Former, informer, sensibiliser pour lutter contre les cyberattaques

Gérard PELIKS
Chargé de cours cybersécurité dans les écoles d'ingénieurs et instituts
Membre de l'ARCSI

La cybersécurité est une discipline qui s'apprend, qui se maintient, mais aussi qui se vit et se partage. Former les experts dans l'enseignement supérieur, puis en entreprise, maintenir leur compétence, sensibiliser l'ensemble des acteurs d'une organisation sont des conditions nécessaires, mais pas suffisantes pour diminuer les risques. Le reste est un travail quotidien pour ces experts et aussi pour l'ensemble du personnel.

Maillons faibles et piliers forts

On a coutume d'affirmer que le maillon faible de la chaîne de sécurité, sur laquelle repose la force de l'architecture globale qui protège une organisation visée par des cyberattaques[1], est situé entre votre chaise et votre clavier.

Pour les utilisateurs, c'est souvent le cas, mais ce n'est pas une fatalité si ces maillons font l'objet d'une sensibilisation aux dangers du cyberespace, avec l'appui de la direction générale. **Les experts en sécurité du numérique**, piliers de la chaîne de sécurité, doivent être correctement formés durant leur enseignement initial et entretenir leur compétence. Ils doivent connaître les attaques les plus récentes, les faiblesses de leur système d'information et aussi les métiers de leur organisation, car le besoin en sécurité d'un constructeur aéronautique n'est pas identique à celui d'une banque ou d'un site marchand. Les experts doivent évaluer le risque qui pèse sur l'information sensible de leur organisation, et le maintenir à un niveau connu, maîtrisé et « acceptable ».

Les experts, des piliers qui doivent être et rester forts

Les experts en cybersécurité doivent placer les contre-mesures indispensables, dans l'état de l'art de la cybersécurité, pour que le système d'information de leur organisation, surtout là où se trouve l'Information sensible, soit protégé contre les fuites, les destructions ou pire les compromissions. Et ces contre-mesures doivent évoluer en parallèle aux attaques de plus en plus sophistiquées, et tenir compte de la psychologie des attaquants. Cartographier l'Information de l'organisation est un préalable indispensable pour que les experts sachent où se trouve l'Information sensible qui devra demeurer disponible, intègre, confidentielle et traçable (le fameux DICT[2] de la cybersécurité). **Former ces experts par une formation initiale** est le rôle de l'enseignement supérieur et des organismes privés. Trouver ces experts encore trop rares sur le marché,

[1] Et toutes les organisations le sont.

[2] DICT : Disponibilité, Intégrité, Confidentialité, Traçabilité.

les embaucher et les retenir sont des problèmes que les organisations, grandes ou petites doivent résoudre. Ces experts doivent entretenir les connaissances acquises lors de leur formation initiale par une veille continue, appliquée aux métiers de l'organisation.

La formation des experts dans l'enseignement supérieur

Des écoles d'ingénieurs spécialisées dans l'enseignement des métiers du numérique, et aussi celles plus généralistes dans leur enseignement initial, mais qui présentent dans leur cursus une option en cybersécurité, des universités, des instituts, des IUT/DUT proposent des formations à la cybersécurité sur plusieurs semaines ou plusieurs mois. Au niveau BAC+5, les apprenants peuvent se diriger vers des masters en cybersécurité qui peuvent conduire à des activités de recherche ou des mastères spécialisés et MBA plus adaptés, après un stage professionnel, aux besoins immédiats des entreprises.

Les métiers de la sécurité du numérique sont très divers. Les formations initiales se différencient par la finalité de leurs spécialisations. Contrairement à certaines idées encore trop bien établies, la sécurité du numérique n'est pas une discipline purement technique. Il est aussi important de préciser que ces métiers peuvent être exercés par des hommes comme par des femmes encore trop peu nombreuses dans cet écosystème qui compte seulement 20 % de femmes, aujourd'hui. Les matières juridiques, l'intelligence économique, la veille technologique, l'enseignement, l'encadrement de projets et d'équipes entrent également dans les métiers de la cybersécurité.

Vers les métiers de la cybersécurité

Côté technique, si on vise une activité de développeur, les langages Python, Java, voire des langages plus proches du matériel, doivent être maîtrisés. Si on vise une activité de chasseur de failles (Bug Bounty) dans les logiciels ou de testeur de la solidité d'une architecture numérique (PenTest), les principes de la sécurité par conception et par défaut doivent être bien connus. Le développement d'algorithmes de chiffrement vous tente ? C'est une question de mathématiques, et bientôt aussi de physique quantique. Il y a les métiers d'architecte sécurité pour lesquels il faut connaître les éléments de base comme l'authentification forte, les coupe-feux, les réseaux privés virtuels, la cryptologie et bien d'autres outils. Mais empiler ces éléments ne suffit pas à constituer une architecture moderne de sécurité. Il y a les édifices à maîtriser comme l'IAM, le PCA, le DLP, le SIEM, le SOC[3].

Il y a également les exercices de simulation de cyberattaques menés en interne ou chez un formateur : une équipe rouge attaque et une équipe bleue défend. Cela permet de connaître les tactiques et stratégies d'un attaquant, et de se connaître soi-même. Comme l'a dit Sun Tzu, il y a 2 500 ans, dans l'art de la guerre : Connais ton ennemi et connais-toi toi-même ; eussiez-vous cent guerres à soutenir, cent fois vous serez victorieux.

Côté organisationnel, on trouve le juridique, comme les lois Godfrain qui sanctionnent l'intrusion et le maintien dans un système de traitement automatisé de données sans y être autorisé, et la perturbation de son fonctionnement. Il y a des règlements, comme le RGPD, des directives comme NIS, des normes comme celles de la famille des ISO27000 et des méthodes, comme eBios et Mehari. Il y a l'élaboration de contrats de sous-traitance, la création d'une charte de sécurité, et aussi la gestion de projets, parfois à gros budget, et la gestion d'équipes parfois avec beaucoup de ressources à animer. En effet, l'évolution d'un expert sécurité peut lui ouvrir des voies royales proches de la direction générale.

[3] IAM : gestion des identités et des permissions ; PCA : Plan de Continuité d'activité (dont la gestion de crise) ; DLP : Prévention contre la fuite de données ; SIEM : gestion des évènements de non-conformités, de vulnérabilités et de cyberattaques ; SOC : Tableau de bord de la sécurité·

Le label SecNumEdu, une garantie, mais pas indispensable

Certaines formations initiales de l'enseignement supérieur, pour les futurs experts en sécurité du numérique, peuvent prétendre au label SecNumEdu de l'ANSSI, décerné après étude d'un dossier assez complexe à constituer. Ce label est valable pour une durée de trois ans, à l'issue desquels une nouvelle demande de labellisation doit être soumise. Ces formations labellisées SecNumEdu sont référencées sur le site de l'ANSSI.

Beaucoup de formations à la cybersécurité qui n'ont pas ce label peuvent néanmoins être excellentes, mais n'ont pas fait l'objet d'une demande de labellisation ou ne cadrent pas exactement à la charte et aux critères définis par l'ANSSI.

L'enseignement supérieur couvre-t-il les besoins du pays ?

Malgré des progrès dus à la prise de conscience des dangers du cyberespace, suite à la multiplication des attaques et à leurs conséquences désastreuses et bien que le sujet soit devenu porteur, on ne trouve pas assez d'experts, immédiatement compétents, pour couvrir les besoins croissants des organisations. Les étudiantes et les étudiants hésitent-ils à se lancer dans cette discipline par manque de connaissances sur l'attrait des métiers de la cybersécurité ? Il y a certes un effort de visibilité à réaliser pour rendre ces enseignements et leurs débouchés plus visibles. Les universités restent souvent peu centrées sur le côté pratique des métiers. Les MBA et les mastères professionnels en temps partiel, une semaine par mois, ou deux jours par semaine en présentiel, et le reste du temps dans une organisation, avec un stage en entreprise donnant lieu à une soutenance, me semblent être une bonne formule.

Et l'enseignement supérieur dans la cybersécurité ne doit pas négliger les aspects non techniques comme le juridique, les normes et les standards, les règlements et directives, et la gestion de crise.

Entretenir son expertise

Une veille technologique dans cette discipline en constante évolution est indispensable. Les lettres d'information, les réseaux sociaux professionnels et les salons comme le FIC, à Lille chaque année en janvier, sont de bons moyens d'entretenir sa compétence. Les magazines comme Global Security Mag et Mag Securs apportent un éclairage et des avis d'experts. S'impliquer dans des associations comme le CyberCercle, le CESIN, le CLUSIF, le CEFCYS, l'ARCSI, permet d'entretenir ses compétences par l'apport de l'extérieur, et de partager les siennes. Dans la cybersécurité, vous ne serez jamais seuls si vous saisissez les occasions de côtoyer vos pairs.

Informer : la nécessaire sensibilisation de tous les acteurs

La sécurité de l'Information est l'affaire de tous les employés d'une organisation, et aussi des sous-traitants et autres partenaires. La chaîne de sécurité doit s'appuyer sur les piliers très solides que sont les experts en cybersécurité. Elle ne doit présenter aucun maillon faible que serait l'employé non sensibilisé, trop naïf, trop impulsif, et pas au courant, par exemple des dangers des hyperliens dans des pages web, et des fichiers attachés dans les courriels, pas au courant des menaces que présentent les clés USB que l'on ramasse sur son chemin, et des attaques en ingénierie sociale. Ajoutons les mots de passe trop faibles, ou complexes, mais écrits sur un Post it, l'hygiène informatique permet d'éviter ces vulnérabilités.

Sensibiliser l'ensemble des employés d'une organisation est une sage précaution pour diminuer les risques. Cette sensibilisation doit être appuyée par la direction générale, être souvent répétée et passe par **l'information de tous les employés**, à l'hygiène informatique.

Dis-le-moi et je l'oublie

Montre-le-moi et je le retiens

Implique-moi et je le comprends

Ce proverbe illustre un travail de sensibilisation du personnel d'une organisation, utile et efficace. Laisser traîner des clés USB dans les couloirs d'une entreprise, qui, une fois connectées sur un poste de travail, avertissent l'utilisateur qu'il vient de faire courir un danger potentiel à son organisation ; envoyer un mail, avec un contenu très bizarre et un fichier attaché ou un hyperlien qui conduit à un message d'alerte en cas d'ouverture du fichier ou de clic sur l'hyperlien, sont de bons moyens de susciter une méfiance salutaire face aux attaques en Ingénierie sociale. Il est indispensable que tous les employés comprennent qu'il faut se méfier du cyberespace.

Citons une campagne célèbre menée par Orange Business Services : un mémo promettait la gratuité pour un siècle sur la 6G illimitée aux premiers répondants qui devaient laisser leurs noms et leur date de naissance. Malgré les fautes d'orthographe bien sûr volontaires, malgré qu'il manquât le « a » dans le logo d'Orange, beaucoup se sont laissés prendre. On peut espérer qu'ils seront moins naïfs les fois suivantes, confrontés à des messages qui pourraient réellement être des débuts de menaces persistantes avancées, ou des tentatives d'hameçonnage ciblé.

Un dernier conseil, allez sur les MooC[4] qui permettent de monter en compétence, chacun à son rythme, comme celui de l'ANSSI[5] sur l'hygiène informatique, et celui de la CNIL[6] sur la protection des données à caractère personnel et la conformité au RGPD.

[4] Massive on line open Courses : cours en ligne, accessibles par un navigateur
[5] MooC de l'ANSSI : secnumacademie.gouv.fr
[6] MooC de la CNIL : https://atelier-rgpd.cnil.fr