LA CYBERSECURITE, ENJEU CRUCIAL DES ENTREPRISES, PETITES ET GRANDES !

CINOV-IT, institution représentative des TPE/PME du secteur numérique, participera au Forum International de la Cyber sécurité, les 24 et 25 janvier prochains. Par la présence de son 2e « village TPME » co-animé par deux auditeurs IHEDN notre syndicat souhaite rappeler l'importance de la cyber sécurité pour notre pays, les administrations et les entreprises, ainsi que la capacité de ses membres à répondre aux enjeux technologiques et organisationnels soulevés. Les deux exemples ci-après démontrent la mobilisation des acteurs du numérique et l'existence d'offres accessibles et pertinentes pour l'ensemble des entreprises.

Entretien avec Ely de Travieso fondateur de Bug Bounty Zone et référent National Cybersécutrité au sein du Cinov IT.

Ely de Travieso

Pourriez-vous nous présenter Bug Bounty Zone ?

Créée à Marseille, Bug Bounty Zone est une plateforme de service en recherche de vulnérabilités informatiques. Nous proposons à nos clients de pratiquer des audits de sécurité avec engagement de résultats, vous ne payez plus que les vulnérabilités. Pour ce faire, nous proposons que les recherches soient réalisées exclusivement par des sociétés reconnues dans les tests d'intrusion sachant que certaines sont également certifiées par l'Anssi. Chaque vulnérabilité remontée est commentée par un expert qui fournit des recommandations précises pour appliquer un patch de sécurité. Le service s'applique aussi bien aux réseaux informatiques qu'aux sites internet et permet à une entreprise de protéger ses données face aux hackers.

Pourquoi avoir créé cette plateforme ?

Après 15 ans d'expertise dans la cyber sécurité dédiée aux grands comptes, mes collaborateurs et moi-même avons commencé à nous intéresser aux PME et aux ETI. Nous avons alors remarqué qu'elles ne faisaient pas appel à des offres de cyber sécurité car ces dernières n'étaient pas adaptées à leur échelle d'un point de vue financier. De plus, aucune solution ne leur permettait de se concentrer uniquement sur les menaces essentielles. Or, contrairement aux grands comptes qui ont besoin de connaître l'ensemble des vulnérabilités de leurs systèmes informatiques, les PME-ETI, elles, doivent d'abord identifier les plus critiques. Face à ce constat, nous avons observé la création des premiers bug bounty aux Etats-Unis, une approche qui nous semblait impossible à réaliser sur le marché européen. Pour nous, il était avant tout essentiel de créer pour nos clients un service avec un niveau d'expertise égal à ceux proposés aux grands comptes. Pour ce faire, nous avons fait appel aux sociétés reconnues pour leur expertise et leur savoir-faire afin de réfléchir ensemble à la création d'un business model unique. Nous sommes aujourd'hui, les seuls à proposer une telle approche proposant un tel niveau d'expertise.

Qui sont vos clients ?

Nous avons deux types de clients, les grands comptes et les PME/ETI. Pour les clients grands comptes, le service est ouvert depuis le mois d'octobre. Nous avons déjà signé avec VOYAGE SNCF, la CMA CGM et JAGUAR NETWORK. De nombreux échanges sont actuellement en cours de discussion et 2017 devrait être une bonne année. Globalement, nous répondons aux attentes de toutes les entreprises qui s'appuient sur nous pour identifier des vulnérabilités critiques pour leur activité. Cela concerne aussi bien le e-commerce, l'industrie, que les métiers de services.

Vous présenterez en janvier 2017 au FIC votre offre, quelles sont vos attentes ?

Le FIC est un événement majeur regroupant un grand nombre de RSSI et il est pour nous important de présenter notre offre et de marquer notre positionnement. Un grand nombre de RSSI s'interrogent encore sur le bienfondé des bug bounty et nous espérons que notre niveau d'expertise leur permettra de franchir le cap sachant que nous leur offrons des conditions de réalisation rassurantes et professionnelles.

LA MENACE VIENT-ELLE DE L'INTERIEUR OU DE L'EXTERIEUR ?

Entretien avec Xavier Domecq, fondateur d'ID-Logism et auditeur INHESJ.

En quoi la demande de vos clients a-t-elle évolué depuis la création d'ID-Logism en 2006? Pourriez-vous nous décrire le contexte dans lequel s'inscrit aujourd'hui votre entreprise?

ID-Logism a été créée pour accompagner ses clients sur l'ensemble des sujets liés à la gestion d'identités (IAM) en dressant un inventaire des personnes qui se connectent au système d'information (collaborateurs ou partenaires) dans l'objectif de maîtriser l'ensemble de ces acteurs.

Petit à petit, la demande a évolué vers des questionnements davantage spécialisés sur les droits et les privilèges des personnes accédant au système d'information. Ces dernières sont en effet multiples et varient en fonction du type de clients. Depuis ces quatre dernières années, ces différentes thématiques nous ont conduit à la problématique du patrimoine informationnel : « Qui accède à ce patrimoine? Dans quel contexte? Comment prévenir les risques de pertes ou de fuites ? » Derrière ces questions se cachent des données plus ou moins sensibles à interpréter selon plusieurs points de vue. Aujourd'hui, on nous demande de réfléchir aux enjeux associés au big data, « nouvelle mine d'or » des entreprises. Nous proposons ainsi désormais une approche plus fonctionnelle et organisationnelle de la sécurité.

Notre activité a donc connu depuis dix ans une croissance régulière corrélée à notre capacité grandissante à accompagner nos clients dans la protection de leurs actifs les plus sensibles.

Comment êtes-vous organisés face à un nombre de données qui ne cesse de s'accroître?

Notre cœur de métier consiste à aider nos clients à identifier ce qu'est une donnée sensible et à apprendre à différencier une information critique d'une autre. Une information sensible se détermine par une approche par les risques : un risque de réputation, un risque concurrentiel, un risque règlementaire ou financier. Notre activité nous fait cotoyer régulièrement les différents métiers d'une entreprise. Nous sommes ainsi conscients de leurs spécificités ce qui nous permet d'apporter des réponses « sur-mesure » à leurs problématiques. Si une information fuit ou échappe à la maîtrise de l'entreprise, cela peut lui porter préjudice. Les données personnelles en sont un bon exemple. Ne pas maîtriser celles de vos clients ou de vos collaborateurs en interne, peut renvoyer une image peu favorable de l'entreprise et vous exposera prochainement à d'autres risques. En effet, une réglementation européenne RGPD (Règlement Général de la Protection des Données) entrera en vigueur en 2018 et imposera de lourdes sanctions aux entreprises « fautives » pouvant atteindre jusqu'à 4% du chiffre d'affaires réalisé. Il existe donc un double risque à la fois de mauvaise réputation mais aussi financier. Une donnée concurrentielle, un brevet, un savoir-faire, des taux commerciaux pratiqués etc. sont également des données qu'il convient de protéger. Typiquement les bonus entre traders sont des informations sensibles en interne d'une banque tout comme peuvent l'être les caractéristiques d'une pièce entrant dans la constitution d'un matériel militaire. Dans ce cas, nous ciblons l'information à protéger et établissons ensuite un niveau de protection.


Xavier Domecq

Comment se protéger?

La protection peut être de différente nature. Il existe d'abord le processus de manipulation de l'information appelé protection de la donnée en mouvement (qui peut y accéder ? dans quel cadre ? et l'utilité de cette donnée). Ensuite, on détermine sa zone de stockage (dans une application, un fichier informatique, un répertoire etc.) pour ensuite appliquer une politique de sécurité propre. Puis, des éléments de surveillance sont mis en place afin de vérifier que la donnée ne sorte pas par mail et ne transite pas d'un espace à l'autre etc. Tout un arsenal fonctionnel et organisationnel est donc engagé en plus d'un outillage informatique capable de contrôler le bon fonctionnement du processus.