5 grandes évolutions pour la cybersécurité en 2019

Attaques d'extorsion ciblant les infrastructures industrielles (OT) /IIoT

Prévision : les infrastructures stratégiques seront perturbées par une attaque d'extorsion de grande envergure.

Nous avons déjà observé des attaques de type extorsion lancées sur des infrastructures telles que des villes ou des ports. Tout laisse à croire que ce type d'attaque va non seulement se poursuivre, mais aussi s'étendre aux infrastructures d'énergie et de transport. À l'heure de l'Internet industriel des objets (IIoT, *Industrial Internet of Things*), le secteur industriel est en passe de devenir une nouvelle cible. Les pirates ciblant les entreprises ont de plus en plus recours à des pratiques d'extorsion.
Dans ce contexte, les cibles potentielles quasiment illimitées ne sont qu'un moyen de parvenir à des fins financières. Au cours de l'année 2019, l'une de ces attaques provoquera, quelque part sur la planète, des bouleversements mémorables.

Intelligence artificielle : le risque des malwares

Prévision : les malwares basés sur l'intelligence artificielle (IA) échapperont au périmètre de leur cible visée avec des conséquences dévastatrices.

Un développeur de logiciels malveillants ayant recours au ciblage d'apprentissage automatique et/ou à l'auto-propagation pourrait créer une souche tellement performante qu'elle risquerait d' « échapper » au périmètre défini de sa cible, provoquant ainsi d'immenses dommages collatéraux. L'emploi de l'intelligence artificielle dans un événement de ce type sera susceptible d'amplifier les retombées de ce que l'on a déjà pu observer avec Stuxnet, Mirai ou encore NotPetya.
En outre, on assistera pour la première fois à une cyberattaque intégrant l'apprentissage automatique pour automatiser des techniques de piratage manuelles, habituellement uniquement associées à des menaces APT.
Pour constituer un contrepoids et combler le déficit de compétences en matière de cybersécurité, les centres d'opérations de sécurité (SOC, Security Operation Center) vont commencer à utiliser des algorithmes d'intelligence artificielle et d'apprentissage automatique. Les analystes de sécurité auront pour mission de s'adapter à leurs nouveaux collègues artificiels.

Vers une réglementation des crypto-monnaies

Prévision : les législateurs vont perdre patience au sujet des crypto-monnaies

La Blockchain représente un risque à court terme, en raison de son immaturité technologique et de sa forte dépendance au sort des crypto-monnaies. La réussite de cette technologie dans des secteurs tels que la sécurité de la chaîne logistique nécessite de parvenir à un certain stade de maturité. À mesure que l'utilisation des crypto-monnaies de la Blockchain se généralise, les craintes d'attaques à visée géopolitique sur ces monnaies vont s'intensifier. C'est la raison pour laquelle ces dernières vont subir des contrôles accrus, destinés à atténuer le risque économique, dans un contexte d'échanges croissants sur les marchés conventionnels.
De façon plus générale, la confiance dans la Blockchain va fléchir. En effet, les préoccupations

relatives aux problèmes de cybersécurité rencontrés avec les crypto-monnaies augmentent, et l'on se rend bien compte que la Blockchain ne constitue pas une panacée.

Le premier traité international sur la cybersécurité

Prévision : deux cyber-puissances vont entamer des négociations pour élaborer le premier traité international sur la cybersécurité

La population est exposée à un risque accru de blessures causées par une attaque (intentionnelle ou accidentelle) menée sur des infrastructures stratégiques telles que des centrales ou des hôpitaux. Pour faire face à ce type de menace, nombre d'idées ont été formulées. Microsoft plaide notamment pour l'adoption d'une Convention de Genève numérique, et appelle à la création d'une ONG indépendante, baptisée « Global Cyber Attribution Consortium », dont l'objectif consisterait à contrôler le respect des exigences de conformité. Il faudra sans doute attendre plusieurs années avant que cette initiative et d'autres initiatives prises par les Nations Unies voient le jour. Cependant, le rapport risque/récompense bascule lentement mais sûrement en faveur d'un système de règles, au moins pour un petit nombre de pays, surtout s'il est possible d'en tirer des avantages géopolitiques reflétés par les relations économiques et militaires entre les pays. Un traité formel de cybersécurité de ce type reposerait donc autant sur son capital politique et symbolique que sur ses détails techniques.

Vers une interdiction des rançons

Prévision : un gouvernement local bannira le paiement de rançons dans le secteur public

En cas d'attaque par extorsion, le paiement de rançons par des organisations du secteur public pour récupérer l'accès à leurs systèmes stratégiques est devenu monnaie courante. Cette pratique a toujours été sujette à polémique, et les règles régissant sa légalité sont complexes, même dans les pays disposant de systèmes judiciaires très développés. Les gouvernements commencent à payer le prix de cette vision à court terme. En effet, non seulement le paiement d'une rançon risque de financer de nouvelles attaques, mais en plus il n'offre aucune garantie que l'attaque ne se reproduira pas. Quant aux montants des rançons, ils ont été multipliés par dix. Les attaquants s'intéressent à présent aux infrastructures stratégiques. Or il s'agit là d'une évolution dangereuse. L'interdiction du paiement de rançons pourrait dissuader les attaques par extorsion et inciter les acteurs concernés à investir dans des solutions de sécurité conçues pour éviter que ces situations ne se produisent.