La cybersécurité se construit dans un écosystème

L'année 2020 et la crise sanitaire a montré à quel point le monde était interconnecté. Un unique virus s'est propagé dans le monde entier, les hôpitaux et systèmes de santé ont été submergés de par le monde… et les pirates informatiques ont profité du chaos pour lancer des attaques dans tous les pays, sans distinctions géographiques ni linguistiques.

La période a également été propice aux cyber-attaques du fait de la généralisation du télétravail. Premièrement, la distance entre un employé et le système informatique auquel il accède multiplie les points d'attaque possible pour les attaquants. Par exemple, un ordinateur personnel n'est pas forcément aussi sécurisé qu'un ordinateur professionnel, le WiFi de la maison peut être moins robuste que la connexion internet dans les locaux de l'entreprise…

En second lieu, les employés ont tendance à être plus détendus lorsqu'ils travaillent depuis chez eux, à faire l'impasse sur certaines bonnes pratiques en matière de cybersécurité simplement parce qu'ils ne pensent pas au danger depuis le confort de leur maison.

Enfin, et cette tendance était déjà clairement présente avant la crise sanitaire, l'informatique s'étend à tous les aspects de notre vie, elle devient incontournable. Cela rend les bénéfices potentiels d'autant plus attrayants pour les pirates.

Pris ensemble, ces trois aspects multiplient le risque d'intrusion dans les systèmes informatiques par des hackers.

A cette évolution mondiale a répondu une communauté de fait internationale : celle des pirates.

Les outils – malwares, spywares, ransomwares, etc – qu'ils construisent ou dérobent sont échangés, vendus voire donnés sur le dark web. Lorsqu'une vulnérabilité a été trouvée par un acteur malveillant, celui-ci peut se la mettre de côté pour l'exploiter seul sur la durée, ou bien il peut décider de la partager avec son réseau.

Les acteurs soutenus par des agents étatiques vont encore plus loin : ils sont mieux organisés, disposent de ressources importantes et des outils les plus sophistiqués. Mais il n'est pas nécessaire d'être soutenu par un Etat pour être dangereux. Il est assez facile de télécharger un kit de virus prêt à être envoyé à sa cible même sans compétences particulières. Le résultat est une diversification du paysage de la menace sur le plan horizontal et une sophistication des attaques les plus poussées sur le plan vertical.

Une communauté dédiée à la cybersécurité

Fort heureusement, la communauté de la cybersécurité s'organise en conséquence.
Entre le CISA (Cybersecurity and Infrastructure Security Agency) américain, l'ANSSI française et leurs homologues dans la plupart des pays, une entreprise où qu'elle soit peut s'appuyer sur des informations de qualité pour orienter sa stratégie de sécurité et avoir connaissance des menaces

du moment.

Ces autorités organisent des webinars réguliers pour aider les entreprises à mettre sur pied une stratégie de cyberdéfense fiable, publient des bulletins sur les dernières vulnérabilités détectées et le modus operandi de certaines attaques, et accompagnent les experts en cybersécurité dans leur travail.

Ces autorités sont un partenaire essentiel pour toutes les entreprises, qui peuvent bénéficier de leurs services selon leurs besoins : les PME pour avoir un résumé du paysage de la menace pertinent pour leur secteur et qui tienne compte des limites de leurs ressources, les grandes entreprises pour avoir des informations plus détaillées et exhaustives avec les signaux faibles à analyser.

Cependant, ces acteurs paient le prix de la rigueur et de la fiabilité de leurs informations par le retard qu'ils ont souvent dans la diffusion de leurs informations.

L'importance de la communauté informelle

Pour pallier ce manque, les experts en cybersécurité ont aussi organisé des communautés informelles, comme par exemple des groupes sur LinkedIn. Ces groupes sont un lieu d'échange, de partage de bonnes pratiques – et de demandes d'aide lorsque des difficultés sont rencontrées. Prenons un exemple édifiant datant de l'année dernière, au plus fort de la crise sanitaire.

Plusieurs hôpitaux américains ont été infectés par un malware. Les agences fédérales et nationales dédiées à la cybersécurité avaient mal jugé le risque que posait ce malware, et n'avaient en conséquence pas informé les hôpitaux en amont de ce risque. Ils n'étaient donc pas armés pour se protéger contre ce virus qui les a infectés les uns après les autres.

Les DSI des hôpitaux ont dû faire appel à leurs propres ressources pour détecter les virus, protéger leurs terminaux et éliminer le virus. Il s'est d'ailleurs avéré que les mesures les plus simples, comme ne pas partager d'emails dont l'origine n'est pas sûre, ont été parmi les plus efficaces.

Ce qui est intéressant est que les DSI ont partagé entre eux ce qui marchait et ce qui ne marchait pas ; en l'absence d'aide en provenance des agences spécialisées, ils ont formé un réseau *ad hoc* pour trouver des solutions, avec une démarche de test & learn, et faire face à cette attaque.

L'année dernière a montré l'interconnexion du monde à plus d'un égard. Les pirates comme les experts en cybersécurité forment des communautés en partageant des informations, outils et conseils. Du côté des défenseurs, les DSI peuvent s'appuyer sur deux types d'organisations : formelles avec les autorités publiques et informelles grâce à leurs réseaux.