DAVID CAUVIN, RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATIONS

Publié le 8 avril 2025

- **Présentez-vous ! Quel est votre rôle au sein de l'université de Rouen Normandie ?**

Je m'appelle David Cauvin et je suis le RSSI (responsable de la sécurité des systèmes d'informations) de l'URN depuis le 1er septembre 2024. D'une manière générale, le RSSI joue un rôle clé dans la protection du système d'information de l'Université. Il conseille la direction de l'établissement sur les risques numériques, veille à l'application de la politique de sécurité des systèmes d'information (PSSI) et s'assure de son évolution. Il sensibilise, forme et alerte la communauté universitaire face aux menaces cyber. Il assure également une veille technologique et réglementaire pour anticiper les évolutions nécessaires. Interlocuteur privilégié des directions métiers, des chefs de projets et des experts, il accompagne la mise en place de solutions sécurisées et coordonne la réponse aux incidents de sécurité.

- **Parlez-nous de votre parcours avant de devenir RSSI de l'URN.**

J'ai effectué un cursus universitaire à l'URN il y a plusieurs années, en sciences cognitives orienté IHM *(ndlr : interactions humain-machine)* apprentissage assisté par ordinateur et j'ai également une formation en ingénierie systèmes & réseaux télécoms. J'ai occupé différentes fonctions dans le secteur public (ministère des armées, centre hospitalier, communauté urbaine Caen La Mer, etc.) mais également dans la sphère privé (banque, France Télécoms & Orange, agence web, etc.). J'ai également fait plusieurs années de réserve militaire cyberdéfense au COMCYBER à Rennes et je suis passionné par mon métier.

- **Quels sont les prochains gros projets en termes de RSSI à l'URN ?**

Plusieurs projets de nature organisationnel et technique ont été identifiés. Il y a par exemple la mise en œuvre d'une PSSI (politique de sécurité des systèmes d'information) opérationnelle, le déploiement d'un EDR (end point detection response) qui permettra de détecter rapidement les menaces potentielles réduisant ainsi considérablement le risque de compromission, la généralisation de l'usage du MFA (authentification multi facteurs), le renforcement de la sécurité des laboratoires sensibles, ou encore le développement d'une culture de la sécurité. La liste est longue et certains projets sont assez dimensionnants.

- **Comment sensibilisez-vous les personnels et les étudiants aux enjeux de cybersécurité ?**

Il est prévu d'organiser sur le long terme des séances de sensibilisation à la sécurité des SI pour l'ensemble du personnel et des étudiants au travers par exemple d'ateliers, de vidéos pédagogiques, de quizz et/ou de formations e-learning, d'escape games, de simulation de phishing, etc. L'objectif est de développer une culture de la sécurité des SI. Nous sommes tous des utilisateurs et tout le monde aujourd'hui possède un ordinateur ou un smartphone, adopter les bons réflexes en matière de sécurité dans sa vie personnelle et professionnelle est aujourd'hui une nécessité, tant les menaces cyber sont présentes.

Des fiches réflexes ont été réalisées avec la collaboration de la Direction de la communication et sont disponibles sur le portail.

- **La cybersécurité représente-t-elle un défi au quotidien ?**

Oui, la cybersécurité est un défi quotidien car le risque zéro n'existe pas.
L'environnement universitaire est complexe et les enjeux sont multiples, notamment :

- **Un large périmètre à sécuriser** : l'URN gère un grand nombre d'utilisateurs (étudiants, enseignants, chercheurs, administratifs) et un parc informatique varié (postes de travail, serveurs, équipements réseau, etc.).
- **Une diversité d'usages** : entre l'enseignement, la recherche, l'administration et la collaboration avec des partenaires externes, les besoins sont nombreux et nécessitent une approche adaptée.

- **Des menaces en constante évolution** : phishing, ransomwares, attaques ciblées, fuites de données, etc. Les cybermenaces se sophistiquent et nécessitent une vigilance permanente. Le contexte géopolitique actuel ne fait que confirmer cette tendance.
- **Un équilibre entre sécurité et accessibilité** : l'URN doit garantir la protection des données et des systèmes tout en facilitant l'accès aux ressources numériques pour la communauté.
- **Une sensibilisation continue** : la cybersécurité est avant tout organisationnelle et elle repose principalement sur les utilisateurs, le respect des bonnes pratiques de sécurité. Former et responsabiliser chacun est essentiel pour réduire les risques, nous sommes tous des utilisateurs.

C'est pourquoi la cybersécurité est un défi quotidien qui demande une approche proactive, des outils adaptés et une implication de tous !

Publié le : 2025-04-08 15:47:25