EN QUOI LA CRISE DU CORONAVIRUS A-T-ELLE ÉTÉ UN ACCÉLÉRATEUR DE LA CYBERCRIMINALITÉ ?

3 questions à Tiago Dias, Consultant EMEA, Cyber Hazards

Depuis le début de l'année, deux tendances significatives de la cybercriminalité ont été observées : d'une part, une monétisation croissante par les cybercriminels de leurs attaques, notamment par le biais de logiciels de rançon ; d'autre part, une augmentation des cyber-risques liés à la pandémie mondiale de Covid-19. Face à cela, quelle approche de la cybersécurité devrait être adoptée afin d'atténuer ces menaces ? Quelques éléments de réponse avec notre consultant en cyber sécurité, Tiago Dias.

Quelles ont été les pertes causées par la cybercriminalité depuis le début de la crise et doit-on s'en inquiéter ?

Tiago Dias – Certains exemples récents de ce qu'on appelle des « cyberpertes » sont particulièrement préoccupants, et montrent que les attaques informatiques entraînent de plus en plus de pertes financières et autres perturbations bien au-delà des réseaux informatiques touchés. Deux exemples permettent de le démontrer :

Début janvier, un employé d'une entreprise gazière américaine a téléchargé par inadvertance un logiciel malveillant sur son ordinateur en cliquant sur un lien figurant dans un courriel de phishing. Mal préparé, l'opérateur gazier a été contraint d'arrêter toutes les activités sur son site et dans tout son réseau pendant deux jours, le logiciel malveillant ayant provoqué une rupture dans la chaîne de traitement du gaz*.

Plus récemment, dans la nuit du 15 au 16 juillet, Twitter a subi l'une des plus grandes cyber-attaques de son histoire. Des dizaines de comptes parmi les plus populaires de la plateforme ont été compromis, puisque des cybercriminels ont utilisé leur accès pour extorquer des dizaines de milliers de dollars par le biais d'une escroquerie au Bitcoin.

Ces deux exemples ne sont que l'arbre qui cache la forêt. En effet, la monétisation du piratage est devenue une tendance de la cybercriminalité. En outre, ces attaques n'auraient pas pu prospérer sans un contexte qui a grandement contribué à la vulnérabilité des réseaux informatiques, à savoir la crise du coronavirus.

Pourquoi les attaques se sont multipliées avec la pandémie ?

TD – Outre une catastrophe sanitaire, la crise du coronavirus a été un véritable catalyseur de la cybercriminalité. Le recours massif au télétravail a mis à rude épreuve les équipes de sécurité informatique des entreprises à tous les niveaux. Avec l'augmentation drastique du nombre d'employés travaillant à distance, les entreprises ont dû veiller à ne pas exposer leurs systèmes critiques en s'appuyant sur des équipes de sécurité internes, des fournisseurs ou des experts tiers. Toutefois, cette stratégie n'a pas toujours été couronnée de succès.

FM Global

Dans ce contexte, la pandémie de Covid-19 a directement influencé le modus operandi des cybercriminels, tout en accélérant considérablement le rythme des attaques. D'après les résultats d'une étude Cequence Security publiée en mai 2020, le trafic malveillant hebdomadaire a augmenté de plus de 270 %** à la fin du mois d'avril, alors que les mesures de confinement de la pandémie étaient toujours en place. Les cyberattaques liées au Covid ont même atteint un pic en mai ; les structures déjà sous la pression du fait de la pandémie, telles que les hôpitaux et les centres de recherche sur le coronavirus, ont été les plus exposées.

C'est sur ce terrain fertile que le phishing a pu émerger. Sans modération, les cybercriminels se sont nourris de la psychose ambiante à l'égard de la pandémie mondiale actuelle pour raviver la menace du phishing, qui préoccupait déjà les entreprises et leurs utilisateurs en temps « normal ». En conséquence, les courriels et les appels téléphoniques se faisant passer pour l'OMS, une autorité gouvernementale ou des entreprises légitimes ont été légion ces derniers mois. Dans ce contexte, face à ce cyber-environnement de plus en plus incertain, comment pouvons-nous nous protéger ?

Quelle est donc la meilleure approche à adopter par les entreprises contre ces cyber-risques ?

TD – Chez FM Global, la résilience est le maître-mot de notre philosophie. Et nous sommes convaincus que l'appliquer aux problématiques cybercriminelles est la meilleure des approches, car mieux vaut prévenir que guérir.

Rappelons tout d'abord que la plupart des pertes sont souvent évitables. Dans un environnement informatique de plus en plus complexe et truffé de pièges, il est donc impératif d'adopter des approches proactives et plus intégrées afin de consolider les systèmes, les réseaux et les logiciels à la source. En d'autres termes, la « cyber sécurité » doit être synonyme de « résilience » et de « sécurité par défaut ».

C'est l'essence même de ce qu'on appelle « approche holistique de la cyber sécurité », qui consiste non seulement à assurer la sécurité de l'architecture du réseau une fois qu'elle est attaquée, mais aussi à renforcer la cyber-résistance des infrastructures utilisées.

Contrairement à une approche traditionnelle, cette stratégie globale exige une connaissance approfondie de la gestion de l'entreprise et de son paysage de risques. Elle nécessite également une hiérarchisation des risques et de leur traitement, ainsi qu'un décloisonnement des différentes entités fonctionnelles qui limitent la collaboration entre les équipes et donc la lutte contre les attaques informatiques qui n'ont que faire de ces frontières. L'objectif est de mieux impliquer les différentes équipes techniques tout en faisant de la cyber sécurité un vecteur d'innovation plutôt qu'une simple arme de dissuasion.

* Source : CISA – Février 2020 : https://us-cert.cisa.gov/ncas/alerts/aa20-049a

** Source : Étude Cequence Security – Mai 2020 : https://www.cequence.ai/blog/tales-from-the-front-lines-attackers-on-lockdown-focus-on-apis/