INGÉNIEUR SÉCURITÉ

UN POSTE MULTIFONCTION À BOUT DE SOUFFLE

Avis d'expert par Sébastien Coll, Pentester - Lead Dev et Marius Vinaschi, Pentester - Dev backend chez PatrOwl

L'INGÉNIEUR SÉCURITÉ D'UNE PME, UN HOMME-ORCHESTRE

Dans l'idéal, un ingénieur sécurité d'entreprise devrait occuper ses journées à rechercher des solutions aux problèmes qu'il rencontre et à les mettre en œuvre. C'est un travail intellectuel de haute valeur, celui pour lequel il (et elle, dans une moindre mesure, encore et toujours malheureusement) a été formé et recruté.
Le métier se conçoit comme une succession de problématiques d'une extrême diversité, au point qu'une double, voire une triple casquette est requise : pentesteur, formateur, expert réseau, au moins, pour embrasser le plus largement possible le champ en expansion permanente du risque cyber. Mais encore ? Auteur et prescripteur des politiques de sauvegarde, gestionnaire des identités, souvent un peu développeur lui-même, etc., dans une PME, l'expertise ne se mesure pas au taux de réussite, mais à l'éventail de compétences parfois insoupçonné de l'ingénieur sécurité.

C'est peut-être aussi ce que l'on trouverait dans la description d'un poste à pourvoir, la recherche effrénée d'un mouton à cinq pattes sachant parler Python, Ruby, Perl, shell, powershell, ASM x86 et x64, C/C++, allemand et portugais (non essentiel), fin connaisseur des systèmes et du matériel, doté d'un sens aigu de la pédagogie. Et pourtant, cela ne ferait quand même pas le tour de l'immense parc d'attractions que visitent chaque jour les assaillants d'aujourd'hui.

FAIRE DES CHOIX RESTE UN MAUVAIS CHOIX

Il est toujours attendu des missions défensives d'un ingénieur qu'elles n'aient pas pour effet de freiner le travail des métiers et par extension leur potentiel effort de créativité. La sécurisation maximum des uns se heurte inévitablement au désir des autres de se libérer des contraintes, conduisant à percevoir les mesures de protection comme un poids, voire un obstacle à l'activité.

« Aujourd'hui cette priorisation naturelle fait apparaître de lourdes failles, ceci à tous les niveaux et contraint les organisations à accumuler des retards majeurs en prévention du risque, en formation et dans la mise en œuvre de solutions. »

À leur décharge, les entreprises ont toujours manqué de temps, de budget et de compétences, ceci depuis trop longtemps, pour travailler en parallèle sécurité et disponibilité de service, pourtant intimement liées.

D'ailleurs, si l'exemple d'une petite entreprise apparaît trop caricatural, rappelons qu'une entreprise de plus grande taille ne s'étoffe pas plus en personnel cybersécurité que les autres, malgré la présence d'équipes de développeurs par exemple dédiés à la création de produits numériques. Dès lors, la sécurité et ses problématiques se déclinent et ouvrent des perspectives de risques toujours plus béants.

L'OPTION AUTOMATISATION N'EN EST PLUS UNE

Compte tenu du coût d'un ingénieur sécurité, d'un processus de recrutement complexe, mais aussi d'un cadre réglementaire plus contraignant et de la pression de l'écosystème pour plus de sécurité, une stratégie efficace serait de dégager toujours plus de temps aux collaborateurs pour qu'ils se concentrent sur les missions qui ne peuvent pas être effectuées sans eux.

On pensera en particulier au rôle pédagogique qu'ils détiennent auprès des collaborateurs métiers pour mieux lutter contre les tentatives de phishing, mais aussi auprès des développeurs, pour qu'ils intègrent définitivement les bonnes pratiques de sécurité by design à leurs méthodes de travail. L'acquisition de compétences en la matière n'ira jamais de soi sans l'intervention répétée et musclée du RSSI et de son équipe, aussi indispensable que chronophage

L'un des axes sur lesquels l'entreprise peut agir en soulageant ses ingénieurs de tâches à la fois difficiles et rébarbatives repose sur l'ensemble des actifs que l'entreprise expose sur internet.

Bases de données, sites web, applications, API, serveurs, services, il est très courant que l'entreprise sécurise mal ses assets voire ignore tout simplement ce qu'elle expose, surtout si elle est sujette au shadow IT. Or, par définition, un serveur oublié n'est pas mis à jour et offre là une occasion en or de pénétrer les systèmes de l'entreprise. S'il s'agit du second vecteur d'attaques après l'ingénierie sociale par hameçonnage, c'est aussi le périmètre que l'automatisation de la surveillance couvre le mieux.

À défaut de pouvoir étoffer son équipe sécurité, c'est son outillage qu'il devient urgent d'enrichir. Les solutions automatisées n'ont pas que pour objectif de faire gagner un temps précieux. Elles affranchissent les collaborateurs de la charge d'activités si répétitives qu'elles provoquent lassitude et inattention. Rappelons, à tout hasard, qu'il sera toujours plus difficile pour un ingénieur de défendre un système entier que pour l'assaillant, de dénicher la vulnérabilité qui lui permettra de pénétrer le système.