2022 Vulnerability Intelligence Report : les points à retenir

Aujourd'hui, le paysage des menaces est radicalement différent de ce qu'il était il y a seulement cinq ans L'écosystème florissant de la cybercriminalité est complexe, diversifié et toujours profitable aux attaquants aux dépens des entreprises mondiales. Les groupes de ransomware et les courtiers en accès initial se sont joints aux opérateurs de botnet et aux acteurs malveillants parrainés par des États-nations pour développer une économie de la cybercriminalité, dont les tactiques et les cibles de grande envergure ne laissent pratiquement aucune organisation indemne, indépendamment de sa taille ou de son secteur d'activité.

Un climat de menace élevé et persistant

- L'année 2021 a marqué un record historique en ce qui concerne la vitesse et l'échelle des cybermenaces, avec des exploits de masse survenant tous les 11 jours en moyenne. L'année 2022 a connu un léger fléchissement des exploits zero-day et des « flambées » de piratages massifs, mais dans l'ensemble, la tendance pluriannuelle à l'augmentation de la vitesse et de l'échelle des attaques reste remarquablement constante.
- En raison de l'évolution du mode opératoire des cybercriminels et du comportement des attaquants, nous prévoyons de légères fluctuations dans les macro-tendances d'une année sur l'autre. Si ces fluctuations donnent lieu à une analyse nuancée concernant les adversaires et leurs motivations, il est peu probable qu'elles contribuent à tempérer le climat de risque élevé persistant pour les entreprises mondiales.

Dans bien des cas, les opérations de cybermenaces bien rodées distancent les équipes de sécurité

- Nous constatons toujours que l'intervalle entre la découverte de nouvelles vulnérabilités et leur exploitation dans des attaques s'amenuise. En 2022, 56 % des failles indiquées dans notre rapport ont été exploitées dans les sept jours suivant leur découverte, et plus de 40 % des attaques généralisées ont commencé par un exploit zero-day. Cela signifie que les équipes de sécurité disposent d'un délai de plus en plus court, voire inexistant, pour corriger les nouvelles vulnérabilités et contrer les attaques. Cette tendance met à rude épreuve les ressources de sécurité déjà très sollicitées d'un grand nombre d'organisations.
- Le fait de disposer d'une procédure de correctifs d'urgence bien élaborée ainsi que d'une solide stratégie d'intervention en cas d'incident peut s'avérer avantageux. Toutefois, les équipes qui peinent à trouver des ressources pour les activités de base de leur programme de sécurité ne peuvent raisonnablement pas mettre en place des procédures d'urgence optimales. Les équipes de sécurité doivent pouvoir mettre en œuvre les bases d'un programme robuste, notamment des pratiques proactives de gestion des actifs et des vulnérabilités, afin de pouvoir réagir efficacement à une crise.

L'efficacité de la technologie repose sur les compétences

- L'adoption du cloud se développe et les piles technologiques deviennent de plus en plus complexes, ce qui étend la surface d'attaque disponible et offre aux adversaires davantage de moyens de compromettre les réseaux d'entreprise. En matière de sécurité, les solutions technologiques sont une composante essentielle, quelle que soit l'approche adoptée par les organisations. Mais

en plus des outils qui offrent une visibilité et une protection sur l'ensemble de l'architecture cloud et sur site d'une société, la lutte et la prévention contre les cybermenaces modernes nécessitent presque toujours un savoir-faire humain. Les dirigeants ne peuvent pas se contenter de miser sur une solution technologique pour faire face aux attaques complexes : ils doivent évaluer la capacité de leur organisation à mettre en œuvre un framework de sécurité qui détecte et stoppe les adversaires les plus déterminés.

Conseils aux cadres dirigeants et aux membres du conseil d'administration

- Dans le paysage actuel des menaces, les équipes sont souvent contraintes d'adopter des postures réactives, ce qui réduit l'efficacité et la durabilité des programmes de sécurité. Les membres du conseil d'administration et les cadres dirigeants gagnent à avoir une visibilité sur les difficultés auxquelles font face ces initiatives et sur l'impact potentiel de leur détérioration.
- Les conditions macroéconomiques difficiles de 2022 et 2023 ont accentué la pression que subissent les équipes de gestion des risques, qui cherchent à gagner en efficacité sans compromettre l'intégrité des données sensibles ou des opérations métier. Dans un climat macroéconomique instable, les contraintes permanentes en matière de ressources peuvent entraîner une accumulation de risques cachés et une perte des compétences techniques nécessaires pour garantir l'efficacité des opérations de sécurité, et notamment la capacité à intervenir en urgence en cas d'incident.
- Outre la nature de plus en plus envahissante des menaces en matière de sécurité, les cadres dirigeants doivent être conscients de l'omniprésence des attaques, tant sophistiquées qu'ordinaires, sur les réseaux d'entreprise. Les indicateurs de sécurité et les modèles de risques organisationnels doivent s'appuyer sur le contexte commercial et être intégrés dans des activités de planification stratégique plus étendues. Idéalement, la sécurité devrait être considérée comme une responsabilité pour l'ensemble de l'entreprise et ne pas dépendre uniquement de départements fonctionnels isolés.
- Pour que les risques soient acceptables, ils doivent être clairement définis. Les membres du conseil d'administration et de la direction doivent comprendre, et pouvoir expliquer, la façon dont les contraintes concernant les ressources des programmes de sécurité et l'environnement réel des menaces affectent la continuité des opérations métier, notamment la confidentialité de la propriété intellectuelle ainsi que l'intégrité des données sensibles et des chaînes d'approvisionnement. Pour les conseils d'administration et la direction, il est totalement logique de tenir compte du risque dans leur prise de décision, pour autant qu'il soit contextualisé et explicite.