SUISSE

Pourquoi les cyberattaques se transforment et comment les entreprises peuvent les éviter

WANNACRY. Ce rançongiciel qui a infecté des centaines de milliers d'entreprises, y compris en Suisse, est symptomatique de nouvelles menaces. Décrytpage et conseils d'experts.

MARJORIE THÉRY

Comment se protéger des rançongiciels, à l'image de WannaCry, qui aurait touché près de 200.000 entreprises ces derniers jours? L'ampleur de cette attaque d'un nouveau genre fait réagir les entrepreneurs. Hier, André Kudelski, CEO de l'entreprise de cyber sécurité du même nom, estimait que «le jour où il y aura un Hiroshima ou un Fukushima en matière cyber, il y aura une vraie prise de conscience». Pour certains, la Confédération doit par exmeple renforcer sa politique de lutte contre le cyber-risque, en se dotant d'une vraie politique en la matière. Malheureusement, Fukushima n'a pas mis un terme au nucléaire. Et il n'y aura probablement pas de Fukushima en matière cyber, car les cyber attaques aujourd'hui ne se concentrent plus (seulement) sur des infrastructures critiques, comme une centrale électrique, une grande banque ou un data center. Tout simplement car ces attaques nécessitent nettement plus de ressources avec un potentiel de réussite très limité. Les cyber attaques sont entrées dans une ère du marché de masse grâce aux rançongiciels, en multipliant les attaques et en exigeant de la part des entreprises ou des personnes infectées une rançon pour pouvoir retrouver leurs données. Un marché bien plus lucratif, avec, pour les criminels, très peu de risques d'être identifiés. Comme le relève les experts que nous avons interrogés *(lire leurs témoignages)*, il n'y a pas de solution miracle pour se prémunir de ces menaces. Mais des bonnes pratiques peuvent considérablement améliorer le degré de sécurité.

ANDRÉ KUDELSKI. «*Le jour où il y aura un Hiroshima ou un Fukushima en matière cyber, il y aura une vraie prise de conscience.*»

Pourquoi la Suisse est peu touchée par WannaCry

Les entreprises suisses seraient-elles déjà suffisamment protégées? Au niveau national, environ 200 entreprises auraient été touchées par ce rançongiciel, sur un total 200.000 au niveau mondial. David Ruefenacht, analyste à la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI, estime qu'il y a probablement plusieurs facteurs à ce nombre relativement faible. L'un d'entre eux est peut être du au fait d'il n'y a pas d'obligation d'annonce. Ensuite, Windows XP, un des systèmes les plus vulnérables à cette attaque, n'est plus très présent sur les systèmes informatiques suisses. «MELANI a fortement sensibilisé les utilisateurs pour qu'ils mettent à jour leur système d'exploitation et dans le cas de Windows XP, de passer à un système de nouvelle génération. Les versions de Windows qui sont encore maintenues ne sont pas touchée si l'utilisateur a choisi les mises à jours automatiques ou s'il a activement mis à jour le système». Une automatisation est-elle souhaitable? « Il n'est pas toujours possible d'automatiser toutes les mises à jour, qui peuvent entrer en collusion avec d'autres systèmes ou application de l'entreprise», relève Sergio Alves Domingues, Chief Technical Officer de la société vaudoise de sécurité SRCT.

Mises à jour et sauvegardes capitales

Comme d'autres spécialistes du domaine, le CTO insiste sur la nécessité de sauvegardes des données. « Si l'entreprise dispose d'un bon système de sauvegardes, elle devrait être en mesure de restaurer les données chiffrées par le rançongiciel». Comme MELANI, l'entreprise ne recommande pas de payer les rançons, qui alimentent les organisations criminelles derrière ces attaques, et leur indique que l'entreprise n'est pas en mesure de restaurer ses données.

Pour le CTO, cette attaque est en tous cas particulièrement inquiétante, car contrairement aux rançongiciels d'anciennes génération, qui affectaient en général uniquement la machine de l'utilisateur infecté, dans le cas de WannaCry, il suffit d'une seule machine contaminée dans l'entreprise pour que le virus se propage dans les systèmes.

La montée en puissance de l'IoT ne devrait rien arranger dans ces circonstances. Et que dire des promesses (et des risques) de l'industrie 4.0 et de son autonomisation croissante des processus? Il ne faut toutefois pas céder à la psychose: ce sont des hommes qui conçoivent ces rançongiciels dans le but de s'enrichir, et ce sont des hommes encore qui ouvrent des emails malveillants, par inattention ou manque de sensibilisation. Ainsi, malgré la sophistication croissante de ces technologies, le facteur humain restera la principale source de menace comme de résolution du problème.■

Bitcoin: des transactions qui sont anonymes mais pas intraçables

Les auteurs de la cyberattaque mondiale lancée vendredi exigent le versement des rançons en bitcoins car cette monnaie immatérielle permet l'anonymat, mais cela ne suffira peut-être pas pour effacer leurs traces.

Le bitcoin, qui tire son origine d'un logiciel mis en ligne en février 2009 par un ou plusieurs informaticiens se cachant sous le pseudonyme de Satoshi Nakamoto, est une monnaie virtuelle autorégulée.

«Le bitcoin, c'est le cash du numérique», explique à l'AFP Nicolas Debock, investisseur chez Balderton Capital, spécialiste des monnaies virtuelles. «Les transactions sont totalement anonymes, non répudiables. En revanche, elles sont totalement traçables».

«Toutes les transactions sont inscrites dans les chaînes de stockage, appelées blockchains. C'est anonyme, mais tout le monde peut surveiller une adresse bitcoin et voir comment l'argent bouge», ajoute-t-il. «Personne ne pourra leur prendre cet argent, mais il sera possible de suivre à la trace l'activité de ce compte. Cependant, les comptes n'ont pas d'adresse physique, pas d'adresse bancaire, il n'y a pas d'hébergeur central».

Des services appelés «tumblers» promettent aux détenteurs de bitcoins d'anonymiser entièrement leurs comptes en monnaie virtuelle. «Le tumbler va diviser les sommes en bitcoins en milliers de petits morceaux, les répartir sur des milliers d'adresses différentes et faire plein de transactions», explique Manuel Valente, directeur à Paris de la maison du Bitcoin. «Au bout d'une semaine, on remet tous ces bitcoins sur une nouvelle adresse, en espérant avoir couvert ses traces. Ce sont des systèmes de blanchiment de bitcoins».

Mais si les polices et services de renseignement du monde entier s'allient pour surveiller le compte des pirates, cet argent virtuel ne pourra être récupéré sans se faire repérer.■

«Une mise à jour classique suffisait à se protéger»

THIERRY BLANC. Le directeur de la gouvernance du groupe de sécurité informatique DFI met en garde contre les effets à venir. La Suisse est peu touchée pour l'instant.

Pour quelles raisons, la Suisse est-elle peu touchée par WannaCry?

La Suisse n'a pas été spécialement visée. On parle pourtant d'une attaque à l'échelle mondiale. J'émettrai donc plusieurs hypothèses. Soit, les personnes, qui ont lancé cette attaque m'avaient pas de cible particulière en Suisse. Soit, les entreprises suisses sont plus attentives à la sécurité. Il s'agit de rester prudent, à ce stade. L'attaque de vendredi ne constitue qu'une première vague. A savoir une campagne majeure de diffusion d'emails infectés, avec quelques 5 millions d'emails envoyés chaque heure répandant le logiciel malveillant. Le bilan n'est donc pas définitif.

Dans le cas particulier de WannaCry, une simple mise à jour classique de Microsoft suffisait à se protéger?

On n'évitera pas le 100% des risques, mais, en effet, une simple mise à jour classique proposée par Microsoft le 13 avril suffisait à se protéger. Bien que le produit ne soit plus supporté, Microsoft a quand même édité un patch. Il est donc possible de mettre à jour les machines XP. Il faut aussi savoir que toutes les machines Windows sont vulnérables. Notons que cette mise à jour ne coûte rien en argent. Elle coûte en temps et en surveillance. Les PME doivent en être conscientes.

Quel budget les PME doivent-elles consacrer à leur sécurité?

Elles doivent consacrer du temps, des ressources et un budget financier à leur sécurité. Je dirai autour de 17% de leur chiffre d'affaires annuel. La prise de conscience est primordiale. Vous m'interrogiez dans *L'Agefi* sur le manque de conscience des risques de la part des entrepreneurs. La réalité de l'attaque cyber est là. Selon le Gartner, les budgets informatiques connaissent une hausse de 2,2% en 2016 et vont passer de 16 à 37 % du chiffre d'affaires total au cours des 5 prochaines années. A titre de comparaison, les entreprises dans le monde dépensent en moyenne 17% de leur budget informatique pour la sécurité informatique (selon le cabinet Vanson Bourne).

Quelles sont les mesures à prendre par les PME?

Une mise à jour de leurs systèmes (notamment le patch MS17-010), une sauvegarde des données séparées des réseaux, une vigilance vis à vis des emails (pièces jointes, liens vers des sites web....) et la déconnexion des ordinateurs infectés. De manière plus générale, les administrations et les entreprises de toutes tailles (notamment les PME qui sont les premières victimes) doivent être sensibilisées et tenir compte de menaces liés à la cybersécurité. Il faut absolument investir dans ce domaine. Ne pas laisser les risques latents. Les failles s'échangent à vitesse éclair dans le dark web où les attaquants jouent la montre. C'est le jeu des gendarmes et des voleurs. Les entreprises, prises au piège, courent pour patcher leurs systèmes d'information.

INTERVIEW: ELSA FLORET

Les entreprises ne communiquent pas assez

SOLANGE GHERNAOUTI. Réaction de la professeure à l'UNIL, suite à l'attaque mondiale de WannaCry.

Pourquoi la Suisse est-elle peu touchée?

De la chance, à moins qu'elle soit meilleure que les autres pays en mettant régulièrement à jour ses logiciels et réparant les failles de sécurité connues? Rappelons que le problème est issu d'une vulnérabilité Microsoft exploitée pour infecter les ordinateurs. Les cibles les plus rapidement et facilement accessibles se sont trouvées ailleurs qu'en Suisse, ce qui nous a certainement favorisés. La situation est similaire à celle d'une épidémie de grippe, toutes les populations ne sont pas touchées de la même manière et nous pouvons avoir plus ou moins de chance en fonction de notre situation au regard de l'origine du virus et de son vecteur de propagation. Ainsi, en n'étant pas dans les premières victimes, nous avons eu le temps d'isoler les systèmes vulnérables de l'Internet, de les remplacer ou de les corriger. Mais à ce jour, nous ne disposons ni du recul, ni des informations nécessaires pour affirmer quoi que cela soit.

Quel budget les PME doivent-elles consacrer à leur sécurité?

Il est très difficile de parler de budget, car tout dépend du secteur d'activité, des valeurs exposées, des menaces réelles et des risques encourus, mais aussi de l'appétence aux risques des dirigeants. Un risque d'interruption de toutes les activités, de perte de savoir-faire, d'altération ou de pertes de données et processus critiques sont toujours synonymes de perte de productivité de compétitivité, souvent de marchés et d'emplois. L'arnaque au président est très répandue mais souvent passée sous silence. Les entreprises n'ont pas d'obligation légale d'annoncer les cyberdélits, on ignore l'ampleur de ces nouvelles formes d'escroqueries favorisées par internet et le nombre réel de victimes de cyberattaques. La médiatisation des cyberincidents et le fait que les entreprises soient victimes, favorisent cependant la prise de conscience de la nécessité de pouvoir anticiper, prévenir et réagir aux cyberattaques. Mais si les entreprises communiquaient plus, partageaient plus d'informations et surtout dénonçaient les délits, cela contribuerait certainement à ce que le politique en Suisse dégage plus de moyens pour lutter contre ce phénomène relativement caché. Cela permettrait d'initialiser un cercle vertueux. Pour lutter contre la cybercriminalité, il faut un changement de paradigme dans la manière de penser et de réaliser la protection et la défense de nos intérêts. Une dénonciation des actes relevant de la cybercriminalité, même de faible intensité (comme une rançon de 300 dollars) permettrait de lutter efficacement contre elle.

Quelles sont les mesures à prendre par les PME?

Une hygiène informatique de base est cruciale, comportant la duplication et la sauvegarde des données notamment dans des data centers spécialisés et hébergés en Suisse. Mais cela suppose une grande anticipation. En Suisse, l'association des data centers Vigiswiss, apporte des solutions qui permettent de protéger physiquement et logiquement les données. Il y a une véritable opportunité pour les entreprises, mais aussi pour la Confédération, les cantons et communes de pouvoir utiliser d'anciens bunkers de l'armée pour stocker des données. – (EF)