Les bonnes pratiques pour lutter contre la cybercriminalité

	Les bonnes pratiques pour lutter contre la cybercriminalité

Les entreprises modernes sont très vite confrontées aux dangers que représente un modèle commercial actif en permanence. Les clients ont de plus en plus recours à des outils en ligne pour accéder à des comptes, à des services ou à de l'expertise.

Quant aux employés, ils souhaitent pouvoir se connecter à distance et à tout moment aux réseaux de leur entreprise. D'où l'aspiration à un accès quotidien plus simple et plus pratique. Mais cette souplesse à aussi son revers. Les hackers, qui l'ont également bien compris, créent par conséquent des virus et des logiciels malveillants, dans l'unique intention de nuire. À la lumière des récentes révélations de l'organisme britannique Office for National Statistics selon lequel plus de 5,8 millions d'incidents de cybercriminalité ont eu lieu l'an dernier, il est crucial que les entreprises protègent les données de leur personnel et de leurs clients contre la cybercriminalité.
Dans ce contexte, quelles sont les principales activités de cybercriminalité dont les entreprises ont à se prémunir, et que faire pour les combattre ?

La manipulation sociale (Social engineering)
À l'ère du numérique, les pratiques de manipulation sociale sont devenues un problème préoccupant. Du fait que l'internet offre aux fraudeurs un voile d'anonymat, il est important que les sociétés qui détiennent des données clients sensibles soient au courant des pratiques les plus répandues parmi les hackers qui utilisent la manipulation sociale.
Le phishing aussi appelé hameçonnage, est peut-être la forme la plus connue de piratage de fraude par abus de confiance. Il recourre les tentatives de fraudeurs qui généralement déploient de multiples moyens pour acquérir des données sensibles telles que les noms d'utilisateur, les mots de passe et les détails de paiement en se faisant passer pour une personne connue ou des organismes de confiance par courrier électronique ou une autre forme de communication numérique. Régulièrement, les cas de hameçonnage beaucoup plus ciblé, où les hackers se présentent comme des personnes de confiance, sont à la hausse. En cas de succès de l'attaque, les données des clients ou les documents sensibles d'une entreprise et donc sa réputation - sont en danger.
En effet, la recherche par Get Safe Online indique que la fraude liée au phishing à contribué aux organisations britanniques qui ont perdu plus de 1 milliard de livres sterling au cours de la dernière année en raison de la cybercriminalité.
Selon l'enquête, réalisée avec Spectum Mdp et dévoilée en exclusivité par Europe 1, 84% des sociétés française ont été ciblées par des pirates informatiques en 2015.
Le vishing et le smishing sont les variantes du phishing passant respectivement par les communications téléphoniques et SMS. Dans un cas comme dans l'autre, le principe est de récupérer les données sensibles de vos clients ou de votre entreprise. Compte tenu de l'impact dévastateur que peut avoir l'utilisation de la manipulation sociale par les cybercriminels sur les entreprises modernes, les dirigeants d'entreprise et les responsables informatiques doivent être très attentifs à ce type d'activités.

Menaces internes
À l'instar de la manipulation sociale qui peut porter préjudice aux entreprises de l'extérieur, il est légitime de se méfier également des menaces internes. Votre personnel peut disposer de privilèges d'accès aux données sensibles et en faire usage pour nuire à votre entreprise. Les employés où à l'heart, les prestataires présents ou le personnel de maintenance sur site pourraient également représenter un danger pour votre société.
Les problèmes posés par les activités malveillantes des sociétés ne sont pas toujours visibles immédiatement mais ils ne sauraient pour autant être ignorés. Prenons le cas d'un employé qui s'avère frustré ou de perdre son poste dans une entreprise pour une autre raison. Il est possible que cette décision provoque chez lui de la colère et l'amène à vouloir exprimer son ressentiment envers son ancienne société. S'il possède toujours les droits d'accès au stockage partagé ou à des documents, il a la possibilité de modifier, supprimer ou falsifier les données
Dépendant, comme c'est le cas avec les dangers de la manipulation sociale, le fait de connaître et de mesurer la menace potentielle des activités malveillantes peut permettre de faire un grand pas en avant dans la prévention des activités de cybercriminalité ciblant les entreprises. Les responsables informatiques et les dirigeants d'entreprises doivent rester vigilants en accordant aux utilisateurs des droits d'accès limités à leurs besoins et se méfier des récentes évolutions des techniques frauduleuses pour protéger leur entreprise contre les intentions malveillantes des cybercriminels.

Comment riposter
La lutte contre la cybercriminalité devrait dominer les débats et les plans stratégiques des dirigeants d'entreprise dans les années à venir. Pour optimiser leurs chances de l'emporter, les entreprises peuvent prendre plusieurs mesures.
1. Abandonner la technique des mots de passe, trop simple, au profit d'un système d'authentification forte en entreprise : Les hackers qui dérobent le nom d'utilisateur et le mot de passe d'un employé peuvent la plupart du temps parcourir le réseau sans être repérés et charger des programmes malveillants ou bien voler ou encrypter des données. Pour protéger les systèmes et les données, les entreprises ont besoin d'un système d'authentification forte qui ne repose pas exclusivement sur une information connue de l'utilisateur (mot de passe). Au moins un autre facteur d'authentification doit être utilisé, par exemple un élément que possède l'utilisateur (ex: un jeton d'ouverture de session informatique) et/ou qui le caractérise (ex: une solution d'identification biométrique ou comportementale). Il est également encourageant d'abandonner totalement les mots de passe et d'envisager cartes, jetons ou biométrie.
2. Profitez de la commodité accrue d'un modèle d'authentification forte mobile : Les utilisateurs sont de plus en plus désireux d'une solution d'authentification plus rapide, plus transparente et plus pratique que celle offerte par les mots de passe à usage unique (OTP). Les cartes d'affichage et autres dispositifs physiques. Désormais, les jetons mobiles peuvent figurer sur une même carte utilisée pour d'autres applications, ou être combinés sur un téléphone avec des dispositifs d'identification unique pour accéder à des applications cloud. Il suffit pour l'utilisateur de présenter sa carte ou son téléphone à une tablette, à un ordinateur portable ou à un autre périphérique pour l'authentifier sur un réseau, après quoi l'OTP devient inutilisable. Plus aucun jeton à mettre en place et à gérer. L'utilisateur final n'a qu'un seul dispositif à porter et n'a plus besoin de garder en mémoire ou de taper un mot de passe complexe.
3. Utiliser une stratégie de sécurité informatique par niveaux qui garantit des niveaux d'atténuation des risques appropriés : Pour une efficacité optimale, les entreprises ont intérêt à adopter une approche de la sécurité par niveaux, en commençant par authentifier l'utilisateur (employé, associé, client), puis en authentifiant le dispositif, en protégeant le navigateur et l'application, et enfin en authentifiant la transaction en recourant à l'intelligence basée sur les fichiers signatures ci nécessaire. La mise en œuvre de ces niveaux nécessite une plateforme d'authentification polyvalente et intégrée dotée de moyens de détection des menaces en temps réel. Cette plateforme, associée à une solution antivirus, apporte le plus haut degré de sécurité possible face aux menaces actuelles.

---

[1]
Chip Epps est Vice President, Product Marketing, IAM Solutions de HID Global
_[Lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus,) et vous assister dans ses démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertise, d'audits, de formations et de sensibilisation dans toute la France et à l'Étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03861 84)
Plus d'informations sur : https://www.lemetiergeek.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

[1]
[1]

Réagissez à cet article

Source : *Les bonnes pratiques pour lutter contre la cybercriminalité Chip Epps, HID Global*

Ransomware : ne payez jamais la rançon

Ransomware : ne payez jamais la rançon

Lors d'une conférence sur la cybersécurité organisée la semaine dernière à Boston par SecureWorld, un consultant a recommandé de ne pas régler la rançon réclamée par les cybercriminels pour obtenir la clef de décryptage des fichiers verrouillés. Il recommande plutôt de veiller à bien sauvegarder ses données.

Dès qu'une demande de rançon apparaît sur l'écran, il faut immédiatement déconnecter le poste de travail du réseau. (Crédit D.R.)

Lors d'une conférence sur la cybersécurité organisée la semaine dernière à Boston par SecureWorld, un consultant a recommandé de ne pas régler la rançon réclamée par les cybercriminels pour obtenir la clef de décryptage des fichiers verrouillés. Il recommande plutôt de veiller à bien sauvegarder ses données. « Cela semble facile à dire, surtout quand le risque de perdre des données critiques est assez faible. Cela nécessite aussi une certaine préparation », a ainsi déclaré Michael Corby, consultant exécutif pour CGI. Selon lui, « le plus important est de stocker ses données sous une forme qui ne pourra pas être affectée par le ransomware, en les chiffrant et en les stockant hors du réseau de production ». Ajoutant que l'entreprise « a besoin d'une copie propre des données qui sera facile à restaurer ». Celui-ci recommande également de vérifier « que les sauvegardes fonctionnent ». Restauration et récupération sont donc les maîtres mots, et « il faut bien penser à supprimer le malware avant de procéder à ces opérations ».

Si le consultant préconise de ne pas payer de rançon, il sait aussi que les autorités judiciaires estiment généralement que le paiement de la rançon est parfois inévitable et que c'est aussi le seul moyen pour l'entreprise de récupérer des données essentielles. Elles vont même jusqu'à les encourager à se doter d'un porte-monnaie bitcoin avant d'être affectées par un ransomware. Elles pourront ainsi effectuer un paiement rapide si nécessaire, les ultimatums posés par les pirates étant souvent assez courts.

Déconnecter immédiatement le terminal

La première règle que tous les employés doivent connaître quand l'entreprise est confrontée à un ransomware c'est de ne pas essayer de comprendre ce qui se passe. Dès que la demande de rançon apparaît sur l'écran, le ou les utilisateurs doivent déconnecter immédiatement le poste de travail du réseau et en informer le responsable de la sécurité. À son tour, ce dernier doit mettre en branle son équipe d'intervention, c'est à dire lui-même, mais aussi le département juridique, les relations publiques, les relations humaines, les cadres et l'IT.

En France, l'entreprise doit immédiatement informer la cybergendarmerie ou la police judiciaire. La procédure est contraignante, car en s'adressant aux forces de l'ordre, l'entreprise renonce au contrôle de l'enquête et parfois aux dispositifs et aux données qu'ils contiennent, puisqu'ils peuvent seraient saisis pour la recherche de preuves.

Comment bloquer les ransomwares

Voici quelques-unes des meilleures pratiques que les entreprises doivent adopter pour lutter contre les ransomwares. Ces mesures seront également très bénéfiques pour le réseau en général :

– Sensibiliser les utilisateurs finaux sur les logiciels malveillants en proposant des programmes d'information réguliers.
– Corriger et mettre à jour ses systèmes, y compris les solutions de sécurité et le logiciel antivirus.
– Déculpabiliser l'utilisateur final, afin qu'il n'ait pas peur de signaler l'attaque immédiatement.
– Bien gérer les privilèges des comptes d'administration.
– Désactiver les macros.
– Limiter le Byod à quelques périphériques et leur appliquer des politiques de sécurité strictes.

Article rédigé par Tim Greene / Network World (adaptation Jean Elyan)

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Ransomware : ne payez jamais la rançon – Le Monde Informatique*

Le cyber-espionnage, en tête des menaces en 2017 ?

Le cyber-espionnage, en tête des menaces en 2017 ?

Selon Trend Micro, l'augmentation des ransomware et des attaques menées par des Etats constituent un risque croissant pour les infrastructures critiques.

La dernière étude menée par Trend Micro, soutient que 20 % des entreprises mondiales classent le cyber-espionnage comme la plus forte menace pour leur activité, 26 % luttant pour suivre et anticiper l'évolution rapide des différentes menaces. Aux Etats-Unis, 20 % ont déjà subi une attaque de ce type en 2016.
L'étude révèle que le cyber-espionnage arrive en tête des préoccupations de sécurité pour 2017, suivi par les attaques ciblées (17 %) et le phishing (16 %). Les entreprises situées en Italie (36 %), en France (24 %), en Allemagne (20 %) et aux Pays-Bas (17 %) sont celles qui craignent le plus le cyber-espionnage, ce qui s'explique notamment par la tenue d'élections dans chacun de ces pays cette année.
Huit pays sur dix ont mentionné le caractère de plus en plus imprévisible des cybercriminels (36 %) comme étant le plus grand frein à la protection contre les cyber-menaces. Ils sont également 29 % à faire état de lacunes concernant la compréhension des dernières menaces, et 26 % à s'efforcer de suivre l'évolution rapide des menaces et la sophistication croissante des activités cybercriminelles.
Selon l'étude, près des deux tiers (64 %) des entreprises avaient subi une cyber-attaque majeure « connue » au cours des 12 derniers mois. En moyenne, elles en avaient même connu quatre. Les menaces de type ransomware étaient de loin les plus courantes, 69 % des personnes interrogées indiquant avoir été attaquées au moins une fois au cours de la période. En réalité, seul un quart (27 %) des entreprises interrogées n'avait pas été ciblé par un ransomware.

Autre fait notable : à peine 10 % des entreprises pensent que les attaques de type ransomware constitueront une menace en 2017, alors que l'année 2016 a été marquée par une augmentation de 748 % de ces attaques, avec 1 milliard de dollars de pertes pour les entreprises à travers le monde. On estime que le nombre de ransomware va augmenter d'encore 25 % en 2017, s'attaquant à divers appareils tels que les téléphones portables, les objets connectés (IoT) et les dispositifs d'IoT industriel (IIoT)…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Le cyber-espionnage, en tête des menaces en 2017 | Assurance & Banque 2.0*

Arnaques entre cybercriminels !

	Arnaques entre cybercriminels !

Les chercheurs de Kaspersky Lab ont découvert PetrWrap, une nouvelle famille de malware exploitant le module d'origine du ransomware Petya et distribuée via une plate-forme RaaS (Ransomware as a Service) pour mener des attaques ciblées contre des entreprises. Les créateurs de PetrWrap ont produit un module spécial qui modifie le ransomware Petya existant « à la volée », laissant les auteurs de ce dernier impuissants face à l'utilisation non autorisée de leur propre malware. Ce pourrait être le signe d'une intensification de la concurrence sur le marché souterrain du ransomware.

En mai 2016, Kaspersky Lab avait découvert le ransomware Petya, qui non seulement chiffre les données stockées sur un ordinateur mais écrase aussi le secteur d'amorce (MBR) du disque dur, ce qui empêche le démarrage du système d'exploitation sur les machines infectées. Ce malware est un modèle de RaaS (Ransomware as a Service), c'est-à-dire que ses créateurs proposent leur produit malveillant « à la demande », afin de le propager via de multiples distributeurs en s'octroyant un pourcentage des profits au passage. Pour s'assurer de recevoir leur part du butin, les auteurs de Petya ont inséré certains « mécanismes de protection » dans leur malware de façon à prévenir un usage non autorisé de ses échantillons. Les auteurs du cheval de Troie PetrWrap, dont les activités ont été détectées pour la première fois au début de 2017, sont parvenus à contourner ces mécanismes et ont trouvé un moyen d'exploiter Petya sans verser de redevance à ses auteurs.

Le mode de diffusion de PetrWrap reste à éclaircir. Après infection, PetrWrap lance Petya afin de chiffrer les données de sa victime, puis exige une rançon. Ses auteurs emploient leurs propres clés de chiffrement privées et publiques en lieu et place de celles fournies avec les versions « standard » de Petya. Cela leur permet d'exploiter le ransomware sans avoir besoin de la clé privée d'origine pour décrypter la machine de la victime, dans le cas où cette dernière paie la rançon…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *PetrWrap : des cybercriminels volent le code de ransomware d'autres criminels Le nouveau ransomware mène des attaques ciblées contre des entreprises – Global Security Mag Online*

Le Ransomware Dharma enfin décrypté

	Le Ransomware Dharma enfin décrypté

Les clés de déchiffrement du ransomware Dharma ainsi que toutes ses variantes ont été mises en ligne par un utilisateur. Kaspersky et Eset ont mis à jour leurs outils de lutte contre les ransomwares pour permettre à toute personne ou entreprise de déchiffrer gratuitement leurs fichiers chiffrés.

Les fournisseurs de sécurité dont Kaspersky et Eset ont mis à jour leurs outils pour permettre de déchiffrer les fichiers piégés par le ransomware Dharma. (crédit : D.R.)

C'est une belle victoire qui vient d'être remportée contre le diabolique ransomware Dharma. Les personnes ayant des fichiers chiffrés par ce programme peuvent en effet souffler car ils peuvent désormais avoir accès à des clés de déchiffrement pour pouvoir les retrouver. Apparu pour la première fois en novembre, Dharma est basé sur l'ancien programme de ransomware Crysis. Il est facile de le reconnaitre par l'ajout aux fichiers chiffrés de l'extension .[email_address].dharma. , l'adresse mail correspondant à celle utilisée par le pirate pour tenter d'extorquer sa victime.

Mercredi, un utilisateur sous le pseudonyme de gektar a publié un lien vers un post Pastbin sur le forum du support technique de BleepingComputer.com. Un post indiquant contenir les clés de déchiffrement du ransomware Dharma et de toutes ses variantes. Etrangement, la même chose s'est produite en novembre avec les clés de son prédécesseur, Crysis ce qui a permis à des chercheurs de créer des outils de déchiffrement. Aucune autre motivation que celle de mettre à disposition ces clés n'a été enregistrée concernant gektar. La bonne nouvelle est que ce leak a permis aux chercheurs de Kaspersky et d'Eset de vérifier son travail. Bingo : les deux sociétés ont mis à jour leurs outils de déchiffrement respectifs à savoir RakniDecryptor et CrysisDecryptor.

Une guerre des gangs dans les ransomwares

Cette situation devrait résonner à l'oreille des personnes touchées par des ransomwares qui ne devraient pas oublier de conserver une copie de leurs fichiers chiffrés à leur insu. Les chercheurs trouvent en effet parfois des failles dans les implémentations du chiffrement des ransomwares leur permettant de casser le chiffrement des clés. Dans d'autres cas, les autorités judiciaires et de police saisissent les serveurs de commande et de contrôle utilisés par les gangs de ransomware et publient ces clés.

Dans d'autres cas comme ici, les clés arrivent à la surface par d'autres moyens inexpliqués. Peut être parce que le développeur du ransomware a décidé de fermer boutique et décide de lâcher les clés, ou alors a-t-on à faire à une rivalité entre deux gangs de hackers qui se mettent des bâtons dans les roues pour court-circuiter l'activité des uns et des autres. Dans tous les cas, il est également recommandé de jeter un oeil sur le site NoMoreRansom.org, régulièrement mis à jour et proposant aussi bien des outils que des conseils pour lutter contre ces fichus ransomwares.

Article rédigé par Lucian Constantin / IDG News Service

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Un ransomware piège les Mac*

Les collectivités territoriales cibles des Pirates Informatiques

Les collectivités territoriales cibles des Pirates Informatiques

Si elles n'en ont pas toujours conscience, les collectivités territoriales peuvent bel et bien être victimes de cyberattaques. Et ce, pour de multiples raisons. En cas de faute avérée, les sanctions encourues peuvent devenir particulièrement difficiles à assumer.

Par Pierre-Alexandre Conte

Une République numérique. C'est ainsi qu'a été baptisée la loi portée par l'actuelle secrétaire d'Etat chargée du numérique, Axelle Lemaire, parue le 8 octobre 2016 au « Journal officiel ». Un nom ô combien symbolique et révélateur de la profondeur de la transformation vécue par l'ensemble de la société.

Celle-ci touche naturellement les collectivités territoriales, qui bénéficient des multiples avantages qu'elle génère, mais qui doivent, dans le même temps, composer avec de nouvelles obligations. Parmi elles, figure en tête de liste la sécurisation de leur système d'information.

En préambule de son rapport d'activité annuel paru en 2016, l'Agence nationale de la sécurité des systèmes d'information (Anssi) introduisait le sujet comme suit : « Les technologies numériques procurent des gains de productivité et sont donc source de richesse et de compétitivité pour notre pays, mais elles induisent également des vulnérabilités nouvelles. La cybersécurité est devenue, de ce fait, une condition structurante, non seulement de la sauvegarde de notre patrimoine économique et intellectuel, mais aussi de la protection physique de nos concitoyens. » Des propos signés Louis Gautier, secrétaire général de la défense et de la sécurité nationale.

FOCUS

Dans son rapport d'activité concernant l'année 2015, l'**Anssi** explique avoir reçu 4 000 signalements, soit 50 % de plus qu'en 2014. L'Agence a aussi dû traiter une vingtaine d'incidents de sécurité majeurs.

Les sites web en première ligne

La première erreur en matière de sécurité informatique consiste à penser qu'une collectivité, quelle que soit sa nature, n'a aucune raison d'être la cible d'une attaque. C'est pourtant un raisonnement fréquemment rencontré au sein des petites et moyennes communes, qui considèrent parfois qu'elles ne détiennent rien qui puisse intéresser d'hypothétiques assaillants. « Comme tout un chacun qui dispose d'une visibilité sur internet, les collectivités territoriales peuvent faire partie des victimes d'une vague d'attaques, précise Guy Flament, référent de l'Anssi au sein de la région Nouvelle Aquitaine.

Leur présence sur internet, notamment par le biais de leurs sites web, offre des surfaces pour les attaquants, qui peuvent leur permettre d'afficher des messages de revendication ou de propagande. Ensuite, les collectivités subissent des attaques par des « rançongiciels » qui prennent en otage leur système d'information et offrent de le libérer contre une rançon. En ce qui concerne les autres menaces informatiques que peuvent être le sabotage ou l'espionnage, elles ne sont pas, pour le moment, particulièrement visées. Mais elles pourraient le devenir, notamment à cause du nombre de données à caractère personnel qu'elles hébergent. »

À LIRE AUSSI

• Plusieurs milliers de sites Internet de communes mal sécurisés

Les collectivités territoriales brassent en effet de plus en plus de données, dont certaines s'avèrent particulièrement sensibles. Elles sont au cœur de toutes les préoccupations, comme en témoignent les nombreux articles qui leur sont consacrés au sein de la loi pour une République numérique. Il convient donc de les protéger.

« Les collectivités détiennent notamment l'état civil. Il ne faudrait pas qu'un jour ces fichiers puissent être modifiés par des attaquants. Les comptes de la commune intéressent aussi les gens et tout ce qui touche aux dossiers de consultation publique », lance Guy Flament.

À LIRE AUSSI

Notre dossier : Données personnelles, un gisement sous haute protection

Sanctions pénales

La protection des données du citoyen est garantie par la loi « informatique et libertés ». C'est évidemment la Commission nationale de l'informatique et des libertés (Cnil) qui veille au respect de cette dernière. Ses compétences ont été élargies par la loi pour une République numérique.

Sur le plan financier, les collectivités encourent une amende pouvant s'élever jusqu'à 3 millions d'euros ; ce n'est pas rien ! La Cnil peut aussi ordonner que l'organisme sanctionné informe à ses frais les victimes. La loi prévoit par ailleurs la possibilité de sanctionner pénalement les maires, les présidents de conseils régionaux et de conseils généraux en cas de manquement grave, comme le fait de ne pas prendre les mesures nécessaires pour garantir la confidentialité des informations ou l'utilisation de ces dernières à d'autres fins.

A partir du mois de mai 2018, les collectivités devront appliquer le règlement européen sur le sujet. Concernant ce dernier, selon Pierre Deprez, avocat du cabinet DS avocats dans le département « droit de la propriété intellectuelle, technologies numériques et data », on parle d'un « changement de paradigme ». Cela signifie le passage « d'un régime de déclaration et d'autorisation des traitements à un régime d'accountability, d'autoresponsabilité ».

Les communes devront conserver « une trace des moyens techniques et organisationnels qu'elles auront mis en œuvre pour assurer la sécurité des données », dans le but de montrer patte blanche en cas de contrôle.

Mais les données ne sont pas l'unique préoccupation des collectivités. D'autres domaines requièrent leur attention, à l'image des objets connectés. Ce sont de formidables outils, mais ils peuvent aussi se retourner contre ceux qui les utilisent.

« Les objets connectés, comme les smartphones il y a quelques années, représentent une augmentation de la surface d'attaque puisqu'ils sont, par nature, connectés à internet. Si ces objets ne sont pas correctement configurés et sécurisés, ils offrent une porte d'entrée à d'éventuels attaquants », précise Guy Flament.

Des risques divers

« L'émergence des outils connectés implique de prendre ses précautions, déclare de son côté Olivier Fouqueau, directeur général des services d'Infocom94, syndicat intercommunal informatique du Val-de-Marne. Quand une direction générale des services techniques, voire un élu, décide que c'est super d'équiper toutes les places de parking d'un capteur pour permettre de savoir, à distance, par le biais de son téléphone portable, s'il y a une place pour se garer, mais qu'il n'y a pas de sécurité autour, cela peut très vite devenir difficile à gérer. »

Les rapports affirmant que la cybercriminalité est en constante augmentation sont rendus publics de manière quasi quotidienne. Pour autant, il n'est pas si évident de trouver une collectivité territoriale qui accepte de faire part d'une mauvaise expérience. La raison est simple : elle relève de la peur de voir son image se détériorer. C'est là l'un des principaux risques encourus, notamment par les villes.

« Il ne se passe pas une journée sans qu'il y ait un site internet défiguré dans la région », déplore le référent de l'Anssi en Nouvelle Aquitaine. En cas de pertes de données et de responsabilité avérée, le règlement européen demandera également aux collectivités, en 2018, d'informer le public quant à ses failles de sécurité. Si les communes sont concernées par leur image, elles doivent en plus composer avec l'inaccessibilité de leur site. Ce qui peut altérer de manière plus ou moins grave la mission de service public.

La perte peut aussi être financière, notamment s'il y a demande de rançon, les sommes demandées étant, la plupart du temps, élevées.

« Le sujet de la sécurité est souvent diabolisé, regrette Frank Mosser, expert dans le domaine de la cybersécurité et président de MGDIS, société éditrice de services logiciels de pilotage et de valorisation de l'action publique, basée à Vannes. Quand ça fait trop peur, on a tendance à mettre la tête dans le sac et à faire l'autruche. Il y a quelques années, ce n'était pas si grave que cela. Là, ça le devient un peu plus. »

FOCUS

Le « rançongiciel », fléau international en pleine expansion

Extorsion Tout le monde ou presque a entendu parler de Locky. Ce « ransomware » – « rançongiciel » en français – s'est rendu populaire en faisant de nombreuses victimes au cours de l'année passée. Une fois activé sur l'ordinateur de la personne visée, ce dernier chiffre les données et demande une somme d'argent en échange de leur restitution. S'il reste l'exemple le plus connu, Locky n'est pas un cas unique. Loin de là.

290 millions de dollars – Le FBI estime que durant le premier trimestre de l'année 2016, environ 209 millions de dollars ont été extorqués par le biais de « rançongiciels ». Aux Etats-Unis, le Hollywood Presbyterian Medical Center a fait partie des victimes au mois de février 2016. Paralysé pendant plus d'une semaine, il avait fini par débourser la somme de 17 000 dollars pour reprendre une activité normale. Et ce, après avoir dû envoyer de nombreux patients vers d'autres établissements.

Une mésaventure similaire est arrivée trois mois plus tard au Kansas Heart Hospital. Mais cette fois, après avoir payé la rançon, l'hôpital n'a pas pu récupérer ses fichiers. Pire, une seconde somme d'argent lui a été demandée. Fin janvier, c'est la police de Washington qui s'est aperçue que le réseau de vidéosurveillance de la ville ne fonctionnait plus correctement. Avant de prendre connaissance du problème : depuis le 12 janvier, un « ransomware » avait commencé à faire son œuvre, paralysant 123 des 187 caméras utilisées. En cherchant la source du dysfonctionnement, des enquêteurs sont tombés un peu plus tard sur un message les invitant à payer une somme. Ce qui n'a pas été fait. Le réseau a été réinstallé dans l'urgence.

FOCUS

L'expérience traumatisante d'une commune piratée

Chaque jour ou presque, des collectivités découvrent qu'elles ont été victimes d'une attaque informatique. Mais difficile de témoigner à visage découvert. Voici ce qu'une victime raconte, sous couvert d'anonymat : « Nous sommes arrivés un matin et nos postes informatiques étaient bloqués, explique cette directrice générale des services. Impossible de travailler dans ces conditions. Sur les écrans était affiché un message énigmatique et surtout, une demande de rançon. »

Si la police a rapidement été prévenue, la commune a dû se résoudre à trouver une solution au plus vite pour reprendre une activité normale. « Nous ne pouvions pas payer la somme, explique-t-elle. Nous avons appelé notre prestataire informatique qui a fait le déplacement et nous a indiqué qu'une grande partie de nos données, notamment les plus récentes, étaient perdues.

Personne n'avait anticipé le problème. Cela a créé beaucoup de remous au sein de la collectivité, dans la mesure où nous ne savons pas qui est responsable de l'attaque. L'enquête est toujours en cours. Plusieurs pistes ont été évoquées, dont des personnes hostiles à certaines décisions locales. C'est une expérience qui reste encore assez traumatisante pour nous. »

Si le prestataire informatique a fourni une solution d'appoint pour que les données soient plus fréquemment sauvegardées, aucun changement en profondeur, en termes de sécurité, n'a été apporté à ce jour.

A Lire aussi :

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Le RGPD, règlement européen de protection des données. Comment devenir DPO ?

Comprendre le Règlement Européen sur les données personnelles en 6 dessins

Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Cybersécurité : les collectivités territoriales, des cibles potentielles sous surveillance*

En 2016, les ransomwares sous Android ont augmenté de plus de 50%

	En 2016, les ransomwares sous Android ont augmenté de plus de 50%

Basé sur sa technologie LiveGrid®, ESET® publie un rapport sur les menaces Android™ : sur l'ensemble des logiciels malveillants détectés en 2016, la catégorie ransomware a augmenté de plus de 50% par rapport à 2015, le plus fort taux de menaces enregistré.

« Au total, nous avons constaté **une augmentation de près de 20% des logiciels malveillants** (tous confondus) **sous Android en un an.** Sur cette plateforme, les ransomwares sont ceux qui se sont le plus développés. Selon le FBI (1), cette menace aurait rapporté jusqu'à 1 milliard de dollars aux cybercriminels l'année dernière. Avec une forte augmentation au cours du premier semestre 2016, nous pensons que cette menace ne disparaîtra pas de sitôt », déclare Juraj MALCHO, Chief Technology Officer chez ESET et qui abordera ce sujet lors du Mobile World Congress 2017.

Au cours des 12 derniers mois, **les cybercriminels ont reproduit des techniques identiques à celles utilisées pour la conception de malwares infectant des ordinateurs**, afin de concevoir leurs propres logiciels malveillants sur Android : écran de verrouillage, cyrpto-ransomwares… Ainsi, ils ont réussi à développer des méthodes sophistiquées permettant de cibler uniquement les utilisateurs des différentes versions de cette plateforme.
En plus d'utiliser des techniques d'intimidation comme le « Police ransomware (2) », les cybercriminels chiffrent et cachent la charge utile malveillante sous l'application compromise, afin de rendre sa présence indétectable.
D'après les observations d'ESET, les ransomwares sous Android se concentraient sur l'Europe de l'EST puis sur les Etats-Unis en 2015, avant de migrer vers le continent asiatique en 2016. « Ces résultats montrent la vitesse de propagation de cette menace, active à l'échelle mondiale », ajoute Juraj MALCHO.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

=

Réagissez à cet article

Source : *Boîte de réception (252) – denis.jacopini@gmail.com – Gmail*

Autopsie d’un virus qui se cache dans les pixels d’une publicité

	Autopsie d’un virus qui se cache dans les pixels d’une publicité

Soyez prudents ! Les pirates informatiques sont très inventifs, et là, ils nous font, une fois de plus, la démonstration qu'ils sont de plus en plus malins. En effet, un laboratoire de sécurité a découvert un logiciel malveillant qui se cache dans les pixels composant l'image d'une publicité. Ce virus profite en fait d'une faille du navigateur Internet Explorer et de Flash Player, ce petit complément vous permettant notamment d'afficher des vidéos sur les pages que vous visitez.

Et parce qu'il s'intègre dans une photo, ce virus a été baptisé Stegano, en référence à la technique de la sténographie qui permet de dissimuler des informations secrètes dans des supports anodins. Très concrètement, vous ouvrez votre navigateur, quelques clics au cours d'une recherche et vous arrivez sur une page sur laquelle va aussi s'afficher une bannière publicitaire. Et du coup, le processus d'exécution du logiciel malveillant va se mettre en route. Il va d'abord vérifier si votre navigateur lui permet de s'installer et il va aussi récolter quelques informations au sujet de votre ordinateur.
Si ces informations sont favorables à la poursuite du processus, l'image de la publicité va être remplacée par une image similaire mais légèrement modifiée. Même en zoomant, la différence n'est pas facile à percevoir. Et c'est via cette image que l'installation va se poursuivre.
Durant cette seconde phase, le niveau de sécurité de votre ordinateur va être testé. Si la voie est libre, la dernière phase consistant à installer le logiciel malveillant va se déclencher. Ce dernier permettra, par exemple, aux pirates de collecter des données personnelles ou encore d'ouvrir une porte dérobée sur votre ordinateur pour en permettre l'accès et ceci, sans attirer votre attention.
Il est aussi possible que certains des internautes touchés voient leur ordinateur infecté par un logiciel qui va crypter les données, ce qui permet ensuite aux pirates de réclamer une rançon pour obtenir la clef permettant de les récupérer…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Virus informatique: attention Stegano se cache dans les pixels d'une publicité*

Rapport 2017 sur la Cyber Sécurité de F-Secure

	Rapport 2017 sur la Cyber Sécurité de F-Secure

F-Secure vient de publier son Rapport 2017 sur la Cyber Sécurité qui décrit et analyse l'état actuel de la cyber sécurité dans le monde. Ce rapport s'attarde en particulier sur les problèmes que rencontrent les entreprises, dans un contexte où les pirates délaissent les malware conventionnels au profit d'attaques plus sophistiquées, et donc encore plus dangereuses.

« Les menaces actuelles peuvent déjouer les approches unilatérales classiques de la sécurité, même les plus efficaces. En ayant recours au phishing (avec désormais des listes, vendues en ligne, de comptes ou réseaux pré-exposés) ou via d'autres méthodes, les pirates peuvent beaucoup plus facilement viser un gouvernement ou une entreprise du Fortune 500 », explique Sean Sullivan, Security Advisor chez F-Secure. « Nous vivons dans un monde post-malware, où le piratage s'est industrialisé. Et les cyber criminels ne comptent plus seulement sur les malware les plus communs pour se faire de l'argent. »

Ce rapport offre une analyse détaillée des problèmes majeurs diagnostiqués par les chercheurs et experts sur le plan de la cyber sécurité. Parmi les principaux résultats :

• Une grande partie du trafic de reconnaissance active en 2016 était liée à des adresses IP majoritairement situées dans 10 pays, et notamment la Russie, les Pays-Bas, les États-Unis, la Chine ou encore l'Allemagne.

• Les versions obsolètes d'Android sont de plus en plus nombreuses et rendent les appareils mobiles particulièrement exposés. L'Indonésie possède le nombre le plus important d'appareils Android non mis à jour, la Norvège, le plus faible.

• La plupart des cyber attaques font appel à des techniques basiques et s'en prennent à des infrastructures peu robustes.

• 197 nouvelles familles de ransomware ont été découvertes en 2016, contre seulement 44 en 2015.

• Le recours aux exploit kits a diminué au cours de 2016.

Ce rapport relate également les évènements marquants et les tendances de l'année 2016. Au programme : des informations sur les botnets de type Mirai, sur les attaques préparées en amont, sur le cyber crime et sur les dernières tendances globales en matière de cyber menaces. Certaines organisations comme l'Autorité finlandaise de régulation des communication, le Virus Bulletin ou encore AV-Test, ont contribué à ce rapport à travers plusieurs articles…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Nouveau Rapport F-Secure sur la Cyber Sécurité : un monde « post-malware » – Global Security Mag Online*

Ransomwares : Pourquoi les entreprises préfèrent-elles payer ?

	Ransomwares : Pourquoi les entreprises préfèrent-elles payer ?

Le ransomware, 1ère menace informatique en Europe et « machine à cash » pour les cybercriminels : pourquoi les entreprises préfèrent-elles payer ? par Désirée Rodriguez

Pour Europol (Rapport annuel cybercriminalité 2016), le « *ransomware est devenu la première menace en Europe* » et les faits vont empirer dans les mois et années à venir. Régis Bénard, consultant technique du spécialiste français Vade Secure (leader mondial des solutions de protection des boîtes de messagerie contre ce type de menaces) confirme cette tendance qui n'est pas prête de laisser sa place puisqu'encore aujourd'hui, et malgré une hausse de la sensibilisation, les entreprises préfèrent souvent payer plutôt que de perdre du temps… et de l'argent. C'est tout le dilemme du ransomware.

« **Pour maximiser leurs profits, les cybercriminels innovent en permanence** »
Les cybercriminels sont organisés comme de vraies entreprises du crime numérique avec un accent très fort mis sur l'innovation pour maximiser leurs résultats.
Actuellement, Cerber est le ransomware le plus actif en France. Connu dans le monde entier, Cerber a notamment initié le concept du *ransomware-as-a-service*. L'idée est simple mais terriblement efficace : pour maximiser leurs profits, les cybercriminels proposent à des volontaires de diffuser le ransomware dans leur propre pays. Depuis 2016, Cerber est également une véritable entreprise du cybercrime avec un marketing quasi professionnel, un service après-vente qui propose d'accueillir les victimes pour les aider à payer leur rançon, etc.

« Locky, endormi ? Le ransomware le plus célèbre en France n'a pas fini de faire parler de lui »

Le ransomware le plus présent en France en 2016, marque une pause. Mais l'accalmie ne va malheureusement pas durer. L'année dernière, Locky avait déjà connu des périodes d'absence quasi totale. Plusieurs raisons peuvent expliquer ce ralentissement de l'activité de Locky mais la plus évidente est que les cybercriminels travaillent à des évolutions sur leur ransomware. Il va donc revenir prochainement sous une autre forme et donc encore plus fort. Deuxième explication possible : les réseaux de PC ou objets connectés piratés (botnets) pour diffuser en masse les attaques de Locky, ne sont pas disponibles car loués à d'autres cybercriminels ».

« L'humain : la protection la plus efficace contre les attaques de phishing et ransomware »

Les ransomware sont véhiculés par des emails de phishing ou spear phishing (D'après le Gartner 65 % des attaques informatiques étaient initiées par un phishing en 2015 alors qu'une étude récente de PhishMe souligne la montée en puissance du phishing puisque 91% des attaques informatiques commencent aujourd'hui par du phishing). L'email est donc le canal prioritaire utilisé par les cybercriminels pour piéger les entreprises. Le problème est que l'humain est loin d'être infaillible : plusieurs études le rappellent régulièrement.
Les failles humaines peuvent ainsi aller jusqu'à mettre en péril une entreprise. Alors que le nombre de victimes continue d'augmenter, il est temps d'accélérer la résistance pour ne plus tomber dans le piège. Et pour mieux se protéger, l'éducation et la formation des utilisateurs sont des axes primordiaux pour que chacun prenne conscience des enjeux et des risques.
Pour les entreprises tout comme pour les pouvoirs publics, il s'agit d'organiser des réunions d'information régulières sur la sécurité, des formations sur le phishing, des recommandations sur le bon usage des réseaux sociaux, sur des conseils de bon sens, ou sur des bonnes pratiques à mettre en place : n'ouvrir les pièces jointes suspectes que si l'expéditeur est confirmé, supprimer le message d'un expéditeur suspect inconnu sans y répondre, etc…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Le ransomware, 1ère menace informatique en Europe et « machine à cash » pour les cybercriminels : pourquoi les entreprises préfèrent-elles payer ? – Globb Security FR*