Cyber-sécurité

« La cyber protection est aussi une question d'organisation »

L'AP-HP victime d'une cyberattaque

Les Echos - le 23 mars 2020 - Par Florian Dèbes

L'assistance publique-Hôpitaux de Paris (AP-HP) a été prise pour cible dimanche 22 mars. L'ampleur de l'épidémie de Covid-19 accroît les risques d'attaques informatiques.

C'est une autre vague dont les centres hospitaliers se seraient bien passés… Alors que des centaines de patients atteints par le Covid-19 affluent dans les services de réanimation débordés, ce dimanche, l'assistance publique-Hôpitaux de Paris (AP-HP) a été la victime d'une cyberattaque.

D'après « L'Express », qui a révélé l'information, une partie des serveurs informatiques de l'AP-HP ont subi une attaque par déni de services (DDos) au cours de laquelle, brutalement surchargés de requêtes inutiles, ils ont été noyés et rendus inaccessibles. Pendant une heure, l'AP-HP a dû couper l'accès aux mails et aux outils à distance pour ses salariés en télétravail.

Les cyberattaques capitalisent sur le virus

« *Il y a eu un petit souci, mais cela a été réglé en moins d'une heure, sans impact ni sur le fonctionnement des hôpitaux, ni sur l'offre de soin* », rassure Philippe Loudenot, le haut fonctionnaire à la sécurité des systèmes d'information pour le ministère de la Santé, resté pendu à son téléphone avec l'AP-HP tout le dimanche.

L'agence nationale de sécurité des systèmes d'information (Anssi) a été prévenue, mais ce sont les équipes de l'hôpital public qui ont géré la situation en direct.

L'opportunisme des hackers

Ce n'est pas la première attaque du genre en France. En novembre dernier, une attaque par logiciel-rançonneur avait paralysé les ordinateurs du centre hospitalo-universitaire de Rouen. La crise sanitaire accroît encore davantage la pression. « *Les services informatiques des hôpitaux sont hyper-sollicités pour développer le télétravail des équipes administratives et techniques face à des hackers opportunistes* », se désole le responsable informatique d'un centre hospitalier du sud de la France.

Dans ce contexte, plusieurs sociétés de cybersécurité françaises (Tehtris, Systancia) ou étrangères (Kaspersky, Palo Alto Networks), ont offert leurs services aux établissements de santé pour les prochaines semaines. « *On ne peut pas attendre des hackers un début de civisme* », pointe Christophe Corne, le PDG de Systancia.

La semaine dernière, une attaque contre un hôpital tchèque, à Brno, le second plus grand centre de soins du pays et lieu de tests au coronavirus, l'a conduit à éteindre tous ses ordinateurs et à reporter plusieurs opérations chirurgicales. Aux Etats-Unis, le site du département de la santé a lui aussi été rendu inaccessible par une attaque DDos, le 16 mars.

Philippe Loudenot refuse néanmoins de s'alarmer : « e*n France, les hôpitaux ont l'obligation quand ils sont victimes d'une cyberattaque de nous le faire savoir et je n'ai pas reçu d'autres signalements* », assure-t-il.

La région Grand-Est touchée par une cyber-attaque de grande ampleur, 7 500 agents concernés

France Info - 20/02/2020

"Toutes les mesures ont été prises pour gérer cette attaque", a déclaré sur Twitter Jean Rottner, le président de la région Grand-Est.

Depuis une semaine, la région Grand-Est est victime d'une cyber-attaque d'ampleur. Les ordinateurs des agents de la région ainsi que des élus ont été piratés, 7 500 personnes sont concernées, rapporte France Bleu Champagne.

En cause, un virus qui a été introduit dans le système informatique vendredi 14 février. Tous les postes de travail ont été touchés sur les différents sites de la région, en Champagne-Ardenne, en Lorraine et au siège, à Strasbourg. Des lycées ont aussi été victimes du virus. Concrètement, les agents n'ont plus accès à leur boîte mail ni aux logiciels internes, les badges d'accès sont hors service, et les documents sur les serveurs communs sont hors d'accès.

A priori, la panne n'a pas de conséquence pour le grand public. La région affirme que la cyber-attaque n'a pas pas permis de récupérer de fichiers financiers ou de fichiers sensibles. Sur Twitter, le président de la région Grand-Est, Jean Rottner, s'est voulu rassurant : *"Toutes les mesures ont été prises pour gérer cette attaque, qui peut encore entraîner quelques retards dans les réponses".*

Une quarantaine de personnes des services informatiques de la région sont en effet mobilisées pour un retour à la normale d'ici la fin de la semaine. La région a également dû faire appel à un prestataire externe, ainsi qu'à l'agence nationale de la sécurité des systèmes d'information. Les agents peuvent désormais simplement à nouveau envoyer des mails, mais sans pièce jointe trop volumineuse.

Cybersécurité : Les 10 Plus Grosses Attaques de 2019

FORBES – 06/01/20

L'année 2019 vient tout juste de s'achever et une chose est sûre, cette année a été marquée par une cybersécurité fortement menacée. On a pu signaler tous types d'attaques, des 100 pires mots de passe jusqu'au « piratage » du FaceID de l'iPhone en moins de 2 minutes. Voici les 10 menaces qui ont marqué l'histoire de la cybersécurité en 2019.

1. **L'application Google Camera menaçant des centaines de millions d'utilisateurs Android (1,9 millions de vues)**

Le 19 novembre dernier, Davey Winder a rapporté comment des chercheurs en cybersécurité avaient découvert une vulnérabilité qui affectait les utilisateurs des applications Google Camera et Samsung Camera. Qu'ont découvert les chercheurs ? Oh, seulement un moyen pour un hacker de prendre le contrôle des applications de caméra de smartphone et de prendre des photos à distance, d'enregistrer des vidéos, d'espionner vos conversations en les enregistrant lorsque vous portez le téléphone à votre oreille, identifier votre emplacement, etc. Tout cela s'est déroulé en silence, en arrière-plan. Davey Winder se demande si ce sera la dernière fois qu'il écrira à propos d'une application pour smartphone très en vue, utilisée par des millions de personnes, qui comporte une vulnérabilité de haut niveau. « Je voudrais dire oui, mais la vérité est que je ne pense pas attendre très longtemps avant que la première histoire de ce type arrive en 2020 ». Il semble étonnant que Google, avec toutes les ressources à sa disposition, ne puisse toujours pas bloquer ce type de menaces.

2. **Vulnérabilité de sécurité critique pour 40 millions d'utilisateurs de Samsung Galaxy et Note (1,2 million de vues)**

Début octobre, Samsung a confirmé tout un tas de vulnérabilités qui affectaient les utilisateurs des smartphones Galaxy S8, S9, S10 et Note 9 et 10. Le plus grave des 21 problèmes de cybersécurité révélés par la version de maintenance de sécurité (SMR) d'octobre était une vulnérabilité critique susceptible d'avoir un impact sur un total de 40 millions d'utilisateurs de Galaxy S9 et de Note 9. Bien que la vulnérabilité ait été corrigée dans ce SMR, le problème de l'ouverture de la fenêtre de menace entre la divulgation du problème et le moment où les utilisateurs pouvaient appliquer le correctif reste problématique. Comme un utilisateur Android le sait bien, la fragmentation de l'écosystème des smartphones signifie que les mises à jour de sécurité sont rarement déployées immédiatement pour tout le monde. C'est un problème qui ne disparaîtra pas en 2020. Le 9 décembre, Davey Winder a écrit à propos d'une vulnérabilité de « déni de service permanent » d'Android dans les versions 8 à 10 du système d'exploitation du smartphone. Cela a été corrigé par la mise à jour de décembre qui a rapidement été déployée. Le 27 décembre, le Note 10+ 5G n'avait toujours pas reçu les modifications.

3. **Le gouvernement américain entame une démarche préventive pour que les utilisateurs de Windows effectuent la mise à jour au plus vite (1 million de vues)**

La question de mises à jour se poursuit avec une histoire qui se concentre sur la Cybersecurity and Infrastructure Security Agency (CISA) du Département de la sécurité intérieure des États-Unis, émettant un avertissement aux utilisateurs de Windows à propos d'une vulnérabilité critique de la sécurité. La menace en question n'est autre que BlueKeep, et le problème de mise à jour réside dans le fait que les anciennes versions du système d'exploitation Windows étaient en danger car elles n'étaient pas mises à jour avec le correctif correspondant. Ceci malgré le fait que Microsoft propose un correctif de sécurité d'urgence pour les systèmes fonctionnant sous Windows XP. Alors que Windows 7 atteindra le statut de fin de vie le 14 janvier 2020, il est peu probable que ce soit la dernière fois que nous entendions parler de problèmes de sécurité comme celui-ci.

4. **La Nouvelle-Orléans déclare l'état d'urgence à la suite d'une cyberattaque (731 000 vues)**

Le 2 octobre dernier, le FBI a émis un avertissement de cyberattaque « à fort impact » en réponse à des attaques de rançongiciels contre des cibles des gouvernements étatiques et locaux. Le FBI a communiqué des conseils d'atténuation qui comprenaient la mise à jour des systèmes d'exploitation, des logiciels et du micrologiciel des appareils avec les derniers correctifs de sécurité et la garantie que les données étaient sauvegardées régulièrement et ces sauvegardes vérifiées. Avance rapide jusqu'au 14 décembre : la ville de la Nouvelle-Orléans a déclaré l'état d'urgence à la suite, vous l'avez deviné, d'une attaque de rançongiciel. Étant donné que l'État de Louisiane a déjà été attaqué en novembre dernier et que 23 agences gouvernementales du Texas ont été mises hors ligne à la suite d'une cyberattaque en août, Davey Winder est malheureusement presque sûr d'écrire des rapports similaires en 2020.

5. **Confusion des mises à jour du micrologiciel Samsung (590 000 vues)**

Ce rapport a couvert une autre histoire de mise à jour du smartphone Samsung, mais sans rapport avec une vulnérabilité critique des appareils Galaxy et Note cette fois. Il s'agissait d'une application qui avait été téléchargée par 10 millions d'utilisateurs de Samsung et qui était conçue pour aider à gérer les mises à jour du micrologiciel, et ainsi améliorer la sécurité de ces appareils. Les chercheurs en sécurité ont averti que l'application n'était pas « officiellement affiliée à Samsung » et que les utilisateurs pourraient se retrouver à payer des frais annuels pour télécharger gratuitement les mises à jour. À la suite d'une discussion avec les développeurs de l'application, qui ont expliqué les malentendus sur l'identité de l'application et les problèmes résolus, l'application a été supprimée de Google Play pendant plusieurs mises à jour. Un résultat satisfaisant, et des développeurs prenant note des préoccupations et prenant des mesures immédiates pour y remédier. « C'est une histoire qui, je l'espère, se répétera, en termes de résultats, en 2020 », annonce l'expert en informatique et en cybersécurité.

6. **Problèmes de mise à jour de Windows 10, première partie (539 000 vues)**

Maintenant, vous vous demandez probablement pourquoi Windows 10 n'a pas été cité dans le top 10 jusqu'à présent. Si c'est le cas, vos attentes sont sur le point d'être satisfaites. Les problèmes de mise à jour de Windows 10 ont été un thème

récurrent pour Davey Winder en 2019, et le bilan était rarement positif. Le 9 octobre dernier, les utilisateurs étaient déjà confus vis à vis du processus de mise à jour qui assurait la sécurité de leurs ordinateurs. Plus que de simples promesses non tenues : un Windows Defender ATP défaillant, pour les utilisateurs d'entreprise. Dans cette histoire, Microsoft conseillait aux utilisateurs de Windows 10 d'installer les mises à jour dans un ordre spécifique pour empêcher une boucle de redémarrage multiple. « J'espère que 2020 sera l'année où j'arrêterai d'écrire sur les problèmes de mise à jour de Windows 10. Mais je ne mettrai pas ma main à couper… », affirme-t-il.

7. **Problèmes de mise à jour de Windows 10, deuxième partie (518 000 vues)**

Le 17 août, Davey Winder a rapporté la façon dont Microsoft a confirmé un avertissement de mise à jour pour les utilisateurs de Windows 10 ainsi que Windows 8.1 et Windows 7 et 8. En plus de provoquer des écrans noirs après la mise à jour pour certains utilisateurs, cette histoire a mis en garde contre les scripts *Visual Basic* qui ont cessé de fonctionner et ont affecté les utilisateurs de Microsoft Office. Les problèmes de sécurité de Microsoft Office ne disparaîtront certainement pas en 2020.

8. **Problèmes de mise à jour de Windows 10, troisième partie (515 000 vues)**

La mise à jour Windows 10 a rompu le service *Windows Defender Advanced Threat Protection (ATP)* dans de nombreux cas. Microsoft a annoncé: « Ne pas installer cette mise à jour ». « Pour être honnête, je ne pense pas qu'il y ait quoi que ce soit de plus à ajouter. Juste un autre problème parmi une longue série d'histoires liées à la mise à jour Windows de 2019 », déclare Davey Winder.

9. **Avertissement de menace de vol d'informations d'identification Google Gmail et Google Agenda (513 000 vues)**

Il a été constaté que les auteurs de menaces exploitaient l'incroyable popularité des services Google Agenda et Gmail pour cibler une attaque de vol d'informations d'identification. Les chercheurs l'ont décrit comme une « arnaque sophistiquée » qui a utilisé l'intégration étroite et automatique entre différents services Google contre les utilisateurs pour les cibler avec des exploits malveillants. « Au-delà du *phishing*, cette attaque ouvre la porte à toute une série d'attaques d'ingénierie sociale », a déclaré Javvad Malik, défenseur de la sensibilisation à la sécurité chez KnowBe4. Javvad Malik a expliqué à Davey Winder que pour avoir accès à un bâtiment, par exemple, il serait possible d'écrire simplement une invitation pour un entretien ou bien un rendez-vous en face à face de ce genre qui, selon lui, "pourrait permettre un accès physique à des zones sécurisées". L'exploitation des fonctionnalités de l'application est un vecteur d'attaque qui ne mènera nulle part en 2020, attendez-vous à voir beaucoup plus de rapports sur de telles choses.

10. **National Security Agency avertit les utilisateurs de Windows (473 000 vues)**

L'entrée finale dans ce top 10 des histoires de cybersécurité et qui a attiré votre attention en 2019 est directement liée au numéro trois de la liste. Oui, c'est un autre avertissement BlueKeep. « Le 7 juin, j'ai rapporté la façon dont la U.S.National Security Agency (NSA) avait exhorté les utilisateurs de Microsoft Windows à faire rapidement la mise à jour si leurs systèmes n'étaient pas entièrement corrigés », annonce Davey Winder. À ce moment-là, Microsoft avait déjà publié plusieurs avertissements concernant l'urgence des mises à jour, telle était la gravité de la menace BlueKeep. Pour 2020, la cybersécurité risque de beaucoup faire parler d'elle encore. Il faut s'attendre à voir de nouvelles menaces émerger.

2020 : La France championne des cyberattaques ?

SILICON - Mick Bradley, 28 novembre 2019

L'année 2019 aura vu la France battre des records de cyberattaques, avec 67% d'entreprises victimes de cyberattaques et seulement 10% aptes à y faire face.

Contrairement aux aprioris, les premières victimes n'étaient ni les multinationales, ni les petites entreprises, mais les ETI, dont le nombre de victimes a crû de 36% à 63%. À force de voir leurs DSI comme des tiers et la cybersécurité comme une fonction support, les entreprises et institutions françaises vont-elles devenir championnes des cyberattaques ?

Si aucune entité (institution, entreprise) n'est invincible, quand bien même elle serait protégée par le meilleur logiciel de sécurité au monde, il est important, en cas de cyberattaque, de disposer d'un système d'information suffisamment protégé pour garantir la récupération des données, la continuité des opérations et la reprise d'activité après sinistre. C'est pourquoi les décideurs doivent intégrer la protection des données au cœur de la stratégie opérationnelle et non la reléguer au rang de fonction support. Il en va de la protection de leurs données, réputations et revenus, qu'ils soient acteurs publics ou privés.

Toutes les entreprises ne survivent pas aux cyberattaques

Les conséquences d'une cyberattaque sont multiples et dans certains cas, elles peuvent aller jusqu'à provoquer la faillite d'une entreprise. Un temps d'arrêt de l'activité peut avoir de lourdes répercussions. 93% des décideurs informatiques rapportent que leur système pourrait tolérer une perte de données minimale, mais 50% d'entre eux estiment qu'au-delà d'une heure d'arrêt, les revenus de l'entreprise pourraient être lourdement affectés.

Une heure ! Cela donne matière à réfléchir. L'entreprise française Saint-Gobain s'était par exemple vu bloquer ses activités dans les ports, les usines et les bureaux. Au final elle s'était acquittée d'une lourde addition de 250 millions d'euros.

Les effets négatifs d'un temps d'arrêt de l'activité quand ils ne mènent pas à la faillite vont en tout cas au-delà des pertes financières. Atteintes à la réputation, perte de confiance, de la valeur boursière, sont autant de conséquences « douloureuses ».
Prenons le cas d'une entreprise cotée. Les données privées de ses clients se retrouvent subitement dans la nature, exposées. Sans plan de récupération des données, de continuité et de reprise d'activité, la situation de l'entreprise peut très rapidement dégénérer. Ses clients se mettent à exprimer leur mécontentement sur les réseaux sociaux et pendant ce temps, son cours de bourse chute, son service informatique se démène pour corriger la faille quand une cellule de crise prépare une déclaration pour… tenter d'apaiser la situation.

Les mairies françaises futures cibles de choix ?
Comme beaucoup de grandes tendances, les signes avant-coureurs nous parviennent des États-Unis. Depuis le début de l'année, 22 municipalités américaines ont été victimes de cyberattaques. Les pertes se chiffrent en millions. La ville de Baltimore, par exemple, estime ses pertes à 18 millions de dollars. Alors que la tendance ne fait que débuter, les municipalités françaises ne sont pas en reste.
Les villes de Sarrebourg (Moselle), Sequedin (Nord), Huez (Oisans), Sequedin (Nord) autant de communes de tailles moyennes ou moins, qui se sont vu attaquer par des cyberpirates.
Derrière ces attaques se cachent des rançongiciel (malwares) dont l'unique but est d'extorquer de l'argent. Si contrairement à une entreprise, une mairie ne peut pas faire faillite, les pertes de ses données et la paralysie de ses systèmes d'information peuvent provoquer des pertes irréversibles et paralyser des services publics comme le SAMU. Les conséquences n'en seraient pas moins dramatiques.
Les mairies ne sont pas que des centres de fonctionnement opérationnels des municipalités, ce sont aussi des sanctuaires de la vie collective qui portent la mémoire de la vie de leur commune parfois sur plusieurs décennies et doivent être protégée comme tel. Là aussi la protection des données doit être mise au centre de son fonctionnement et non reléguée à la marge. Le DSI ne doit et ne peut pas être **cet inconnu** qui intervient ex post.

Mettrez vos données et leur protection au centre de votre stratégie et faites-en une priorité
Les cyberattaques sont aujourd'hui plus sophistiquées que jamais, les données étant très recherchées. Dès lors qu'une entreprise, ou une institution n'est pas correctement protégée, elle s'expose à de nombreuses attaques, par ailleurs, le fait de survivre financièrement à une attaque n'est plus une garantie de survie et de bon fonctionnement sur le futur. Un an après une cyberattaque, certaines villes en sont encore au stade de récupérer leurs données.
Que vous soyez une entité publique ou privée, la cybersécurité ne peut plus être traitée comme une fonction support, vous devez pouvoir compter sur une solution de protection des données solide, taillée pour votre infrastructure.

A Roissy, 733 PC portables perdus chaque semaine

Website : https://www.sbedirect.com/grand-comptes/fr/

Environ 88 % des ordinateurs sont perdus ou volés en dehors du lieu de travail. Les cas les plus fréquents se déroulent dans les transports, en particulier les aéroports ou les gares. En effet, chaque semaine plus de 4000 ordinateurs sont oubliés ou égarés dans les aéroports européens, tandis qu'au moins un ordinateur est volé chaque jour dans les trains Thalys sur les trajets Paris-Bruxelles. Les données sont donc beaucoup vulnérables lorsqu'elles quittent l'enceinte de l'entreprise.

Les vols d'ordinateurs en entreprise

Website : https://www.sbedirect.com/grand-comptes/fr/

Avec l'omniprésence des appareils électroniques en entreprise, le cambriolage informatique est devenu une problématique primordiale pour tous les dirigeants. Environ 33 000 ordinateurs sont ainsi perdus ou volés chaque année en France.
De plus, 95 % de ces ordinateurs ne sont jamais restitués à leur propriétaire. Cela représente un coût d'autant plus important, car toutes les données contenues dans l'ordinateur sont perdues définitivement. Cette perte peut même devenir très grave si ces données sont confidentielles pour l'entreprise. Ce coût varie en fonction des secteurs d'activité : par exemple, la perte d'un ordinateur coûte en moyenne 87 500 € pour une entreprise du secteur des services.
Certains secteurs d'activité sont plus sensibles que d'autres aux cambriolages ou aux vols d'ordinateurs, tels que l'éducation et la recherche, la santé et le secteur pharmaceutique, ou encore le secteur public.

Témoignage : François Asselin (CPME) : "Les cyber-attaques peuvent détruire nos petites entreprises"

Par Ségolène Mahias, le 06 octobre 2017

Un sujet qu'il connaît bien pour avoir connu les trois formes de cyberattaques les plus courantes. À la tête de l'entreprise éponyme Asselin (14,5 M€ de CA et 140 salariés), dans les Deux-Sèvres, il intervient sur les secteurs de la charpente, menuiserie, ébénisterie, ferronnerie pour la restauration des monuments historiques.
« La première attaque, c'était un ramsomware, deux jours après mon élection à la tête de la CPME ! Notre serveur a été atteint. Plus aucun ordinateur ne fonctionnait. Notre chance a été d'avoir une entreprise d'infogérance qui a pu réimplanter la sauvegarde. Sans cela, je pense que nous avions un exercice foutu. » Quelques temps plus tard, c'est une arnaque au président qui a frappé la société. « Le scénario était très bien ficelé. J'ai la chance d'avoir une responsable comptabilité perspicace et qui savait que je ne travaille pas comme cela. » Enfin, il y a un an c'est un essai de détournement de domiciliation bancaire qui a été tenté. Trois attaques et un seul enseignement : « Il n'y a pas que les grands groupes, les PME et les TPE sont aussi victimes. Il faut faire preuve de vigilance ! »

Internet. Les 100 mots de passe les plus piratés en 2017

Le Télégramme - Publié le 25 décembre 2017 à 16h37 Modifié le 25 décembre 2017 à 17h39

L'éditeur Splashdata publie chaque année la liste des mots de passe les plus piratés de l'exercice en cours. Le podium de l'édition 2017 est composé de : "123456", "password" et "12345678". Découvrez ci-dessous le top 100 ainsi que quelques conseils pour éviter de se faire piéger.

La saison de 2017 du world wide web a été marquée par l'activité intense des pirates informatiques. En mai, une attaque mondiale "sans précédent" a touché plus d'une dizaine de pays. Les malfaiteurs ont utilisé un logiciel de rançon pour bloquer des milliers d'ordinateurs. En novembre, les données personnelles de près de 60 millions d'utilisateurs de Uber ont été subtilisées...

Pour le particulier, la meilleure façon de se prémunir d'un piratage informatique reste de ne pas surfer sur des sites internet non-sécurisés, de ne pas ouvrir de pièce jointe dans un mail provenant d'un expéditeur inconnu et, évidemment, d'adopter des mots de passe suffisamment complexes pour résister aux tentatives de décryptage automatique.

Prénoms, années de naissance...

Visiblement, les hackers ont encore de beaux jours devant eux. Splashdata a une nouvelle fois compilé les données de plus de 2 millions de comptes piratés dans l'année. Le grand vainqueur 2017 du mot de passe le plus facilement contourné reste encore "123456", suivi de "password" et "12345678". Les prénoms fleurissent également dans ce top 100, tout comme les années, le nom de disciplines ou de films populaires (football,starwars,hockey)...

Vous vous demandez peut-être comment les pirates ont pu décrypter facilement certains mots de passe présents dans ce classement comme "1qaz2wsx" ou "1q2w3e" ? Baissez les yeux, imaginez que vous disposez d'un clavier "qwerty" et la solution apparaît : il s'agit simplement d'un alignement de touches assez facile à modéliser.

Comment faire, alors, pour trouver un bon mot de passe sans l'oublier ? La Cnil (Commission nationale de l'informatique et des libertés) fournit une liste complète de conseils et de pistes. Et si on inscrivait la sécurisation de nos données sur la liste des bonnes résolutions 2018 ?

Cyberattaques. Entreprises, gare au virus à la rançon

Le Telegramme - Publié le 11 mars 2016 - Anne-Cécile Juillet

Cet après-midi du 18 février, Julie s'en souviendra longtemps. Cette assistante d'un groupe qui emploie plusieurs centaines de personnes dans le Finistère-Nord ouvre sa boîte mail. « Un courriel m'invitait à ouvrir deux pièces jointes apparemment anodines, des fichiers Word et Excel, soi-disant pour régler une facture ». Julie l'ouvre et c'est le début des ennuis. « J'ai ouvert la pièce jointe par curiosité et j'ai été déçue puisqu'il s'agissait d'une page blanche. En revanche, mon ordinateur s'est mis à ramer. Je l'ai éteint et lorsque je l'ai relancé, j'ai vu tous les fichiers de mon bureau modifiés avec une extension .Locky et un lien qui me demandait de payer si je voulais récupérer mes données ». En somme, Julie et son entreprise viennent de se faire prendre en otage leurs données informatiques contre une demande de rançon.

« Il faut sauvegarder en plusieurs exemplaires »

« Plus le temps passait, plus le prix de la rançon s'élevait.

Pendant une semaine, j'ai vécu l'enfer, on n'était pas sûrs du tout de pouvoir récupérer nos fichiers. Pour notre entreprise, cela aurait pu avoir un impact considérable : dans mon ordinateur, il y avait six années de travail ». Finalement, grâce à des sauvegardes rigoureusement faites, Julie et ses patrons ont réussi à retrouver la quasi-totalité de leurs données. « Sauvegarder sur différents supports, c'est l'un des conseils que l'on donne aux entreprises qui font appel à nous », précise Gwenaël Forest, informaticien de Bureautique de l'Ouest. Prestataire, il n'arrête pas d'être confronté à ce virus qui s'attaque à de nombreuses entreprises de la région : « En ce moment, ce type de cyberattaque déferle de façon massive sur le Finistère, visant des entreprises de toutes tailles. On ne cesse de rappeler d'être très vigilant lorsqu'il s'agit d'ouvrir des pièces jointes ». La compagnie de gendarmerie de Brest a été saisie de plusieurs plaintes. Un sujet d'autant plus inquiétant que même les ordinateurs de marque Apple, réputés hermétiques aux virus, ont été récemment attaqués.

Les vols de matériels informatiques sur les lieux de travail prennent de l'ampleur

Source : Kensington, Étude réalisée par Kensington

Les pertes de données sont préjudiciables pour les entreprises. De ce fait, il est très important pour la DSI de mettre en place des stratégies de sécurité afin de protéger au maximum les données de l'entreprise. Cependant, il arrive souvent que les responsables de la sécurité informatique se concentrent davantage sur les moyens logiciels que matériels. Spécialisée dans les verrous de sécurité pour ordinateurs, l'entreprise Kensington a réalisé une étude basée sur l'utilisation des moyens matériels de sécurité auprès de 300 entreprises. Les résultats de son analyse ont montré que même si plus de la moitié des entreprises ont effectivement mis en place une politique sur la sécurité matérielle de leurs équipements informatiques, 23 % des vols d'ordinateurs se passent au sein même de l'entreprise.

Plus de la moitié des vols d'ordinateurs portables et autres appareils mobiles professionnels se sont produits dans des lieux publics, notamment les transports en commun (25 %), les aéroports et les hôtels (14 %) ainsi que les restaurants et cafés (11 %). Mais ce qui a le plus marqué dans cette étude c'est que 23 % des vols de matériels informatiques professionnels se sont produits au sein de l'entreprise elle-même (23 %).

Pourtant, plus de la moitié des entreprises interrogées (66 %) ont affirmé avoir mis en place une politique sur la sécurité matérielle pour protéger les ordinateurs portables, les dispositifs mobiles et les autres équipements électroniques. Cela dit, seulement 46 % des employés affirment avoir déployé effectivement des moyens matériels pour verrouiller leurs équipements informatiques, dont les ordinateurs portables (77 %), les ordinateurs de bureau (34 %), les vidéo projecteurs (30 %), les disques durs (23 %) et les moniteurs (18 %) et les haut-parleurs (8 %).

Selon un responsable auprès de l'entreprise Kensington, cette étude met en avant le fait que le pourcentage des vols d'ordinateurs et autres équipements informatiques, au sein même de l'entreprise, n'est pas négligeable. Il est donc important pour les entreprises « d'implémenter une politique sur la sécurité matérielle » pour protéger leurs équipements informatiques ainsi que les données qu'ils contiennent.

Les vols des matériels informatiques dans un lieu public sont assez courants. L'analyse réalisée par Kensington montre que le lieu de travail est aussi un lieu propice où l'employé peut perdre son ordinateur portable et autres équipements informatiques. Cela dit, l'étude ne précise pas si les vols se sont produits aux heures de bureau ou après. Dans tous les cas, les entreprises devraient reconsidérer leur politique sur la sécurité matérielle de leurs systèmes informatiques. En effet, quand l'entreprise se fait voler un ordinateur ou un disque dur, il n'est pas à écarter que des données clés soient exposées et se retrouvent dans les mains d'une personne malveillante, pouvant créer un préjudice autant pour l'entreprise elle-même que pour ses clients et partenaires.