avec toi, mais surtout avec une immense gratitude pour tous les numéros, que nous te souhaitons le meilleur pour cette nouvelle étape de ta vie professionnelle, après tes 18 années au service de l'Amue et de ses adhérents.

Depuis le tout début de l'aventure de la Collection Numérique, tu as été une des pierres angulaires de son succès. Ton implication sans faille, ta passion débordante et ta créativité infinie ont été les ingrédients magiques qui ont transformé cette idée en une réalité florissante.

Ton soutien et engagement indéfectibles dans le développement de cette collection, notamment le nouveau design, a été une source constante d'inspiration pour nous deux. Chaque édition bimestrielle a porté l'empreinte de ton dévouement, de ta vision et de ton amour pour le travail bien fait. Il fallait le dire aujourd'hui.

Nous ne pouvons passer sous silence ta remarquable capacité à améliorer continuellement le support, à l'enrichir, à nous faire découvrir les rouages de la bonne titraille et des percutants chapô. Ton esprit créatif, ta disponibilité sans failles, et ton œil aiguisé ont donné à la Collection une dimension qui va au-delà du simple bulletin d'informations. Tu as su lui insuffler une âme, celle que porte l'Amue, en faisant de chaque publication un rendez-vous incontournable pour notre communauté. Et toujours avec le sourire en plus.

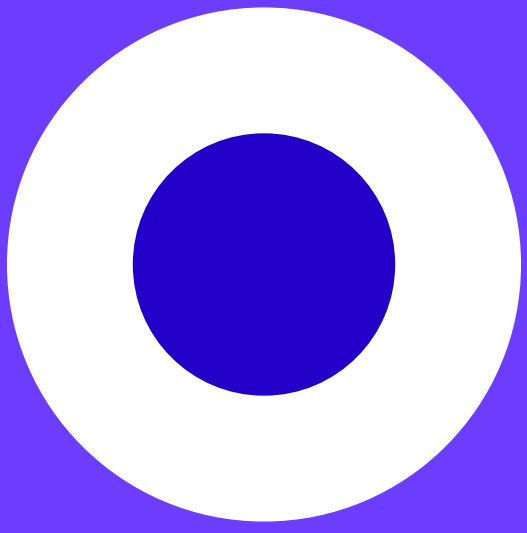
Ton professionnalisme exemplaire s'est manifesté à chaque étape du processus, toujours on time pour les relectures et les validations. Ton sens aigu du timing a assuré la qualité et la pertinence de chaque parution, faisant de la collection numérique une référence dans notre domaine.

Sylvie, tu nous quittes en laissant derrière toi un héritage indélébile. Ton travail passionné, ta détermination sans faille et ton dévouement total sont le reflet de ce que tu apportes dans chaque aspect de ta vie professionnelle. Nous sommes infiniment reconnaissants d'avoir partagé cette aventure avec toi.

Alors que tu t'apprêtes à ouvrir un nouveau chapitre de ta carrière, nous te souhaitons le succès, la satisfaction et la joie dans tout ce que tu entreprendras. Puisses-tu trouver autant d'épanouissement dans tes futurs projets que tu en as apporté à la Collection Numérique.

Merci pour tout, Sylvie.

Avec toute notre amitié,
Bertrand et David



février 2024

amue.fr

prochain numéro

Le numéro d'avril 2024 sera consacré aux stratégies du numérique universitaire.

À suivre dans les prochains numéros : formes de mutualisation dans d'autres pays, Usages saison 6

Ces sujets vous intéressent, vous avez une expérience, un point de vue à partager, vous avez une proposition de thème pour un prochain numéro : contactez l'équipe numérique de l'Amue qui est à votre écoute : numerique@amue.fr

2 rue Albert Einstein + 75013 Paris
Nos réseaux sociaux : @Amue_com