JAN KERKHOFS ET PHILIPPE VAN LINTHOUT, À PROPOS DE LA CYBERCRIMINALITÉ

UNE CYBERATTAQUE ? PAS DANS MON ENTREPRISE !

La cybercriminalité est la forme de criminalité qui croît le plus vite à l'ère numérique. « Pas dans mon entreprise ! » pensez-vous ? C'est ce que pensaient de nombreux chefs d'entreprise jusqu'à ce qu'ils soient victimes d'une cyberattaque. Deux experts judiciaires qui combattent la cybercriminalité au quotidien vous expliquent le business model des criminels. Leur conseil ? Soyez sur vos gardes et préparez-vous.

Jan Kerkhofs est magistrat fédéral auprès de la Cyber Unit du parquet fédéral et Philippe Van Linthout est juge d'instruction à Malines. Tous deux font autorité en Belgique dans le domaine de la cybercriminalité. La tendance la plus marquante de cette forme de criminalité en croissance rapide est le professionnalisme. « La cybercriminalité n'est plus le fait de personnes isolées dans leur grenier, elle s'est professionnalisée en un business model solide et mondialisé », explique Ph. Van Linthout. « Les cybercriminels sont des entreprises qui ont leurs propres produits – y compris un helpdesk (!). Ils ne cherchent pas à concurrencer vos produits ou services, mais plutôt à gagner de l'argent en sapant vos activités ou en soutirant des fonds. » Tout est à vendre sur le darkweb. Un hacker peut y trouver des bases de données de courrier électronique, des logiciels malveillants ou même une liste spécifique d'entreprises vulnérables dans un secteur déterminé. « Mais vos propres collaborateurs représentent aussi un risque. Une personne qui s'estime traitée injustement peut s'en aller avec les secrets commerciaux ou la comptabilité noire. »

EFFETS PERVERS

De nombreuses entreprises semblent prêtes à payer, en dépit de tous les conseils. Cela donne aux criminels la possibilité d'aller encore plus loin. « Les cybercriminels sont même prêts à exiger une lettre de référence afin de démontrer à la prochaine victime qu'ils ont effectivement aidé votre entreprise à se remettre sur pied après un blocage ou un piratage de votre système », a constaté Kerkhofs dans ses dossiers. De nombreuses entreprises essaient de s'assurer contre les demandes de rançon et, de cette manière, elles entretiennent la criminalité. « De plus, vous ne pouvez jamais être sûr que le criminel ne laisse pas un accès ouvert pour une attaque ultérieure ou pour vendre cet accès à un tiers. »

Selon Ph. Van Linthout, toutes les attaques ne visent pas à extorquer ou à voler de l'argent. Une Advanced Persistent Threat (APT) est une attaque par laquelle un cybercriminel obtient un accès à long terme et invisible dans une organisation. Bien souvent, l'entreprise ou l'autorité visée ne sait pas qu'elle est piratée. « L'enjeu est un espionnage d'entreprise persistant ou l'accès au réseau d'autres organisations. »

SI VOUS LAISSEZ VOTRE PORTE D'ENTRÉE OUVERTE…

J. Kerkhofs considère que la fonction de Chief Information Security Officer est un des métiers les plus pénibles. « Ce responsable doit réunir un budget pour construire un bouclier contre une attaque qui n'a jamais frappé auparavant. Souvent, le comité de direction n'a aucune connaissance de la configuration informatique et encore moins de ses faiblesses. Trop d'entreprises investissent encore trop peu dans une base de sécurité solide. » Il devrait être normal d'avoir un système qui détecte automatiquement les activités suspectes, les exportations anormales de données…

« LA PRÉPARATION FAIT LA DIFFÉRENCE ENTRE UN INCENDIE OU UN DÉTECTEUR DE FUMÉE »

JAN KERKHOFS, MAGISTRAT FÉDÉRAL (CYBER UNIT – PARQUET FÉDÉRAL)

En effet, si vous laissez votre porte d'entrée ouverte, il ne faut pas vous étonner d'être victime d'une intrusion.

De plus, les entreprises permettent trop facilement à leurs collaborateurs de se connecter avec leurs propres appareils, en commençant pas la clé USB. Un serveur ne va pas bloquer l'innocent pilote de clavier sans fil que la clé USB prétend être et il ouvrira ainsi la porte à des logiciels malveillants cachés. Ph. Van Linthout : « Une personne ayant un minimum de compétences en ingénierie sociale peut entrer très rapidement dans le réseau d'une organisation. La Russie a distribué un jour des clés USB lors d'un sommet européen sans que personne ne s'en aperçoive. Combien de fois n'avez-vous pas branché une clé USB gratuite ? Nous sommes notre propre pire ennemi. »

QUE FAIRE EN CAS DE PROBLÈMES ?

De nombreuses entreprises dissimulent l'attaque dont elles sont victimes, cherchent discrètement de l'aide auprès d'un consultant et espèrent ainsi éviter de nuire à leur réputation. Une telle attitude est non seulement irresponsable sur le plan éthique, mais elle donne aussi au criminel la possibilité d'utiliser votre entreprise comme plaque tournante pour des attaques futures contre d'autres entreprises. « Vous devenez, en quelque sorte, complice et coresponsable en droit pénal », met en garde Ph. Van Linthout. « De plus, la loi oblige[1] certaines entreprises à signaler les cyberincidents. »

D'autres signalent l'infraction, mais sont déçues que la justice n'offre pas de solution toute faite. « C'est encore plus ennuyeux lorsque l'incident n'est signalé qu'après que l'on ait d'abord essayé de réparer soi-même les dégâts. Si la justice doit agir alors que des traces ont déjà été effacées, elle a beaucoup moins de chances de pouvoir intervenir de manière significative. Bien entendu, il faut trouver l'équilibre entre 'l'extinction du feu' et la réparation du toit. »

Préparez-vous, car toute organisation peut être victime un jour ou l'autre de manière directe ou indirecte. Même dans les entreprises les mieux protégées, il peut arriver que quelqu'un clique sur un courrier électronique frauduleux. « La préparation fait la différence entre un incendie ou un détecteur de fumée », confirme J. Kerkhofs. « La confiance et l'intégrité sont de puissants facteurs de différenciation. Ironiquement, vous gagnez davantage la confiance des clients lorsque vous faites une erreur malgré une sécurité forte et que vous pouvez la corriger correctement. En effet, vous prouvez ainsi votre pertinence sur le marché. On ne peut donc que conclure qu'investir dans la cybersécurité, c'est investir dans la compétitivité ! »

1 Cf. loi sur la sécurité des réseaux et des systèmes d'information et Code de droit économique

« NOUS SOMMES NOTRE PROPRE PIRE ENNEMI »

PHILIPPE VAN LINTHOUT, JUGE D'INSTRUCTION À MALINES

BACK-UP, BACK-UP, BACK-UP !

Répondre aux exigences d'un criminel est pervers. Avec un back-up optimal, le redémarrage après une attaque classique ne fera pas perdre plus qu'une journée de travail. En revanche, un back-up ne sert pas à grand-chose en cas d'ATP, car le criminel est alors déjà installé depuis longtemps dans le système. La situation est encore plus pénible lorsque le logiciel malveillant ne s'active qu'après la connexion du serveur de sauvegarde. Il n'existe donc pas de protection étanche contre la cybercriminalité sophistiquée. Par contre, vous pouvez minimaliser les dégâts :

- **en conscientisant vos collaborateurs et toutes les parties prenantes de votre entreprise ;**
- **en investissant dans des solutions de cybersécurité solides et avancées ;**
- **en créant à l'intérieur du système un espace 'externe' (appelé sandbox). Il est possible d'y tester des appareils étrangers avant de les connecter au cœur de votre entreprise ;**
- **en faisant appel, en cas d'incident, à un expert qui aide à faire les bonnes démarches au bon moment (déposer plainte, garder les traces, sécuriser les codes d'accès, redémarrer en préservant les traces...).**

BESOIN D'AIDE OU DE CONSEIL ?

- **Le Centre pour la cybersécurité Belgique (ccb.belgium.be)**
- **La Computer Emergency Response Team fédérale (cert.be)**
- **La Cyber Security Coalition (cybersecuritycoalition.be)**