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

octobre 2021

Sécurité des Systèmes d'information

amue
MUTUALISATION + SOLUTIONS

#17

Sécurité des Systèmes d'information

Directeur général de la publication · Stéphane Athanase

Rédacteurs en chef · Bertrand Mocquet, David Rongeat et Philippe Bader

Secrétaire de rédaction · La com'

Graphisme & mise en page · @yay.graphisme

Photographie couverture · by Pete Linforth

ISSN 2650-8494

Ont collaboré comme auteur(e) à ce numéro · Bertrand Mocquet, Guy Mélançon, Vincent Toubiana, Michel Chabanne, Philippe Bader, Cédric Servaes, David Rongeat, Jérôme Notin, Héloïse Faivre, Victor Larger, Marion Lehmans, Guillaume Pourquié, Frantz Gourdet, Philippe Werle, Damien Sauveron, Isabelle Rigbourg

Remerciements spéciaux pour le réseautage · Philippe Bader, Cedric Servaes et Frantz Gourdet

Editeur · Amue · 103 boulevard Saint-Michel · 75005 Paris

Fabriqué en France

à télécharger !

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

prochain numéro de la collection numérique (Décembre 2021) :
Approche des organisations universitaires par le prisme de la donnée - Saison 2. Vos propositions de témoignage et retours d'expériences dès maintenant à numerique@amue.fr

Tous concernés par la sécurité numérique

↘ DES CIBLES FORT PROBABLES POUR LES PIRATES

Dans le monde entier, les universités et établissements sont des cibles « intéressantes » pour les pirates. Et pour cause, elles concentrent en un seul point, des données personnelles sensibles en nombre (les usagers comme les membres) mais aussi des données de recherche potentiellement stratégiques économiquement (brevet, jeu de données, ...) : il y a peu d'organisations publiques qui concentrent autant d'intérêt en termes de marchandisations des données collectées. Leur probabilité d'attaques est donc forte, et quotidiennement. Vivre un piratage, c'est souvent l'occasion d'améliorer les pratiques numériques de l'organisation, de repenser les mécanismes, non pas comme un échec, mais comme une mise en évidence de pistes d'amélioration.

↘ DES VULNÉRABILITÉS AU NIVEAU DU SYSTÈME D'INFORMATION

Comme vous le lirez dans la plupart des articles, les risques de vulnérabilité du Système d'Information (SI) ne sont pas uniquement liés à des technologies pas ou peu entretenues (accès au matériel ou mise à jour logiciel), ce sont aussi des pratiques et usages d'employés ou d'usagers qui permettent ce type d'intrusion illégale. Par inadvertance, par manque de formation ou par négligence, il peut arriver que l'une des portes du SI (login ; Mot de Passe) s'ouvre en un seul point du système d'information, par exemple l'ouverture d'une pièce jointe associée à un mail.

↘ UN IMPACT SUR L'ORGANISATION

On l'a vu dans le cas des Ransomwares, la perte des données produites par l'établissement, qu'elles soient scientifiques ou administratives, met l'activité de l'établissement dans une situation proche de la paralysie pour plusieurs jours voire semaines. C'est un sujet stratégique pour l'organisation que de mieux appréhender la sécurité numérique.

↘ LE RISQUE DE SÉCURITÉ NUMÉRIQUE ET SON TRAITEMENT

Probabilité, vulnérabilité et impact sont les trois composants d'un risque en sécurité du système d'information (SSI) (CNRS, 2014). Traiter comme un risque pour l'organisation devient un autre paradigme de résolution, celui de rendre robuste son organisation en évaluant le risque : c'est bien de la stratégie de l'établissement ou de l'université dont on parle.

Ce numéro propose de regarder ce risque droit dans les yeux, en faisant ainsi la part belle à la vulgarisation des termes employés, à des recommandations d'institutions mais aussi à des témoignages de praticiens luttant au quotidien pour éviter le pire ou réparer les destructions.

Au fait, c'est quand la dernière fois que vous avez changé vos mots de passe ?

Bonne lecture.

Bertrand Mocquet,
expert numérique, Amue

CNRS. (2014). Guide de Bonnes Pratiques pour les Administrateurs Systèmes et Réseaux. Repéré ici.
ISO/CEI 27002. (2021). Dans *Wikipédia*.
Nunès, P. E. (2021). Les universités, cible de choix des hackeurs. La Matinale du Monde. Repéré dans Europresse

vue d'ensemble

auteur
Guy Melançon,
vice-président
en charge
du numérique,
Université
de Bordeaux

La sécurité des SI vue depuis la vice-présidence en charge du numérique

Affaire de tous en établissement, la sécurité des SI requiert vigilance et organisation. A l'université de Bordeaux, c'est une priorité.

Nous avons tous en tête l'image d'un virus informatique qui vient perturber le bon fonctionnement d'une application neutralisant un processus financier ou d'une « attaque » bloquant le réseau de communication, par exemple. La notion de sécurité renvoie en effet spontanément à l'idée d'une menace externe qui empêcherait le bon fonctionnement d'un établissement.

Ce risque « cyber » doit être pris très au sérieux par nos établissements. Selon l'ANSSI (*Agence Nationale de la Sécurité des Systèmes d'Information*), la déstabilisation, l'espionnage, le sabotage voire la cybercriminalité constituent les principales menaces dont il faut se prémunir. L'ANSSI, connue des DSI et RSSI (*Responsable de la Sécurité des Systèmes d'Information*) des établissements, trace en quelque sorte le cap à suivre pour amener nos universités à conduire une réelle politique de sécurité et à déployer les moyens qui la garantissent[1].

Nous avons tous en tête l'image d'un virus informatique qui vient perturber le bon fonctionnement d'une application neutralisant un processus financier ou d'une « attaque » bloquant le réseau de communication

Cet impératif sécuritaire appelle le déploiement de moyens parfois importants, et une transformation de l'organisation de manière à accorder processus internes et sécurité. Au-delà des infrastructures et dispositifs sécuritaires se pose la question d'un positionnement politique propre à l'élaboration d'une politique de sécurité et à son opérationnalisation. La nécessaire priorisation de la mise en sécurité conduit naturellement à aborder la sécurité informatique par une évaluation du risque, qui amène fatalement à arbitrer sur nombre de questions.

Par conséquent, l'importance du sujet mérite éventuellement que les directions désignent un membre de leur équipe dont la fonction est garante de cet objectif stratégique. Les liens de la sécurité numérique avec la sécurité au sens large (du campus, des personnes), et avec celle de la protection des données personnelles méritent cette réflexion. Il peut être opportun et utile de nommer un vice-président ou un chargé de mission sécurité assurant le portage de la PSSI (Politiques de Sécurité des Systèmes d'Information) auprès des acteurs et communautés.

1 | https://www.ssi.gouv.fr/administration/bonnes-pratiques/

Une « organisation SSI » dans l'établissement reposera typiquement sur le RSSI, le FSD (*Fonctionnaire de Sécurité Défense*), l'AQSSI (*Autorité qualifiée pour la SSI) et le DPO (Délégué à la Protection des Données*) et fera intervenir des acteurs des différents niveaux structurels de l'établissement. Dans une telle organisation, en étroite relation avec le VP Numérique, le responsable politique sécurité SI mène une feuille de route conduisant à la construction de solutions et infrastructures fiables et sécurisés en adéquation avec les enjeux de l'établissement. Le choix de la bonne organisation implique de pouvoir clairement dessiner le champ du numérique dans l'établissement et les rôles des différents acteurs politiques dans cette arène.

La question de la sécurité n'est pas qu'une affaire reléguée aux spécialistes, elle doit être comprise, acceptée et intégrée dans les pratiques de tous les usagers

Pour nombre d'usagers, sécurité informatique rime souvent avec contraintes, alors que l'on doit y voir des mesures pour protéger nos libertés. Ce sont bien les libertés et droits fondamentaux des citoyens que vise à protéger le RGPD (Règlement Général sur la Protection des Données), alors qu'il peut être ressenti comme une limitation de la liberté académique. Ce constat souligne l'importance de sensibiliser nos communautés aux questions de sécurité, comme chacun l'est dans d'autres domaines : les notions de sécurité routière nous sont maintenant coutumières, et nos comportements de conducteurs se plient globalement aux exigences de sécurité.

Il en va de même avec la sécurité informatique : monde physique et monde numérique se fondent, l'usager navigue dans un univers informationnel où son identité numérique tend à supplanter son identité physique. Ainsi, le développement d'une pleine conscience et d'une maîtrise du risque cyber par les usagers, typiquement inscrite à la charte des usages du système d'information, doit être l'un des piliers de la politique de sécurité du système d'information.

Sur la trajectoire suivie par la plupart de nos établissements, la gouvernance par la donnée implique de pouvoir en garantir la fiabilité et la disponibilité, et est donc solidaire d'une politique de sécurité du SI. Cela pose par conséquent ses exigences en matière de sécurité à tous les niveaux évoqués ici :

- Sur nos infrastructures informatiques,
- Par une organisation portant les enjeux de sécurité du SI au niveau politique,
- Par une réelle adhésion de tous les usagers à une charte de bonnes pratiques.

Il appartient à notre communauté, et à chacun de nous, de garantir la qualité et la sécurité de notre environnement dont le numérique est une dimension constituante.

enjeux et stratégie

auteur
Vincent Toubiana, responsable du LINC (Laboratoire d'innovation numérique de la CNIL) à la CNIL Commission Nationale de l'Informatique et des Libertés

Protection des données personnelles, la CNIL vous accompagne

Passage en revue des actions concrètes proposées par la CNIL en termes d'analyse des risques

L'article 32 du Règlement Général sur la Protection des Données » (RGPD) précise que la protection des données personnelles nécessite de prendre des « mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ». Cet article fait implicitement référence à la gestion des risques qui permet de déterminer les précautions à prendre « au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données[1] » .

La gestion des risques permet ainsi une prise de décision objective et la détermination de mesures strictement nécessaires et adaptées au contexte. Il n'est cependant pas toujours simple de mettre en œuvre une telle démarche et de s'assurer que le minimum a bien été mis en œuvre.

Afin d'accompagner les acteurs qui souhaitent se mettre en conformité, la CNIL met à disposition plusieurs ressources :

→ Un outil « Privacy Impact Assesment » (PIA) qui peut être installé sur une machine ou déployé sur un serveur afin de vous guider dans l'analyse de risque. Cet outil permet un recensement détaillé des risques et mesures à mettre en place

→ Un guide en ligne listant les principales mesures de sécurité.

L'analyse de risque se découpe en quatre étapes :

Tout d'abord, dans **la première étape** il est nécessaire de recenser les traitements de données à caractère personnel, automatisés ou non, les données traitées et les supports sur lesquels elles reposent qu'il s'agisse des matériels (ex : serveurs, ordinateurs portables, disques durs), des logiciels (ex : système d'exploitation, logiciel métier), des canaux de communication (ex : fibre optique, Wi-Fi, Internet) ou des supports papier (ex : document imprimé, photocopie).

1 | Article 34 de la loi du 6 janvier 1978 modifiée, dite loi Informatique et Libertés

La seconde étape consiste à apprécier les risques engendrés par chaque traitement :

→1● Identifier les impacts potentiels sur les droits et libertés des personnes concernées en cas d'un événement redouté tel que :

a. accès illégitime à des données,

b. modification non désirée de données,

c. disparition de données,

→2● Identifier les sources de risques avec une vision assez large (attaquant externe ou interne, inondation, problème matériel)

→3● Identifier les menaces réalisables qui pourraient provoquer un des événements redoutés

→4● Déterminer les mesures existantes ou prévues qui permettent de traiter chaque risque

→5● En tenant compte des mesures mise en place, estimer la gravité et la vraisemblance des risques.

Afin d'aider les différents acteurs à adresser les risques, la CNIL propose un guide de la sécurité des données personnelles listant les mesures techniques et organisationnelles qui peuvent être mises en place.

La troisième étape consiste à mettre en œuvre les mesures jugées appropriées à la fin de l'étape 2 et à contrôler leur bonne application.

Enfin **la quatrième étape** consiste à réaliser des audits de sécurité périodiques. Chaque audit devrait donner lieu à un plan d'action.

Le laboratoire d'innovation numérique de la CNIL (LINC)

Au sein de la DTI (Direction des technologies et de l'innovation), LINC (Laboratoire d'Innovation Numérique de la CNIL) est un dispositif : **1/** de réflexion, d'information et de partage sur les tendances émergentes d'usage du numérique et des données ; **2/** de conduite de projets d'expérimentation et de prototypage d'outils, de services ou de concepts autour des données.

LINC Laboratoire d'Innovation Numérique de la CNIL

CNIL.

enjeux et stratégie

auteur
Récension du site web **par Bertrand Mocquet**, expert numérique Amue

Entrez dans l'univers ANSSI

Une occasion inespérée de découvrir la richesse des ressources et publications mises à disposition par l'ANSSI !

Créée par le décret n° 2009-834 du 7 juillet 2009, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) s'occupe « *de la sécurité des systèmes d'informations de l'État et une mission de conseil et de soutien aux administrations et aux opérateurs d'importance vitale ». Elle contribue aussi « à la sécurité de la société de l'information, notamment en participant à la recherche et au développement des technologies de sécurité et à leur promotion.* ».

La Loi de programmation militaire promulguée le 19 décembre 2013 a renforcé les missions de l'ANSSI : elle peut depuis cette date « imposer aux Opérateurs d'Importance Vitale (OIV) des mesures de sécurité et des contrôles de leurs systèmes d'information les plus critiques. ». La mission Recherche des universités et établissements est dans le périmètre du renforcement de cette mission, mais ce n'est pas la seule : morceaux choisis.

↘ PROTECTION DU POTENTIEL SCIENTIFIQUE ET TECHNIQUE DE LA NATION

Depuis avril 2018, l'ANSSI propose un guide méthodologique pour les chercheurs et ceux qui travaillent pour la recherche répondant aux « nombreuses vulnérabilités induites par une dépendance de plus en plus grande aux systèmes d'informations ». Cette « protection contre l'espionnage technologique est l'objectif premier du dispositif de protection du potentiel scientifique et technique de la nation (PPST) », et elle se doit d'être mise en œuvre par tous les opérateurs et acteurs de la recherche, notamment ceux qui travaillent dans les zones à régime restrictive (ZRR)

Vous pourrez y retrouver :

- Le contexte règlementaire pour les ZRR
- Un rappel des règles d'hygiènes informatiques indispensables
- Quelles mesures de sécurisation des systèmes d'information communes à toutes les zones à régime restrictif ?
- Quelles mesures de sécurisation particulières à chaque zone à régime restrictif ?
- Qu'est-ce que la politique de sécurité des systèmes d'information (PSSI) ?

↘ FORMATION AVEC LES UNIVERSITÉS COMME PARTENAIRE ET CIBLE

En parcourant le site web de l'institution, il est remarquable de constater les interactions entre l'ANSSI et les universités dans le domaine de la formation SSI.

Tout d'abord dans le cadre de la SecNumAcadémie, « la formation en ligne sur la sécurité informatique gratuite et ouverte à tous » prenant la forme d'un MOOC « pour vous initier à la cybersécurité, approfondir vos connaissances, et ainsi agir efficacement sur la protection de vos outils numériques ».

Mais aussi dans la labellisation de formation initiale en cybersécurité de l'enseignement supérieur, le label SecNumedu. Ce « programme de labellisation de formations initiales est ouvert à tout établissement d'enseignement supérieur répondant à un des critères ci-après :

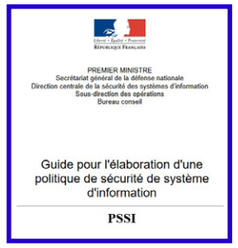
- Les formations universitaires délivrant un grade de Licence ou Master.
- Les formations d'ingénieur dont le diplôme est reconnu par la Commission des Titres d'Ingénieurs (CTI).
- Les Mastères spécialisés reconnus par la Conférence des Grandes Écoles (CGE).
- Les certifications de niveau I et II inscrites au Répertoire national des certifications professionnelles (RNCP).

Le processus de labellisation est géré par l'ANSSI qui tient à jour un répertoire des formations labellisées. »

Enfin, SecNumedu-FC, labellisation de formations continue en cybersécurité, dont « l'objectif de cette labellisation lancée à titre expérimental est de disposer d'une liste des formations continues en sécurité du numérique (formations courtes de quelques jours à quelques semaines) » qui répondent à une charte et des critères. »

Sécurité et Plan de Relance

La sécurité des SI, appelée ici cyber sécurité, a été retenue dans le plan de relance comme un sujet prioritaire. Un dispositif de France Relance doté de 136 Millions d'Euros confiés à l'ANSSI dont vous trouverez les détails ici ou dans ce communiqué de presse de juin 2021.



↘ UN SOUTIEN À LA POLITIQUE SSI (PSSI) DES ÉTABLISSEMENTS

Les universités et établissements étant opérateurs pour le MESRI d'une mission de service public, elles se doivent de suivre la PSSI de l'Etat. L'ANSSI fournit un outillage précieux pour la mise en place et le suivi de la PSSI, sous la forme d'un guide et des outils associés.

Le guide PSSI a pour objectif de fournir un support aux responsables SSI « pour élaborer une politique de sécurité du ou des systèmes d'information (PSSI) au sein de leur organisme ».

Il est décomposé en quatre sections :

- l'introduction, ce présent document, permet de situer la place de la PSSI dans le référentiel normatif de la SSI au sein de l'organisme et de préciser les bases de légitimité sur lesquelles elle s'appuie ;
- la méthodologie présente, de façon détaillée, la conduite de projet d'élaboration d'une PSSI, ainsi que des recommandations pour la construction des règles de sécurité ;
- le référentiel de principes de sécurité ;
- une liste de documents de références de la SSI (critères d'évaluation, textes législatifs, normes, codes d'éthiques, notes complémentaires…).

↘ ET EN CAS D'INCIDENT

Même si notre communauté n'aime pas trop en parler, plusieurs universités, établissements ou opérateurs de l'ESR ont subi une attaque plus ou moins paralysante durant ces 5 dernières années. L'ANSSI propose un certain nombre de services pour éluder la situation.

témoignage

auteur
Michel Chabanne,
RSSI, CNRS

SSI dans les unités de recherche publique - un état des lieux

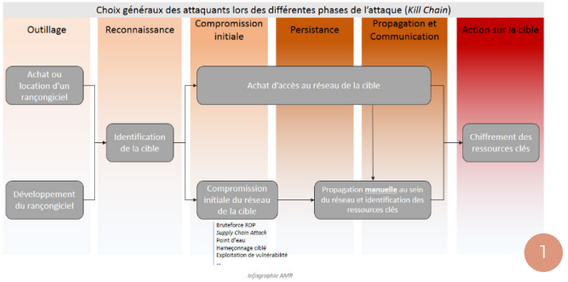
Il existe des parades aux attaques malveillantes, mais avant tout, il s'agit d'être tous acteurs, car tous concernés. On passe en revue les causes et les conséquences des menaces qui pèsent sur le cyberespace.

Le développement de la « société du savoir » est une réalité quotidienne depuis plusieurs années. La recherche publique doit faire face aux grands enjeux sociétaux que sont l'énergie durable, la conservation de notre environnement, le traitement et la valorisation de l'information numérique, et bien évidemment la santé publique dont la crise du COVID nous a rappelé la prépondérance. Il n'est plus de savoir qui ne prenne une forme numérique, dans toutes les sciences. L'interdisciplinarité densifie encore les échanges d'informations, encouragés par la dynamique « open science ». Corollairement, le monde multipolaire aujourd'hui est aussi ultra compétitif et source de menaces toujours plus nombreuses pour nos unités et nos chercheurs.

1 | Les phases d'une attaque de type rançongiciel

2 | Nombre d'incidents de type rançongiciels traités par l'ANSSI en 2019

QUELS RISQUES POUR LES UNITÉS ?



1

Depuis le début des années 2010, l'État a pris conscience de la nécessité de revoir sa posture de maîtrise des risques pour la recherche. Historiquement, la protection du secret de la **défense nationale**, qu'il s'agisse d'armement conventionnel ou nucléaire, représentait le premier enjeu. **Si cet aspect reste important**, trois autres dimensions de risques ont été identifiées comme pesant sur l'activité des unités :

→ l'**atteinte aux intérêts économiques** de la nation, visant la capacité à valoriser la recherche ;

→ la **prolifération des armes de destruction massive** (nucléaire, radiologique, biologique et chimique) et de leurs vecteurs :

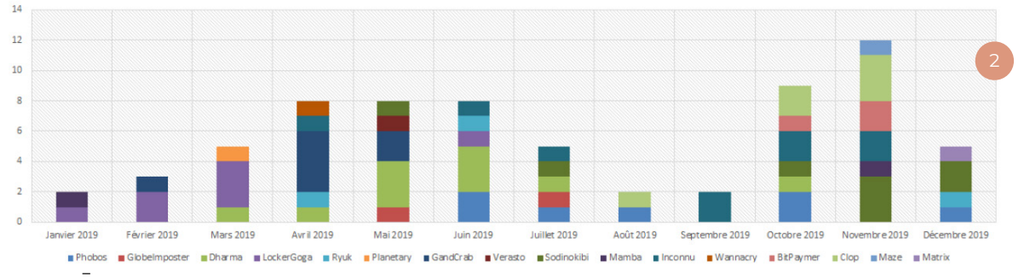
→ le **terrorisme**, autant dirigé contre les unités que dans le détournement de leurs activités et leurs savoirs et savoir-faire à cette fin.

Il semble naturel de dire que le risque d'intelligence économique existe dans la majorité des activités de recherche. Si les autres risques peuvent paraître plus éloignés du quotidien, il est par exemple utile d'évoquer l'existence dans les unités de biens « à double usage » (équipements et savoir-faire susceptibles d'avoir une utilisation tant civile que militaire ou pouvant contribuer au développement, à la production, au maniement, au fonctionnement, à l'entretien, au stockage, à la détection, à l'identification, à la dissémination d'armes de destruction massive) dont le risque induit est moins évident et doit pourtant être considéré.

QUELLES MENACES ?

Elles sont toujours plus diverses et plus avancées, en particulier quand on s'intéresse au support le plus courant des données à protéger : les systèmes d'information des unités. Il est loin le temps où de jeunes pirates plus ou moins conscients des conséquences de leurs actes s'introduisaient dans des SI par jeu ou par goût du défi. Aujourd'hui, des groupes organisés liés aux organisations mafieuses ou à certains États font du piratage une activité commerciale très lucrative. Ils ont pour buts aussi bien l'exfiltration des données à des fins de revente, de discrédit (on pense par exemple à la divulgation inopportune de données du GIEC[1]) que la destruction ou l'arrêt pur et simple des SI cibles. Les conséquences peuvent être catastrophiques: pendant la crise du COVID, la mise en panne des SI de certains hôpitaux a conduit au décès de patients.

On ne peut ignorer la dimension géopolitique des attaques sur les SI. Les Etats-Unis, la Russie et la Chine ont été les premiers à développer une réelle stratégie de lutte dans le cyberespace avec une hausse considérable des moyens affectés à cette guerre. Au-delà des capacités d'attaque ou de défense, ces États ont aussi agi au plan législatif pour imposer des réglementations parfois trans nationales leur permettant en toute légalité d'avoir accès aux données étrangères (on pense ici au CLOUD Act[2] ou au FISA[3] américains) réaffirmant leur puissance dans un monde cyber aux contours flous.



2

Plus prosaïquement, la matérialisation efficace de ces menaces modernes n'est pas mieux illustrée que par l'omniprésence des **rançongiciels**, traduction technique de tous les objectifs que nous venons de décrire. Par un simple logiciel délivré par courrier électronique ou introduit dans le SI en exploitant une vulnérabilité quelconque, le groupe d'attaquants :

→ chiffre les données de sa cible, les rendant indisponibles (arrêt de l'activité) ;

→ exfiltre les données plus intéressantes (monétisation parallèle) ;

→ demande une rançon pour restituer l'accès aux données ou au SI (intérêt économique) ;

→ menace de divulguer les données en cas de non-paiement (atteinte à l'image, aux intérêts de la cible).

On est à la fois ébahis et horrifiés de la facilité de mise en œuvre de la menace et de la portée des impacts possibles.

Il existe des menaces plus pernicieuses encore qui peuvent faire passer les unités

de recherche du statut de victime à celui d'acteur malveillant. En prenant le contrôle du SI de l'unité, le groupe d'attaquants restant alors silencieux s'installe durablement, étend son emprise latéralement en prenant le contrôle de systèmes adjacents à ceux initialement compromis et se tient prêt à tirer parti de ces systèmes « zombies » et des énormes réseaux de l'ESR pour lancer des attaques en masse vers d'autres cibles, *incognito*.

L'unité cible initiale se retrouve alors en position d'éventuel accusé d'attaque, avec les conséquences légales qu'on devine.

« POURQUOI TANT DE HAINE ? »

Si les établissements de recherche sont aussi ciblés par les attaquants depuis plusieurs années, les raisons de cet intérêt sont évidentes :

→ La **maturité en sécurité des systèmes d'information** est significativement plus faible que dans les entreprises privées de taille équivalente, même si elle reste globalement un peu meilleure que dans les collectivités territoriales. Une cible vulnérable est une cible de choix…

→ Les **capacités de calcul disponibles, la dimension des réseaux** ESR, les capacités de stockage font des SI des unités des espaces confortables voire luxueux pour les activités des attaquants. Des clusters aux grands calculateurs nationaux, jusqu'aux postes de travail eux-mêmes, toutes les ressources sont utiles pour les pirates qui vont les utiliser à leurs propres fins (attaques distribuées, minage de cryptomonnaies…) ou en revendre l'usage à d'autres ;

→ L'**exposition sur Internet** de nos ressources informatiques est (souvent trop) large, augmentant la surface d'attaque disponible pour les pirates. L'élargissement du travail à distance a provoqué une hausse de cette exposition, qu'il nous faut mieux contrôler alors que ces pratiques vont s'installer dans la durée ;

→ La **relative faiblesse des moyens humains** affectés à la gestion des ressources engendre une obsolescence technique et un retard de mise à jour qui augmente le nombre des vulnérabilités disponibles pour l'attaquant et facilite son entrée ;

→ Enfin, les données produites et manipulées par nos unités ont des valeurs immenses !

Il est nécessaire de prendre un peu de recul sur les données existantes dans les SI des unités afin d'en mieux comprendre l'intérêt pour l'attaquant. Leur revente ou leur cession à des tiers concurrents, étatiques ou privés, représente un bénéfice considérable comparé à l'effort nécessaire pour les obtenir.

→ Les données brutes, la description des savoir-faire et les résultats avant publication constituent évidemment le premier centre d'intérêt ;

→ Les fonctions de soutien aux activités (achat, budget, comptabilité, ressources humaines, contractualisation/projets, missions…) représentent une masse de métadonnées dont l'analyse et la corrélation permettent une connaissance intime des activités de l'unité, parfois même une prévision de son activité future (dialogue budgétaire…) ;

→ L'agrégation de données de nombreuses unités dans des systèmes d'information centraux au niveau des établissements augmente, par effet de masse, l'intérêt pour l'attaquant et donc la sensibilité résultante du SI qui porte ces données ;

→ Dans des nombreuses disciplines, les données à caractère personnel qui sont utilisées à des fins scientifiques peuvent être détournées pour usurper des identités, procéder à un ciblage commercial… On pense immédiatement aux sciences humaines et sociales et à leurs nombreuses cohortes. Le rôle de la sécurité des SI dans la protection de ces données rejoint alors la mission du délégué à la protection des données.

Quelles sont les cibles prioritaires des attaquants ? On constate aujourd'hui un tropisme évident vers le domaine de la santé, à la fois par son actualité brûlante mais aussi par sa vulnérabilité chronique. De nombreux laboratoires privés ont eu à subir douloureusement les conséquences de ces attaques récentes[4]. Cependant, la vision quotidienne des incidents de sécurité SI montre sur le terrain qu'il n'y a pas réellement de cible privilégiée et que la diversité des objectifs poursuivis élargit la portée des menaces à toutes les unités.

Enfin, si les conséquences de ces attaques aux SI sont visibles par leurs effets directs sur ces SI eux-mêmes, il ne faut absolument pas oublier les conséquences humaines indirectes. Au-delà des coûts générés pour la gestion des conséquences, la perturbation d'un SI ou la divulgation de données portent des risques humains pouvant aller jusqu'au risque vital pour les personnes concernées. Cela se conçoit simplement pour un patient d'un hôpital victime de cyberattaque, mais que dire d'un opposant politique interviewé par un chercheur en sciences humaines dont les propos et les informations personnelles seraient rendues disponibles pour ses oppresseurs ?

4 | Pierre Fabre | https://www.lemondeinformatique.fr/actualites/lire-pierre-fabre-revil-a-la-manoeuvre-25-m$-de-rancon-demandes-82571.html,

Ceva | https://business.lesechos.fr/entrepreneurs/numerique-cybersecurite/0610998864424-le-patron-du-laboratoire-ceva-raconte-la-cyberattaque-qui-a-paralyse-son-eti-343905.php,

mais aussi AP-HP | https://www.lexpress.fr/actualite/societe/vol-en-ligne-a-l-ap-hp-ce-que-font-les-pirates-de-vos-donnees-medicales_2158573.html,

QUE FAIRE ?

Le temps de la sidération et du découragement est révolu. À tous les niveaux, nous sommes tous acteurs de la sécurité de nos Si et avons tous des leviers et des impacts sur la protection du potentiel scientifique et technique de la Recherche.

Simple utilisateur, je me dois d'être vigilant au quotidien dans mes usages numériques. Je prends le plus grand soin de mes divers accès au SI (mots de passe, certificats…). Je ne mélange pas ma vie privée et mes activités professionnelles. Je sauvegarde mes données, je réalise ou fais réaliser la mise à jour mensuelle des systèmes que j'utilise. J'avertis ma hiérarchie et mon chargé de SSI d'unité en cas d'incident. Je redouble de vigilance quand je suis hors de mon unité (mission, télétravail).

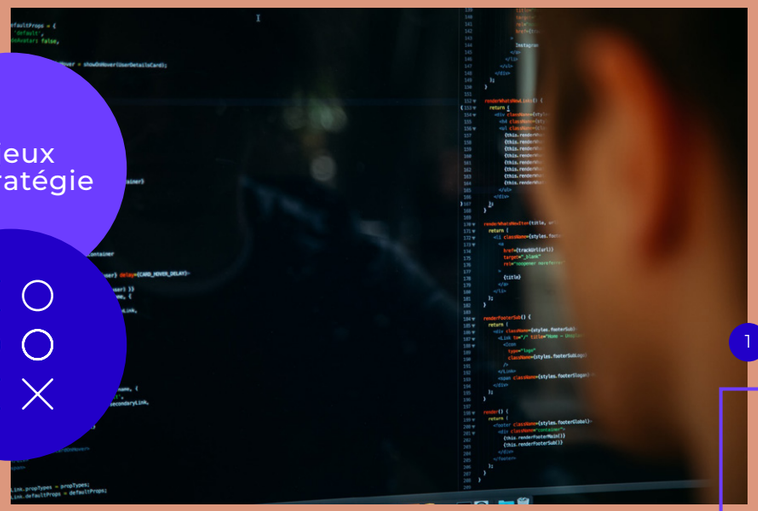
Informaticien d'unité ou Chargé de SSI, j'ai constamment à l'esprit la nécessité de mettre à jour mes infrastructures et de vérifier la présence de vulnérabilités. Je planifie mes activités liées à la sécurité avec mon directeur d'unité. Je sauvegarde les données de l'unité, et je propose à mes utilisateurs des outils qui respectent les enjeux de protection des données (certification par l'ANSSI, insoumission à des réglementations étrangères, opération par des tiers de confiance…).

Directeur/Directrice d'unité, je garde à l'esprit que la SSI est un enjeu important de l'ensemble des projets de mon unité, qu'elle doit être pensée en amont et pas en aval de la conduite du projet, et que je dois affecter les moyens nécessaires à ses missions. Je suis le responsable de la sécurité de l'unité, et à ce titre, je dois évaluer la sensibilité des données que je détiens afin de protéger les plus sensibles. Dans toutes ces tâches, je m'appuie sur un chargé de SSI que je désigne, et je m'entoure des compétences nécessaires au sein d'un comité de pilotage.

Au niveau de nos établissements, et en particulier dans le contexte si particulier des unités mixtes de recherche, la diversité des intervenants dans la maîtrise d'œuvre des SI rend indispensable un dialogue permanent sur la SSI. Comment gérer la sécurité du SI quand le réseau est géré l'université, les serveurs gérés par l'unité et des logiciels fournis par des tiers ? Cela commence par **la reconnaissance par tous de la réalité des risques et des menaces, et de l'intérêt commun de la protection**. Une fois cette communauté de vue acquise, l'identification des ressources et données sensibles en commun, et une répartition des tâches pertinente, dans le cadre d'un plan pluriannuel de sécurisation semble la meilleure manière d'inscrire dans la durée une démarche d'amélioration continue de la SSI.

La chaîne fonctionnelle humaine en SSI dans la communauté ESR (FSSI des tutelles, Fonctionnaires Sécurité et Défense et RSSI d'établissements, CSSI en unité) est forte, organisée et volontaire. Elle est le bras armé de la gouvernance qui doit s'appuyer sur elle. Les membres doivent être reconnus, soutenus et valorisés dans leurs difficiles actions. Qu'elle soit ici remerciée de son travail quotidien !

enjeux et stratégie



1 | Photo by Charles Deluvio on Unsplash

RSSI, PSSI, AQSSI… Et SI on clarifiait les choses ?

C’est complexe, cadré, protégé… et on comprend pourquoi la sécurité des SI est si fondamentale. Explication de texte.

auteur
Philippe Bader, RSSI, Amue

↘ POURQUOI UN RSSI ?

Chaque établissement d’enseignement supérieur est invité à mettre en place une chaîne fonctionnelle de la SSI (Sécurité Systèmes d’Information). Le sommet de cette chaîne comprend l’AQSSI (Autorité Qualifiée de Sécurité des Systèmes d’Information), le Directeur et le RSSI (Responsable de la SSI) et si possible un suppléant. Il est préconisé de consolider ce socle par un réseau interne de correspondants. A l’Amue, nous avons un Consultant technique sécurité dédié aux aspects des projets,travaillant en lien avec le RSSI.

Le RSSI et son suppléant sont désignés par l’AQSSI qui leur remet une « lettre de mission » explicitant leurs attributions. Ils réfèrent directement à l’AQSSI pour les questions formelles et les dossiers « sensibles ». Leur positionnement dans la chaîne fonctionnelle de la SSI, les conduit à avoir différents contacts afin d’échanger sur la sécurité et les problèmes rencontrés. Un processus de désignation complexe permet de garantir le bon fonctionnement des échanges avec les différentes institutions comme l’ANSSI, RENATER, le CERT, etc.

↘ POURQUOI UNE PSSI ET QUID DE LA PSSIE?

La PSSI (Politique Sécurité Systèmes d’Informations) définit un cadre pour gérer la sécurité des systèmes d'information. L'élaboration d'une PSSI s'inscrit dans une démarche globale en cohérence avec la politique de l'établissement et dans un cycle d'amélioration continue. Adopter une PSSI nécessite de faire des choix stratégiques concernant notamment les enjeux à prendre en compte, les besoins et objectifs de sécurité, les moyens humains et financiers pouvant y être affectés et les risques résiduels que l'établissement décide d'accepter. La PSSI propose des mesures organisationnelles et techniques pour atteindre des objectifs de sécurité cibles.

La PSSI s'appuie pour son application et sa révision périodique sur un Système de Management de la Sécurité de l'Information (SMSI). Ce SMSI tire ses bases de la norme ISO 27001 (Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences à voir ici et les normes suivantes) et fonctionne sur le modèle PDCA (Planifier, Déployer, Contrôler, Agir/Améliorer). Il est décrit dans le document Politique de Management de la Sécurité de l'Information (PMSI) qui précise notamment l'organisation des instances de pilotage et des acteurs SSI.

L'objectif à terme est de gérer la sécurité comme étant un processus à part entière. Le RSSI a un objectif de sensibiliser et de convaincre la direction dans la bonne gestion de la SSI par les risques, il effectue une étude du contexte de l’établissement, afin d'adapter le document de PSSI. Il prend comme guide, la partie relative à l'étude du contexte dans les documents de gestion d'analyse de risque notamment le guide d'entretien. Il adapte la politique de sécurité du système d'information en sélectionnant les règles à mettre en place et s’adapte au contexte de l’établissement.

La PSSIE (Politique de Sécurité du Système d'Information de l’Etat) fixe les règles de protection applicables à son SI. Elle est essentielle dans les actions pour faire face aux menaces en mesurant les risques et limiter au maximum les tentatives d’exfiltrations de données sensibles, l’atteinte à la vie privée des usagers et d’éviter les tentatives d’intrusion sur le système d’information.

Cybermoi/s 2021 : se protéger grâce à des mots de passe sécurisés

Et si nous profitions d’octobre pour suivre l’évènement Cybermoi/s de l’ANSSI sur les mots de passes sécurisés ? Toutes les informations ici →

Sécurité et ouverture du code

Certains mettent Sécurité et Open Source en opposition, mais il apparait de plus en plus évident que le degré de sécurisation des solutions Open Source leur apporte un grand avantage.

Vous pouvez relire la collection numérique N°13 (février 2021) « Vive le numérique Libre ! » et notamment les parties qui abordent avec conviction ce sujet de sécurité : l’édito de M. Eric Bothorel ou l’article de l’association des Vp Num, Page 11.

Egalement l’ANSSI qui encourage via cet engagement à investir dans l’open source pour la sécurité de nos SI. Enfin cette annonce récente de l’ouverture, en novembre, du code de France Connect (voir cet article)

L’ENGAGEMENT DE L’ANSSI POUR L’OPEN SOURCE

L’investissement de l’ANSSI – l’un des plus grands contributeurs de l’Etat dans le logiciel libre – se veut pragmatique. Il répond à un réel enjeu de sécurité et de souveraineté, pour protéger les biens communs et investir dans des technologies et des solutions d’avenir. Cette démarche se fonde sur les possibilités inédites qu’offre l’open source en terme d’adaptation, de maîtrise, d’évaluation et de diffusion, à la condition d’y consacrer les ressources nécessaires.

vue d'ensemble

1

auteur
Cédric Servaes,
Agence de Mutualisation des Universités et Établissements, Amue

À l'Amue, la sécurité est une priorité

Stratégie, homologation et protection des données sont les bases de la démarche sécurité à l'Agence, qui mutualise au quotidien avec ses adhérents

Depuis 2016, l'Amue a entrepris une démarche d'intégration de la sécurité dans l'ensemble de ses projets. Une méthodologie spécifique, indexée sur le cycle de vie des projets a été définie. Elle est adaptée à l'environnement de développement des offres de l'Amue (cycle en V, cycle agile, co-construction).

STRATÉGIE

Le constat a été fait que, bien qu'il y ait déjà de nombreuses mesures de sécurité en place dans les produits de l'Amue, une **gouvernance spécifique et une rationalisation des processus devenaient nécessaires.**

Concrètement pour nos adhérents, la mise en œuvre de la sécurité s'est matérialisée sous la forme de la réalisation d'un Dossier de Sécurité pour nos produits proposés en mode « On-Premise ».

Ce dossier atteste de cette prise en compte exhaustive de la sécurité. Les adhérents peuvent, à leur tour, utiliser ce Dossier de Sécurité pour compléter leur dossier d'homologation de sécurité dans leur contexte (infrastructure, exploitation).

Afin de réaliser ce **Dossier de Sécurité**, chaque équipe projet a abordé les points suivants :

- Réalisation d'une analyse de risques basée sur la méthode EBIOS
- Prise en compte des menaces malveillantes et accidentelles et les normes de référence à des fins d'exhaustivité de la démarche

1 | Image par VIN JD de Pixabay

2 | Photo by Jason Leung on Unsplash

- Intégration de la sécurité dans les relations avec les partenaires et sous-traitants

Pour les produits en offre de service, l'Amue s'est conformée à la législation en effectuant une homologation de sécurité type RGS pour les produits **SIHAM-PMS** et **CAPLAB**.

Ainsi, une commission d'homologation composée de l'AQSSI (Autorité Qualifié en SSI) de l'Amue, Stéphane Athanase, notre directeur, et les RSSI représentants des établissements utilisateurs se réunit régulièrement :

- Le service SIHAM-PMS a été homologué tous les 3 ans depuis sa mise en production en mars 2015.
- Le produit CAPLAB, étant dans un processus de construction, a obtenu des homologations dites « provisoires » depuis janvier 2019 (phase pilote).

Pour ces homologations, l'Amue effectue différents audits (tests d'intrusion, audit de code basé sur l'OWASP, audit d'architecture) en s'appuyant sur un PASSI (Prestataire d'Audit SSI) certifié par l'ANSSI.

UNE MÉTHODOLOGIE DE SÉCURITÉ

Afin que les équipes puissent mettre en œuvre le juste niveau de sécurité d'une façon exhaustive sur leur projet, en conformité avec les exigences règlementaires (PSSIE, RGS, PPST), une méthodologie a été élaborée.

Cette méthodologie d'intégration de la sécurité dans les projets a été développée depuis 2016 à partir des documents ANSSI. Les travaux ont permis de produire un kit méthodologie (guides, fiche d'activités, outils, modèles) dont des recommandations d'organisation, des supports de formation EBIOS, des modèles de documents (PAS, Analyse de risques, comitologie, etc).

Une adaptation à l'**agilité** a été faite avec le projet CAPLAB en 2018/2019, basée sur le document ANSSI en intégrant les notions de sprints, abuser story (user story particulier à la sécurité), etc.

De plus, une veille des alertes de sécurité sur les composants des solutions Amue est faite constamment depuis 2016, avec une information aux établissements si besoin.

PROTECTION DES DONNÉES

En complément des actions de cyber sécurité, un audit complet sur la **protection des données** a été réalisé en 2020 sur tous les produits Amue (les 13 offres).

Pour certaines offres Amue, cet audit a amené à la réalisation d'un PIA.

De manière générale, les **plans d'actions** définis suite aux audits et analyse de risques sont revus régulièrement avec chaque équipe.

Ransomware As A Service

Les Ransomware, rançongiciels en Français, sont des logiciels malveillants qui ont pour but de prendre en otage des ordinateurs ou données d'une personne ou d'une entreprise, souvent en les cryptant, et de demander une rançon pour les « libérer ».

Particuliers, entreprises, universités, personne n'est complétement à l'abri de ces attaques qui prennent de plus en plus d'ampleur.

Aussi incroyable que cela puisse paraitre, il existe désormais des offres de Ransomware As A Service (RAAS). Basé sur le même principe que les autres locations de services logiciels (SAAS, Software As A Service), des pirates peuvent louer facilement et à vil prix, des Rançomware et se payer des services additionnels : suivi détaillé et tableau de bord des attaques, assistance client pour que les victimes puissent payer, service de paiement,...

Cette facilité d'accès aux RansomWare accroit les risques de ce type d'attaques.
Pour aller plus loin et voir des parades, ces articles, sources de cet encart, ici et là.

2

vue d'ensemble

auteur
David Rongeat, responsable numérique, Amue

Lumière sur la SSI

Ce qui se cache sous la notion de Sécurité des systèmes d'information, les acronymes, les concepts et la réalité.

1 | Photo by Darwin Laganzon de Pixabay

Essayons en quelques notions clés de faire un tour d'ensemble de la SSI (Sécurité des Systèmes d'Informations) en présentant les principaux concepts d'un sujet qui dépasse la technologie puisqu'il implique les usages, la gouvernance, la **gestion de crise**…

Il ne s'agit pas ici d'être exhaustif : les documents de référence de l'Anssi (voir article page 8) évoquent plus de 160 principes regroupés en 16 domaines, soit l'expertise des acteurs de la SSI, notamment les RSSI (Responsables Sécurité des SI) : voir article page 14)

UNE VISION STRATÉGIQUE, UNE POLITIQUE SSI

La responsabilité de la **gouvernance** d'une organisation sur le sujet de la sécurité des SI est pleine et entière ; de fait, en suivant les recommandations de l'**Anssi** (voir encart), chaque établissement se doit d'adopter une Politique de Sécurité des SI (**PSSI**) qui porte la stratégie de l'établissement en la matière. Une stratégie qui va se doter d'une vision de projet établissements, de moyens suffisants, d'une comitologie, d'outils,…

Cette Politique SSI se décline sur l'ensemble des domaines de la sécurité dont son **organisation**, la définition des **responsabilités**, sa diffusion auprès de l'ensemble des membres de l'établissement, la **protection des données**, la mise en œuvre concrète de cette politique,…

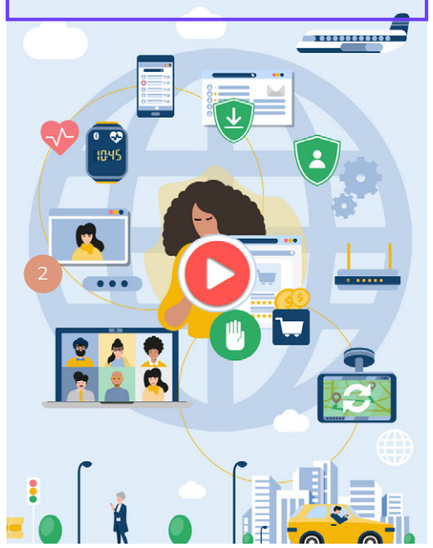
Une stratégie SSI s'appuie, entre autre, sur la **gestion des risques**, discipline qui permet en amont d'identifier, évaluer, pondérer,… les risques associés à la Sécurité des SI. Ensuite elle se décline sur l'ensemble des activités de l'établissement ; Notamment elle doit être systématiquement intégrée dans les projets numériques, ceci pouvant aller jusqu' à une démarche d'**homologation**.

Pour aller plus loin sur la PSSI (politique de sécurité des systèmes d'information) :

rendez-vous sur la page du guide d'élaboration de politiques de sécurité des systèmes d'information →

Un Mooc sur la sécurité des SI

L'ANSSI propose un Mooc sur la SSI. Il est composé en 4 modules :
• Panorama de la SSI
• Sécurité de l'authentification
• Sécurité sur Internet
• Sécurité du poste de travail et nomadisme
Ce Mooc gratuit permet de s'initier à la cybersécurité, approfondir vos connaissances, et ainsi agir efficacement sur la protection de vos outils numériques. Son suivi intégral permet d'obtenir une attestation de réussite.
À faire de toute urgence ici →



2

LES USAGERS

Toute la technicité et le travail des experts en sécurité des SI ne peut fonctionner qu'à condition de sensibiliser l'ensemble des usagers aux problématiques de sécurité des SI. Ils en sont acteurs. Il convient de **former et d'informer** régulièrement les usagers du SI des risques de sécurités, des bonnes pratiques en la matière et de responsabiliser chacun sur ce sujet. L'aspect humain est crucial dans une politique de sécurité, requérant la **sensibilisation régulière** des usagers.

Par ailleurs, les usagers s'attendent à ce que l'accès à leurs données personnelles, gérées dans le SI de l'établissement, soit sécurisé afin de respecter **leurs droits** (voir articles page 6 et page 22)

QUELQUES ÉLÉMENTS CONCRETS

La Politique SSI de l'établissement permet, entre autre, d'**anticiper** les réactions à avoir en cas d'incident : quelles actions concrètes pour limiter les risques ? Comment organiser un plan de continuité d'activité (**PCA**) ou un plan de reprise d'activité (**PRA**) après sinistre ? Quels dispositifs de **sauvegarde** des données ont été mis en place à cet effet ? Qui (et comment) informer en cas d'attaque informatique ? Quelle **communication** prévoir ?... Comment est organisée une cellule de crise ? Tous ces éléments organisés, testés, revus régulièrement permettront d'affronter avec une meilleure réactivité et sérénité un probable problème sur le SI.

Elle permet avant tout de se prémunir au mieux de ces problèmes : **Antivirus**, **antispam**, contrôle d'accès, **authentifications** multiples, veille régulière, **protection** physique des salles machines, **cryptage**, mise à jour régulière des logiciels, **journalisation** et enregistrement des traces d'utilisation, contrôle du réseau, etc etc … sont des outils ou méthodes utilisés quotidiennement par les acteurs de la sécurité des SI.

Et parfois ce mail que vous recevez émanant de votre RSSI : « Attention SPAM : nous recevons un message intitulé « facture à payer », d'une provenance inconnue qui contient un lien ressemblant à une facture (ne surtout pas l'ouvrir) ; supprimez ce message… ».

Une partie visible de l'iceberg, de l'ensemble du travail mené et qui ici va empêcher une attaque de type Ransomware (voir encart page 17) /Merci cher collègue RSSI.

Communication interne et sensibilisation

La sécurité des SI passe par la sensibilisation et la communication auprès des usagers. À l'Amue, le RSSI (voir page 14) partage beaucoup d'informations via un intranet dédié au sujet. Les récentes alertent sécurité côtoient des liens vers des outils de sensibilisation, des documents de référence, une lettre d'information, un blog. Bref toutes les informations utiles aux agents de l'Amue sur le sujet de la sécurité des SI. Sans oublier les mails à dessein en cas d'alerte de sécurité méritant notre attention. Merci Philippe.

vue d'ensemble

auteur
Jérôme Notin, directeur général du groupement d'intérêt public Action contre la cybermalveillance, opérateur de la plateforme Cybermalveillance.gouv.fr.

Se protéger de la cybermalveillance

Devant cette réalité qui touche tous les secteurs et toute la population, la plateforme Cybermalveillance.gouv.fr est un recours précieux qui informe, accompagne et assiste. Et on vous dit comment.

↘ QU'EST-CE QUE LA CYBERMALVEILLANCE ?

Il n'existe pas de définition officielle de la cybermalveillance. Notre dispositif considère toutefois que la cybermalveillance regroupe l'ensemble des crimes et délits pénalement répréhensibles commis par le biais ou à l'encontre de systèmes numériques (ordinateur, téléphone mobile, serveur ou réseau d'entreprise…), et ce avant la phase de judiciarisation. À ce jour, la plateforme Cybermalveillance.gouv.fr fournit de l'assistance aux victimes sur près de 50 formes de cybermalveillances qui vont du hameçonnage (phishing), aux rançongiciels (ransomware), en passant par le piratage de compte en ligne, les fraudes aux virements ou encore le cyberharcèlement.

La cybermalveillance regroupe l'ensemble des crimes et délits pénalement répréhensibles commis par le biais ou à l'encontre de systèmes numériques

↘ POURQUOI SE PROTÉGER ?

L'explosion des usages numériques ces dernières années, qui s'est encore accentuée avec la crise sanitaire par le télétravail massif, le téléenseignement, le commerce en ligne, a vu en corollaire une recrudescence sans précédent des faits de cybermalveillance. Contrairement à l'image d'Épinal, les cybercriminels ne sont plus aujourd'hui les seuls adolescents immatures que l'on peut imaginer. Ils s'organisent sur le darknet en équipes très structurées et compétentes pour maximiser leurs profits. Leur seule idéologie est de chercher à gagner le plus d'argent possible, peu en importe les conséquences pour les victimes. Particuliers, entreprises, collectivités, universités et mêmes hôpitaux, aujourd'hui plus personne n'est, ni ne sera, épargné.

↘ SE PROTÉGER POUR SOI, MAIS AUSSI POUR LES AUTRES

Se protéger de la cybermalveillance c'est avant tout se protéger soi-même. Protéger son identité numérique, mais aussi ses moyens informatiques et de communication contre les différents types d'attaques qu'ils peuvent subir. Mais avec l'interpénétration des usages numériques personnels et professionnels, se protéger soi-même c'est aussi chercher à protéger ses collègues, son entreprise, et même ses administrés. En effet, les conséquences d'un manque d'hygiène cybersécurité individuel peuvent avoir des conséquences sur le collectif et même au-delà. Cela peut aller jusqu'à mettre en danger son emploi et celui des autres salariés. Dans un établissement cela peut avoir des répercussions sur les étudiants en altérant l'enseignement en présentiel ou distanciel, les résultats des examens et même avoir des impacts personnel sur les enseignants, personnels administratifs ou étudiants si leurs données personnelles se retrouvent dans de mauvaises mains.

↘ COMMENT SE PROTÉGER ?

Pour commencer à se protéger il faut déjà prendre conscience des risques pour en accepter les contraintes. Et ces risques sont réels : l'actualité le démontre quasi quotidiennement. Ce premier pas effectué, il faut comprendre que 80 % des cyberattaques pourrait être évité si des mesures simples étaient respectées comme une bonne gestion des mots de passes qui doivent être suffisamment complexes et surtout différents pour chaque service, si les mises à jour de sécurité étaient régulièrement appliquées sur les serveurs, ordinateurs, smartphones, si l'ensemble des données de ces équipements étaient régulièrement et convenablement sauvegardées, si des mesures de filtrage et de supervision basiques étaient appliquées sur ses connexions à distance.

Mais on ne peut pas tout faire en même temps et régler du jour au lendemain la dette du niveau de cybersécurité qui peut parfois s'avérer lourde. Il faut donc prioriser ses actions après avoir réalisé un état des lieux pour commencer par combler ses vulnérabilités les plus critiques. Pour cela, il faut savoir se faire accompagner par des spécialistes en cybersécurité comme les prestataires labellisés ExpertCyber par Cybermalveillance.gouv.fr.

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

Le label ExpertCyber

Construit avec des associations professionnelles et avec le concours de l'AFNOR, le label ExpertCyber de Cybermalveillance.gouv.fr vise à donner un premier niveau de reconnaissance des compétences des prestataires spécialisés en cybersécurité agissant dans les trois domaines de la sécurisation, la maintenance et la réponse aux incidents pour les publics professionnels (entreprises, associations, collectivités…).

À ce jour plus de 110 entreprises ont reçu ce label.

En savoir plus ici →

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

Présentation de Cybermalveillance.gouv.fr

Cybermalveillance.gouv.fr est la plateforme du dispositif national de prévention et d'assistance aux victimes de cybermalveillance.

C'est le dispositif voulu par l'État pour répondre aux besoins de conseils et d'assistance en cybersécurité des particuliers, des entreprises et des collectivités.

Cybermalveillance.gouv.fr est opéré par un groupement d'intérêt public qui regroupe les acteurs de l'État et de la société civile engagés dans sa mission d'intérêt général.

Les missions de Cybermalveillance.gouv.fr sont :
→ la **prévention** et la sensibilisation des publics avec la publication de nombreuses ressources (fiches, articles, infographie vidéos…) gratuites et réutilisables ;
→ l'**assistance aux victimes** qui peuvent réaliser en ligne un diagnostic de leur situation et recevoir les conseils nécessaires pour y faire face, et même être mis en relation avec les près de 1 200 prestataires spécialisés référencés susceptibles de pouvoir les assister ;
→ l'**observation de la menace** dans le but de la prévenir en alertant les populations et les pouvoirs publics.

En savoir plus :
https://www.cybermalveillance.gouv.fr/

vue d'ensemble

auteur·e·s
Héloïse Faivre, DPO adjointe des Universités Grenoble Alpes et Savoie Mont Blanc, **Victor Larger**, DPO de France Université Numérique, **Marion Lehmans**, DPO de Sciences Po, **Guillaume Pourquié**, DPO de Grenoble EM, pour le réseau SupDPO

Protéger les données personnelles, c'est l'affaire de tous

Un article collégial de SupDPO qui fait la lumière sur le rôle de chacun des acteurs en rapport avec le SI et sur l'individuel au service du collectif.

L'impact d'une crise SSI peut être durable, étendu, et coûteux. Parmi les coûts directs et indirects, nul doute que ceux liés aux violations de données personnelles sont particulièrement notables pour l'organisme concerné : perte de confiance des usagers, impact réputationnel, conséquences sur les partenariats et activités, perte définitive des données, actions de groupe des personnes concernées, et naturellement audit de l'autorité de contrôle. Ceci sans compter les dommages que font aussi et avant tout les violations de données sur les personnes concernées (eg. conséquences d'une usurpation d'identité, atteinte à la réputation) allant jusqu'à potentiellement des atteintes physiques, matérielles ou morales irrémédiables pour les personnes.

Très concrètement depuis 2018, la pression sur les établissements, en France et ailleurs, s'est intensifiée et s'est traduite de différentes manières par des tentatives d'atteinte au SI[1] (tentatives d'hameçonnage, de rançongiciel, etc.), pouvant engendrer une interruption totale des services ou des pertes financières considérables[2]. Des sanctions ont ainsi pu être prononcées à hauteur de plusieurs centaines de milliers d'euros, pour des violations de données intervenues du fait de défauts de sécurité.

Pour l'ESR, si l'autorité nationale, la CNIL, a privilégié jusqu'à présent l'accompagnement de nos établissements et a entretenu une relation de confiance tissée depuis 2007 avec SupDPO, l'association des Délégués à la protection des données de l'ESRI notamment, ses homologues européens ont déjà eu à prononcer des sanctions sévères dans le secteur public, ainsi que dans l'enseignement supérieur et la recherche.

Le site du réseau SupDPO recense quelques mises en demeure et sanctions prononcées par les autorités de contrôle européennes. Parmi celles-ci, nous observons avec attention la sanction de l'autorité suédoise à près de 400 k€ pour un manquement concernant les habilitations d'accès aux dossiers médicaux, ou encore la sanction de l'autorité polonaise pour défaut de sécurité des enregistrements collectés dans le cadre d'examens à distance.

1 | Eric Nunes, 20/04/2021. Les universités, cible de choix des hackeurs. Lemonde.fr.

2 | Ex: L'Ecole de médecine de l'université de Californie à San Francisco (UCSF) a été victime d'une attaque au ransomware. Le gang Netwalker a confirmé avoir mis la main sur le système de l'université le 3 juin 2020. Cf. https://www.ucsf.edu/news/2020/06/417911/update-it-security-incident-ucsf

Pour s'en prémunir, on se reportera à la formule consacrée par le RGPD et à la mise en place de « *mesures techniques et organisationnelles* », en veillant à ne pas les réduire au binôme informatique et juridique. En effet, la sécurité des systèmes d'information nécessite, certes, des garanties techniques appropriées (tel que l'authentification via protocole sécurisé, l'usage d'un VPN, des filtrages IP, le déploiement d'une double authentification, des configurations wifi adaptées,…).

Toutefois, il importe de rappeler et marteler que la « *sécurité des systèmes d'information* » dépasse très largement le périmètre de l'informatique. Ce n'est donc ni l'apanage, ni le fardeau des seuls RSSI et DSI : les mesures organisationnelles renforcent le savoir-faire des équipes et contribuent à la sécurité du SI, à travers par exemple le maintien d'une chaine fonctionnelle SSI identifiée et fluide, des procédures de revue de mots de passe, une meilleure compréhension par défaut et dès la conception des processus, et une meilleure identification et gestion de la donnée tout au long de son cycle de vie. Ceci permet d'assurer la minimisation des données et doit être conforté par des actions de sensibilisation régulières et suivies.

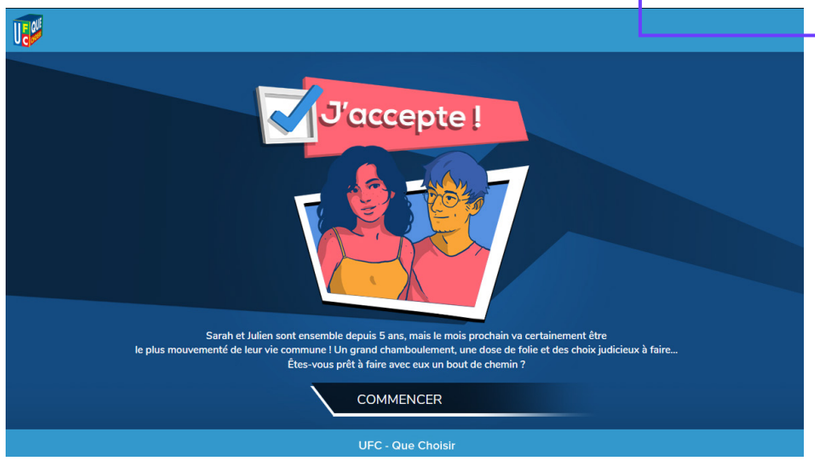
La conclusion à retenir est que chaque utilisateur du système d'information (étudiants, informaticiens, secrétaires, conservateurs, enseignants, DGS,…) impacte la sécurité du SI : l'utilisateur peut l'affaiblir lorsqu'il méconnait les consignes prévues par la charte numérique, la politique de sécurité des systèmes d'information et la politique de protection des données et de vie privée de l'établissement (verrouiller son poste de travail, être vigilant concernant les emails et sites tiers potentiellement malveillants, paramétrer la confidentialité de ses équipements, comptes et navigateurs, apprendre à chiffrer, maintenir la sécurité de ses équipements et sauvegarder ses données, utiliser un VPN, et les moyens de stockage et de communication mis à disposition par l'établissement).

Pour protéger les données d'un établissement, celles des étudiants, des personnels, des partenaires, chacun doit œuvrer, à son niveau c'est à dire *a minima* respecter les règles d'hygiène numérique dont l'ANSSI, la CNIL et SupDPO et, dans les établissements, les DPO et RSSI font la promotion quotidienne.

L'Amue vous partage un jeu en ligne sur les données personnelles

Ce jeu en ligne, proposé par UFC que choisir, vous met dans une situation réelle durant laquelle deux personnages vont se confronter à des questions autour de la gestion de leurs données personnelles. Ludique, cette animation grand public vous prendra 15 minutes.

Attention aux pièges !
À voir ici →



vue d'ensemble

auteur
Frantz Gourdet,
DPO de l'Amue

Sécuriser pour protéger les données personnelles : 13 points de contrôle Privacy by design

Détail de ces mesures agréées par la CNIL

Nous mutualisons ici quelques mesures attachées à treize points de contrôle de conformité au RGPD (Règlement Général sur la Protection des Données). Proposées par l'Amue dès 2016 puis en 2018 à l'occasion de la réactualisation de son label « Gouvernance RGPD », ces mesures – infime partie intégrante de notre « Procédure de Gouvernance Informatique et Libertés » – ont été agréées par la CNIL. Les treize points présentés sont vérifiés à la conception des traitements, ainsi qu'en phase de maintenance évolutive, par les équipes en charge de l'offre SI Amue. Il est à noter que la mise en conformité effective de l'existant peut se dérouler sur plusieurs années, lorsqu'il s'agit de prendre en compte, par exemple, des durées de conservation impliquant une politique d'archivage en base active, intermédiaire puis définitive, non exigée à la genèse d'applications antérieures au RGPD.

1. Finalité : finalité déterminée, explicite et légitime

a. Finalités connues et énoncées de manière détaillée et compréhensible par les personnes dont les données vont être traitées

b. Ne pas aller au-delà des finalités déclarées, et effectuer une nouvelle analyse complète pour tout souhait d'ajout de nouvelle finalité

c. Ne permettre de recueillir des données que pour un usage précis et bien défini (éviter par exemple les zones de commentaires libres)

d. Ne pas aller à l'encontre de la loi, ni des droits ou des libertés fondamentales des personnes

2. Minimisation : réduction des données à celles strictement nécessaires

a. Décrire les données traitées en précisant l'origine de la collecte, les catégories de personnes concernées et les destinataires

b. Veiller à ce que les données à collecter soient pertinentes, adéquates et non excessives c'est-à-dire strictement nécessaires à la finalité déclarée

c. Permettre le stockage d'informations personnelles uniquement si elles sont pertinentes et en relation avec la finalité déclarée du traitement

d. Ne pas procéder à des traitements d'information qui, du fait de leur nature, de leur portée ou de leurs finalités, excluent des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire

e. Éviter de traiter le numéro de sécurité sociale sauf après visa du DPO dans les cas autorisés

f. Eviter de traiter des informations relatives à des infractions, condamnations, mesures de sûreté, biométriques ou subjectives, ou des données sensibles qu'il est interdit de collecter sauf autorisation de la CNIL nécessitant des démarches à anticiper plusieurs mois à l'avance

3. Durées de conservation : durée nécessaire à l'accomplissement des finalités, à défaut d'une autre obligation légale imposant une conservation plus longue

a. Déterminer les durées de conservation par défaut. Ces durées seront consignées dans un document de référence mis à disposition des équipes de conception

b. Implémenter un mécanisme permettant de basculer les données à caractère personnel (DCP) de leur base ou archive active à leur archive intermédiaire

c. Prévoir la possibilité d'appliquer les restrictions d'accès ou d'habilitation qui s'imposeront, ainsi que la possibilité de transférer ces archives intermédiaires aux personnes/services chargés de leur destruction ou de leur archivage définitif

d. Paramétrer les durées afin d'anticiper transitions et évolutions règlementaires/légales

4. Information : respect du droit à l'information des personnes concernées

a. Paramétrer l'affichage de mention d'information afin de permettre à l'exploitant de l'outil conçu de fournir un lien Internet vers sa propre mention d'information ou de personnaliser l'affichage d'une mention type en en renseignant les éléments paramétrés

5. Consentement : obtention du consentement des personnes concernées ou existence d'un autre fondement légal justifiant le traitement

a. Déterminer lesquels des traitements et des DCP à traiter exigent un consentement des personnes concernées en mode opt-in et/ou opt-out

b. Prévoir en conséquence du point précédent des mécanismes de recueil de consentement : case à cocher (opt-in) ou à décocher (opt-out), par exemple

6. Droit d'opposition et autres droits entrant dans le cadre des articles 12 à 23 du RGPD : effacement (droit à l'oubli), limitation du traitement, portabilité et gestion post mortem…

a. Prévoir des mécanismes de suppression des DCP relatives à un traitement donné et à une personne concernée et/ou prévoir des indicateurs/ marques/ témoins permettant d'exclure une personne donnée d'un traitement

b. Prévoir tout mécanisme facilitant l'exercice des droits d'opposition, effacement (droit à l'oubli), limitation du traitement, portabilité, gestion post mortem, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage)

7. Droit d'accès : respect du droit des personnes concernées d'accéder à leurs données

a. Prévoir une fonctionnalité d'extraction de l'ensemble des DCP d'une personne donnée

b. Prévoir les mécanismes facilitant l'exercice du droit d'accès pour les scénarios moins larges

8. Droit de rectification : respect du droit des personnes concernées de corriger leurs données et de les effacer

a. Permettre la rectification - si justifiée - des données personnelles collectées

9. Formalités : définition et accomplissement des formalités applicables au traitement

a. Effectuer l'analyse du régime juridique et des formalités applicables au traitement en fonction de ses finalités et des catégories de données traitées avec l'aide du DPO, en amont du déploiement du traitement dans les établissements

10. En cas de sous-traitance

a. Coopérer à l'adaptation des clauses contractuelles aux prestations de sous-traitance

b. Pour les besoins de bases de formation ou de tests de performance sur données issues des établissements, éviter les « convention de confidentialité » entre l'Amue, le sous-traitant et les établissements autorisant le sous-traitant à récupérer les données des bases de production. Au besoin, le sous-traitant devra fournir aux établissements souhaitant coopérer à la réalisation des tests de masse ou à la constitution de bases de formation, un outil d'anonymisation adapté pouvant être appliqué en toute autonomie par les établissements eux-mêmes sur leurs propres données avant de les transmettre au sous-traitant via l'Amue sous forme déjà « anonymisée »

c. Les mécanismes d'anonymisation proposés par le sous-traitant devront être suffisamment explicités pour faciliter l'évaluation préalable de leur efficience par les établissements

d. Les mises à jour des bases de formation ou de tests seront à réaliser par ré-applications successives de l'outil d'anonymisation sur de nouvelles données réelles i.e. de production

e. Le sous-traitant prévoira la mise à jour de l'outil d'anonymisation lui-même en cas de changement de structure, ou en cas de tout autre possible impact de versions évolutives du produit de l'offre SI Amue sur cet outil

f. Respecter le principe de protection by design/default à toutes les étapes du cycle de vie du produit de l'offre SI Amue

11. Renseignement fiche traitement

a. Dans le cadre de prestations de tierce maintenance applicative ou d'intégration, renseigner la fiche de traitement type de l'application maintenue et/ou intégrée (cf. modèle CNIL), fiche devant être adaptée par les DPO des établissements exploitant ladite application

12. Sécurité

a. Fournir aux établissements exploitant l'offre SI Amue les informations et moyens (liés aux logiciels) permettant aux établissements de prendre des mesures adéquates en fonction des risques afin de garantir l'intégrité, la disponibilité et la confidentialité des DCP

13. Etude d'impact sur la vie privée (EIVP/PIA)

a. En présence de données sensibles ou en raison d'autres critères indiqués par le règlement, fournir aux établissements exploitant l'offre SI Amue les informations et moyens (liés aux logiciels) de mener le volet « gestion des risques » de l'étude d'impact sur la vie privée

LABEL CNIL GOUVERNANCE RGPD
N°2018-279
EXPIRE : 21/06/2021

témoignage

auteur
Philippe Werle,
Responsable Sécurité Système d'Information RSSI/CISO, Université Paris Dauphine-PSL

Sécuriser & organiser la sécurité : enjeu des années à venir

Les failles de sécurité existent dans l'ESRI. Il est urgent de structurer l'offensive, de bâtir une ligne de défense collective et concertée. Prise de conscience !

↘ MANQUE DE CULTURE EN SÉCURITÉ NUMÉRIQUE

Dans son « Avis de la CPU sur les orientations futures de RENATER » du 28 mai 2020, la CPU déclare « Force est de constater que nous avons failli collectivement, gouvernance, tutelle, organismes et universités […] Transversalement à l'ensemble de ces enjeux, la souveraineté informationnelle est sans doute le paramètre le plus important, dans un contexte de société de l'information […] Sur ce point, comme le souligne le rapport public annuel 2020 de la Cour des comptes, « *les établissements s'emparent trop peu de l'enjeu de la sécurité. Ce manque de culture de sécurité numérique est également illustré par l'important recours des usagers de l'ESR aux services en ligne proposés par les entreprises du numérique (messagerie Gmail, utilisation des outils collaboratifs de Google pour le montage de projets stratégiques, outils en ligne d'Amazon ou de Microsoft, etc.). […] Ces enjeux de souveraineté méritent une clarification de la position du ministère.* » Nous sommes aujourd'hui dans une situation de perte de souveraineté. Or l'enjeu majeur qu'accroit encore la crise sanitaire que nous vivons actuellement, c'est bien celui de la souveraineté, de la confidentialité et la sécurité des données.»

↘ UNE CYBERCRIMINALITÉ INDUSTRIALISÉE ET OPPORTUNISTE

Aujourd'hui, le milieu cybercriminel est structuré et industrialisé. Il a établi une économie de la donnée, structurée en sous-traitance, outillée par des plateformes de cyber attaque « as a service » (Voir encart page 17). Après les cyberattaques pandémiques Wannacry et NoPetya de 2017, les leçons n'ont toujours pas été retenues. Nos systèmes restent exposés, peu sécurisés, non mis à jour. Nos mots de passe sont grotesques. La médiatisation est bruyante, notre prise de conscience faible, nos changements d'habitude paresseux. L'université cache ses incidents dans le sable et positionne son RSSI comme un pompier. La cybercriminalité l'a compris. Elle a saisi l'opportunité qu'offraient le distanciel, le télétravail non maîtrisé, les infrastructures sur site mal sécurisées, un « cloud » non souverain commercial criblé de vulnérabilités et une sécurité des systèmes d'information (SSI) sans moyens humains et financiers pour lancer ses opérations. Elle a parfaitement compris que le maillon faible de la chaîne n'est pas technologique, il est culturel et dans sa gouvernance.

En 2020 et 2021, les cyberattaques contre les hôpitaux ont été sans précédent. Exploitant les faiblesses d'un système d'information hospitalier digne d'une usine à gaz, muni d'une sécurité non-invasive à la système-D, les cybercriminels ont « tiré sur les ambulances » à coup de rançongiciel en exposant des vies. Avec la même facilité, ils ont pris pour cible les collectivités, en otage nos données d'administrés. La cible à venir est le temple de la connaissance, riche en données sensibles, l'université[1].

L'université a ouvert de prestigieuses chaires en cybersécurité mais demeure incapable de mettre en œuvre dans son fonctionnement propre la gouvernance de sa SSI. Elle se limite à former ses personnels à des outils, ne permet pas à ses ingénieurs de se mettre à niveau, n'engage pas sa gouvernance dans une culture du risque. L'université fonctionne en silos.

↘ LE NUAGE PROVIDENTIEL

Faute d'une stratégie politique, les plans étatiques nuageux se sont succédés dans l'échec. Plutôt que de poser le problème, il a semblé judicieux de se tourner vers des solutions commerciales non souveraines en ignorant la réglementation des marchés publiques, les expertises en protection des données, SSI et intelligence économique, pour écouter les évangélistes du numérique, lobbyistes juges et parties. Cette habile industrie a aussi identifié le maillon faible culturel et de gouvernance. Sa cible demeure la recherche, les brevets ainsi que les données de santé, fabuleux marché d'avenir.

↘ LA SSI DOIT ÊTRE HUMAINE ET ORGANISATIONNELLE DONC DE GOUVERNANCE[2]

L'état a émis des textes réglementaires pour protéger son patrimoine informationnel[3]. ANSSI et CNIL proposent un ensemble de documents et de formation[4], dont le remarquable « Maîtrise du risque numérique – l'atout confiance ». Le MESRI est doté d'un schéma directeur de la SSI depuis 2005. L'Etat s'est doté d'une politique de SSI en 2015. Le positionnement du RSSI est rappelé dans une fiche AQSSI/RSSI du HFDS du MESRI.

Pourquoi ces éléments stratégiques et organisationnels ne sont-ils pas pris en compte par la direction des établissements ? En effet, force est de constater que nous avons failli collectivement, gouvernance, tutelle, organismes et universités, à intégrer la gestion du risque numérique pour protéger un bien commun, le patrimoine informationnel de notre nation.

Concernant le « nuage non souverain », la CPU a reconnu un enjeu de souveraineté et la Cour des comptes a demandé une clarification de la position du ministère. Le 5 juillet 2021 le Premier Ministre a émis une circulaire « Cloud au Centre » en direction des ministres. Le 15 septembre 2021 le Directeur de la DINUM a émis une note en direction des secrétaires généraux des ministères.

Allons-nous de nouveau faillir collectivement en silos ou commencer à bâtir de façon transverse ?

1 | Le Monde, 20 avril 2021, « Les universités, cible de choix des hackeurs » par Eric Nunès

2 | « Si vous pensez que la technologie peut résoudre vos problèmes de sécurité alors vous n'avez rien compris aux problèmes ni à la technologie »
Bruce Schneier

3 | Tableau de l'ANSSI

4 | https://www.ssi.gouv.fr/administration/bonnes-pratiques/methodologie/

témoignage

1

auteur·e·s
Damien Sauveron, directeur de la Faculté des Sciences et Techniques (FST) et **Isabelle Rigbourg**, chargée de la communication, FST, Université de Limoges

1 | Copyright free photo by Cottonbro from Pexels

À l'université de Limoges, on cybersécure

Affiliée depuis 2021 à l'International Cyber Security Center of Excellence, l'université de Limoges conforte sa place de pionnière en matière de cyber sécurité et fait entrer la France dans la réflexion mondiale

L'Université de Limoges a rejoint le centre d'excellence international de cybersécurité en tant que membre affilié au mois de juin 2021. L'INCS-CoE (International Cyber Security Center of Excellence) travaille avec de nombreuses universités à travers le monde. Keith Mayes, vice-président de l'INCS-CoE « L'Université de Limoges est un atout pour INCS-CoE, en tant que pionnière de longue date dans l'éducation et la recherche liées à l'information et à la cybersécurité. » Le représentant de l'Université de Limoges au sein de l'INCS-CoE est le Doyen de la Faculté des Sciences et Techniques, Damien Sauveron.

L'Université de Limoges a été la première université française à proposer un Master en cryptographie et sécurité de l'information, en 1986. Au cours des trente-cinq années suivantes, elle a formé plusieurs milliers d'étudiants qui occupent aujourd'hui des postes clés dans le domaine de la cybersécurité au sein de diverses universités, organismes de recherche, ministères et entreprises. L'Université de Limoges est également reconnue pour l'excellence des recherches en cybersécurité menées au sein du laboratoire XLIM de l'université de Limoges. L'une des forces de son groupe de recherche est qu'il couvre un continuum allant de la théorie de l'information à la pratique.

[Citation d'Isabelle Klock-Fontanille, Présidente de l'Université de Limoges] *« Devenir Affiliate Member de INCS-CoE est non seulement une reconnaissance supplémentaire de l'excellence du laboratoire XLIM, et du rayonnement de l'Université de Limoges, mais surtout une chance d'asseoir encore davantage ses atouts en collaborant avec les meilleurs centres mondiaux. »*

La vision de l'INCS-CoE est de travailler ensemble dans un environnement multipartite au sein d'un partenariat gouvernement-industrie-université. Conscient du fait qu'un seul État ou qu'une seule organisation ne sera pas en mesure de relever les défis à lui seul, l'INCS-CoE a commencé par une coopération universitaire et se développe en une collaboration plus large entre le gouvernement, l'industrie et le monde universitaire. La collaboration internationale de l'INCS-CoE vise l'éducation, la recherche, la politique, les normes et la réglementation, les symposiums internationaux, les ateliers et les réunions.

[Citation de Professor Keith Mayes - vice-président de l'INCS-CoE et directeur de l'Information Security Group at Royal Holloway University of London] *« J'ai une expérience personnelle d'une très longue et productive collaboration entre le Smart Card and IoT Centre de la Royal Holloway University de Londres, et Damien Sauveron et son équipe. Je suis impatient d'étendre cette relation à l'INCS-CoE, puisque ses membres s'étendent désormais à la France. »*

Les nouveaux membres sont : University of Cambridge pour le Royaume-Uni, Edith Cowan University pour l'Australie, Université de Limoges pour la France, Technion Israel Institute of Technology pour l'Israël, Ben-Gurion University pour l'Israël.

CRYPTIS fête ses 35 ans.

Cette journée devrait réunir professionnels, chercheurs et étudiants (masters, doctorants) pour des discussions, échanges et conférences scientifiques autour de problématiques de cybersécurité, et en particulier, celles liées à la cryptographie et à la sécurité de l'information.

Informations à venir ici →

Plus d'informations

→ INCS-CoE
→ UFR Sciences et Techniques
→ Institut XLIM
→ Damien Sauveron

retour sur...

auteur
Département Stratégie et Programmation des SI, Amue

Webinaire « Numérique responsable » du CSIESR

Le CSIESR a organisé un webinaire, en partenariat avec le CRIP sur le sujet du numérique éco-responsable, souvent nommé green IT. Vous pouvez visionner ces 100 minutes sur cette page mais également lire ou relire la collection numérique « numérique responsable » de décembre 2020.

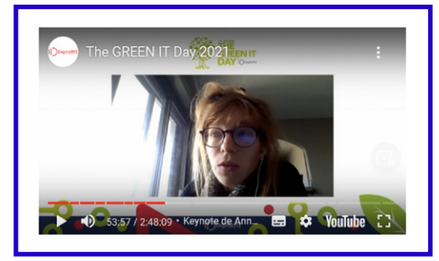
Politique des données

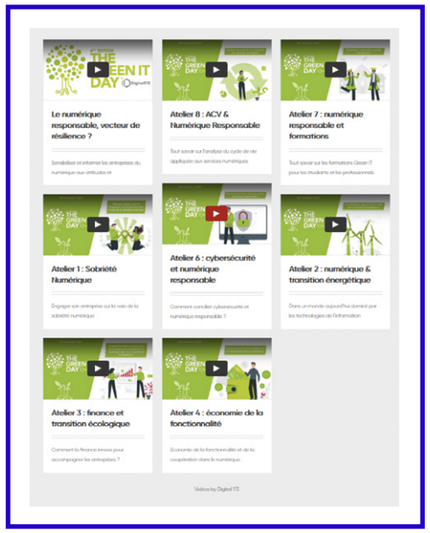
La feuille de route 2021-2024 relative à la politique des données, des algorithmes et des codes sources, élaborée par le ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation, est disponible depuis le 24 Septembre 2021. Elle fixe des enjeux et des objectifs, et met en place un plan d'actions à 4 ans en faveur de l'ouverture, du partage et de l'exploitation des données, des algorithmes et des codes sources de l'administration, de l'enseignement supérieur, de la recherche et de l'innovation.

L'occasion de lire ou relire les collections numériques N°05 - Open Data et ESR, opportunité de créer de nouveaux services, ***septembre 2019*** et N°06 - L'ESR vu par le prisme de la donnée universitaire, ***novembre 2019***

Green It Day

L'Amue contribue à nourrir la réflexion sur le numérique durable en participant au copil de l'évènement annuel « GREEN IT DAY » de Digital113, le cluster des entreprises et organisations du numérique en Occitanie dont elle est membre.





Le replay de la conférence d'introduction : https://thegreenitday.fr/sermons/

À l'heure où la propagation des virus chez l'homme est directement liée aux dérèglements des écosystèmes ; où certains portent un regard différent sur le numérique et ses usages en nous mettant en garde contre le miracle technique, les chercheurs et les chercheuses nous apportent leurs analyses éclairées. Comment penser la vie post-crise et la place du numérique ? Anne Alombert, Membre du CNNUM et enseignante-chercheuse en philosophie à l'Université Catholique de Lille, nous explique "comment les transformations numériques peuvent conduire à de nouvelles pratiques collectives et signifiantes, susceptibles de prendre soin des milieux, des corps, des esprits et des sociétés".

Et les replay des ateliers : https://thegreenitday.fr/sermons/ dont l'atelier 7 animé par l'Amue sur une problématique de formation initiale et continue. L'occasion de montrer à l'extérieur notre intérêt pour ce sujet porté en interne par Mutual'Lab Ecolo.

Assises du CSIESR

Toutes et tous heureux de se retrouver à proximité de l'Université de Côte d'Azur pendant 4 jours de travail, de communications orales, [dont certaines par l'Amue : PC-Scol, Open data/open source, Recherche et Rencontre avec votre référent DREM], et d'échanges de bonnes pratiques, dans le domaine de la stratégie, la donnée, l'architecture logicielle ou bien les solutions disponibles pour les universités.

C'était aussi l'occasion de fêter les 40 ans de cette institution des spécialistes du numérique universitaire, les *makers* de nos universités et établissements.

Un grand merci aux organisateurs.
Replay bientôt disponible
sur https://www.csiesr.eu/

grandes oreilles

auteur
Département Stratégie et Programmation des SI, Amue

Webinaire en ligne sur la SSI

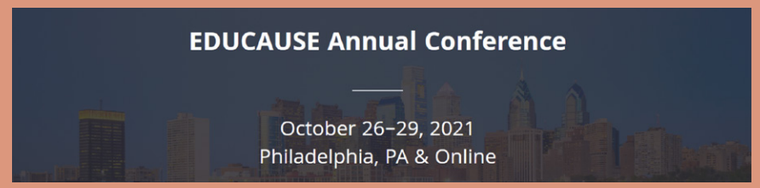
Et si vous étiez la cible de la prochaine cyberattaque ? L'université de Genève propose en amont de son master une conférence introductive en ligne (zoom) sur la SSI le 1er novembre 2021, 18:00 — 19:00

Educatec – Educatice

Le salon professionnel de l'innovation éducative se tient les 24, 25 et 26 Novembre à Paris Porte de Versailles.
Toutes les infos ici →

Prix science ouverte du logiciel libre de la recherche

Les prix, science ouverte données de la recherche et science ouverte logiciel libre de la recherche, sont inscrits dans le deuxième Plan national pour la science ouverte annoncé par la ministre de l'Enseignement supérieur, de la Recherche et de l'Innovation en juillet 2021. Ils récompenseront des initiatives emblématiques en la matière. Les prix seront remis début février 2022. Pour plus d'information, lire cette page → et la récente publication de l'ouverture des candidatures à lire ici →



Délégation française à la conférence annuelle d'EDUCAUSE

Cette année la délégation française suivra de nouveau à distance l'évènement nord-américain du numérique universitaire. Composée de membres d'Universités et d'établissements, du CSIESR, de la Cellule Logicielle, du CNAM, de l'Université numérique Paris Ile-de-France, de l'université de Nantes et de l'Amue, elle couvrira l'événement pour proposer un rapport annuel début 2022.

Le dernier rapport est disponible ici Téléchargez le rapport 2020 de la délégation, en français. (Téléchargez le rapport en haute définition)

Webinaires en Inter-Assos ANSTIA//CSIESR//CUME :

Une série d'actions est menée entre trois associations professionnelles l'ANSTIA, le CSIESR et le CUME dont le lancement a eu lieu le 8 Juillet 2021. Il s'agit de répondre au moyen de plusieurs webinaires à la question principale « Comment les transformations sociétales et numériques impactent-elles l'articulation entre nos différents métiers. Quelles organisations seront pérennes post crise sanitaire ? ». Plusieurs évènements à suivre durant l'année universitaire 2021-2022.

Liste des thèmes de l'année de la Collection Numérique

Pour que toutes et tous puissent se préparer à contribuer à ce travail collectif, nous avons publié les thèmes des prochains numéros 21/22 de la collection numérique. Données, bibliothèques universitaires, les différentes natures de veille, les schémas directeurs et les stratégies numériques, les usages, attendent vos propositions de partage et de retours d'expérience. Vous trouverez également les sujets de veilles prospectives pour lesquels vous pouvez apporter vos lumières : Intelligences artificielles, cloud, protection des usagers numériques, sobriété numérique,... A lire en détail ici →

Contact : numerique@amue.fr

#Auto-promo

Nous avions présenté à EUNIS 2021 cette collection numérique et comment nous travaillons avec vous pour la « fabriquer ». Et bien figurez-vous que l'article associé a été retenu et publié dans une revue internationale *EPiC Series in Computing* indexée sur Scopus.

Nous sommes très heureux et très honorés par cela. Ravis aussi d'avoir porté vos articles en ce lieu, merci à vous toutes et tous.

Mocquet, B., & Rongeat, D. (2021). La Collection Numérique : A way to (better) understand French HigherEd digital (pp. 38-49). *EPiC Series in Computing*, volume 78. ISSN: 2398-7340 https://doi.org/10.29007/sthb

octobre 2021

amue.fr

prochain numéro

Le numéro de décembre 2021 sera consacré à « Approche des organisations universitaires par le prisme de la donnée - Saison 2 »

103 bd Saint-Michel + 75005 Paris
Nos réseaux sociaux : @Amue_com