Cybersécurité : 5 points à retenir du rapport IBM X-Force

IBM Security a livré son rapport 2020* sur les menaces mondiales de cybersécurité repérées ces douze derniers mois (« IBM X-Force Threat Intelligence Index »).

Pour Wendi Whitmore, vice-présidente d'IBM X-Force Threat Intelligence, « le volume de dossiers exposés est tel » que, pour opérer, les attaquants peuvent s'appuyer sur des ressources déjà à leur disposition, des identifiants volés par exemple, plutôt que d'investir.

Les entreprises ont donc intérêt à renforcer leur protection, « par le biais de l'authentification multifacteur » notamment, pour leur cyber-résilience et celle des données utilisateurs.

Record, malware, finance, ingénierie sociale et industrie 4.0

Voici 5 des principaux éléments à retenir de ce rapport :

1. Un mauvais record
Plus de 8,5 milliards de dossiers (*records* en anglais) ont été compromis et signalés en 2019. Ce chiffre a augmenté de plus de 200% par rapport à 2018.

Parmi eux, plus de 7 milliards de dossiers ont été exposés du fait de serveurs mal configurés (dans le cloud y compris), soit 86% des signalements, contre moins de 50% l'an dernier.

2. Malwares et ransomwares
L'utilisation de logiciels malveillants (malwares) fluctue. Les rançongiciels (ransomwares), les cryptomineurs et les botnets ont chacun dominé le paysage à différents moments de l'année 2019, ont souligné les chercheurs en sécurité d'IBM.

Les programmes « destructeurs » ont la capacité de rendre les systèmes touchés inutilisables et de compromettre leur relance. Ces outils sont utilisés à la fois par des pirates informatiques non affiliés à des gouvernements et par des acteurs soutenus par des États.

IBM X-Force IRIS estime qu'une « attaque par malware destructeur coûte en moyenne 239 millions de dollars par multinationale touchée, soit plus de 60 fois plus que le coût moyen d'une violation de données (Ponemon Institute) », ont ajouté les auteurs du rapport.

3. Phishing (ou hameçonnage)
Le phishing (31%), qui consiste pour un fraudeur à se faire passer pour un tiers de confiance dans le but d'obtenir des données sensibles, reste le principal vecteur d'attaque observé par X-Force IRIS (Incident Response and Intelligence Services) en 2019. L'analyse et l'exploitation des vulnérabilités (30%), puis les identifiants volés (29%) suivent de près.

4. Finance ciblée

Le secteur des services financiers est toujours le plus ciblé par les commanditaires de cyberattaques. Commerce (retail), transports, médias, services professionnels, administration (gouvernement), éducation, production, énergie et soins de santé font également partie du top 10 des secteurs les plus exposés. Plus largement, l'Internet des objets (IoT) et l'industrie sont dans la ligne de mire des attaquants.

5. ICS/OT

Selon les données d'IBM X-Force, les tentatives d'attaques ciblant les systèmes de contrôle industriels (ICS) et les technologies opérationnelles (OT) associées ont augmenté de 2000% en 2019 par rapport à 2018. La sécurité des systèmes industriels a besoin de talents.

La tendance devrait se confirmer en 2020 et au-delà.

*Le rapport d'IBM s'appuie sur l'analyse du suivi de 70 milliards d'événements de sécurité par jour dans plus de 130 pays.

(crédit photo © IBM)