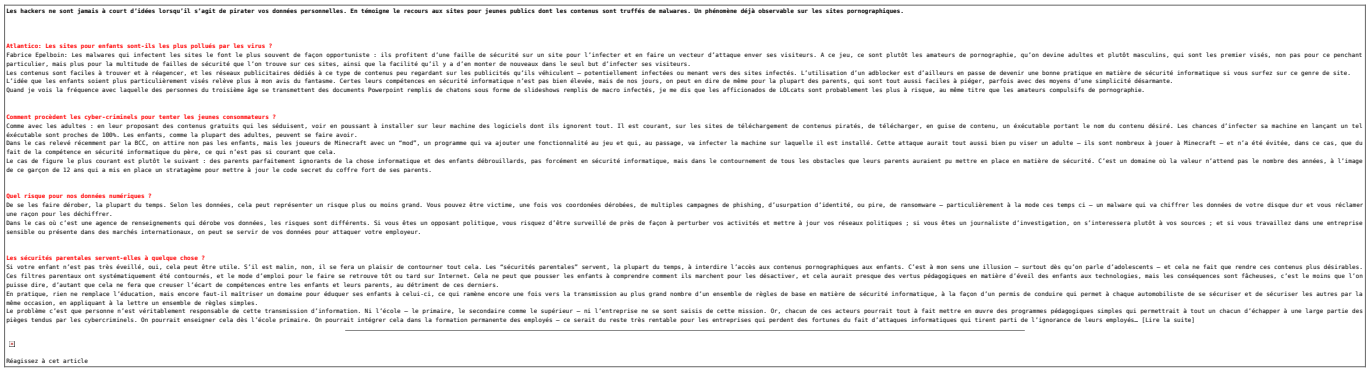
Les sites pour enfants se transformeraient-ils en pièges pour voler les données personnelles de leurs parents ?

Les sites pour enfants se transformeraient-ils en pièges pour voler les données personnelles de leurs parents ?



Les hackers ne sont jamais à court d'idées lorsqu'il s'agit de pirater vos données personnelles. En témoigne le recours aux sites pour jeunes publics dont les contenus sont truffés de malwares. Un phénomène déjà observable sur les sites pornographiques.

Atlantico: Les sites pour enfants sont-ils les plus pollués par les virus ?

Fabrice Epelboin: Les malwares qui infectent les sites le font le plus souvent de façon opportuniste : ils profitent d'une faille de sécurité sur un site pour l'infecter et en faire un vecteur d'attaque enver ses visiteurs. A ce jeu, ce sont plutôt les amateurs de pornographie, qu'on devine adultes et plutôt masculins, qui sont les premier visés, non pas pour ce penchant particulier, mais plus pour la multitude de failles de sécurité que l'on trouve sur ces sites, ainsi que la facilité qu'il y a d'en monter de nouveaux dans le seul but d'infecter ses visiteurs.
Les contenus sont faciles à trouver et à réagencer, et les réseaux publicitaires dédiés à ce type de contenus peu regardant sur les publicités qu'ils véhiculent – potentiellement infectées ou menant vers des sites infectés. L'utilisation d'un adblocker est d'ailleurs en passe de devenir une bonne pratique en matière de sécurité informatique si vous surfez sur ce genre de site.
L'idée que les enfants soient plus particulièrement visés relève plus à mon avis du fantasme. Certes leurs compétences en sécurité informatique n'est pas bien élevée, mais de nos jours, on peut en dire de même pour la plupart des parents, qui sont tout aussi faciles à piéger, parfois avec des moyens d'une simplicité désarmante.
Quand je vois la fréquence avec laquelle des personnes du troisième âge se transmettent des documents Powerpoint remplis de chatons sous forme de slideshows remplis de macro infectés, je me dis que les afficionados de LOLcats sont probablement les plus à risque, au même titre que les amateurs compulsifs de pornographie.

Comment procèdent les cyber-criminels pour tenter les jeunes consommateurs ?

Comme avec les adultes : en leur proposant des contenus gratuits qui les séduisent, voir en poussant à installer sur leur machine des logiciels dont ils ignorent tout. Il est courant, sur les sites de téléchargement de contenus piratés, de télécharger, en guise de contenu, un éxécutable portant le nom du contenu désiré. Les chances d'infecter sa machine en lançant un tel éxécutable sont proches de 100%. Les enfants, comme la plupart des adultes, peuvent se faire avoir.
Dans le cas relevé récemment par la BCC, on attire non pas les enfants, mais les joueurs de Minecraft avec un "mod", un programme qui va ajouter une fonctionnalité au jeu et qui, au passage, va infecter la machine sur laquelle il est installé. Cette attaque aurait tout aussi bien pu viser un adulte – ils sont nombreux à jouer à Minecraft – et n'a été évitée, dans ce cas, que du fait de la compétence en sécurité informatique du père, ce qui n'est pas si courant que cela.
Le cas de figure le plus courant est plutôt le suivant : des parents parfaitement ignorants de la chose informatique et des enfants débrouillards, pas forcément en sécurité informatique, mais dans le contournement de tous les obstacles que leurs parents auraient pu mettre en place en matière de sécurité. C'est un domaine où la valeur n'attend pas le nombre des années, à l'image de ce garçon de 12 ans qui a mis en place un stratagème pour mettre à jour le code secret du coffre fort de ses parents.

Quel risque pour nos données numériques ?

De se les faire dérober, la plupart du temps. Selon les données, cela peut représenter un risque plus ou moins grand. Vous pouvez être victime, une fois vos coordonnées dérobées, de multiples campagnes de phishing, d'usurpation d'identité, ou pire, de ransomware – particulièrement à la mode ces temps ci – un malware qui va chiffrer les données de votre disque dur et vous réclamer une rançon pour les déchiffrer.
Dans le cas où c'est une agence de renseignements qui dérobe vos données, les risques sont différents. Si vous êtes un opposant politique, vous risquez d'être surveillé de près de façon à perturber vos activités et mettre à jour vos réseaux politiques ; si vous êtes un journaliste d'investigation, on s'interessera plutôt à vos sources ; et si vous travaillez dans une entreprise sensible ou présente dans des marchés internationaux, on peut se servir de vos données pour attaquer votre employeur.

Les sécurités parentales servent-elles à quelque chose ?

Si votre enfant n'est pas très éveillé, oui, cela peut être utile. S'il est malin, non, il se fera un plaisir de contourner tout cela. Les "sécurités parentales" servent, la plupart du temps, à interdire l'accès aux contenus pornographiques aux enfants. C'est à mon sens une illusion – surtout dès qu'on parle d'adolescents – et cela ne fait que rendre ces contenus plus désirables. Ces filtres parentaux ont systématiquement été contournés, et le mode d'emploi pour le faire se retrouve tôt ou tard sur Internet. Cela ne peut que pousser les enfants à comprendre comment ils marchent pour les désactiver, et cela aurait presque des vertus pédagogiques en matière d'éveil des enfants aux technologies, mais les conséquences sont fâcheuses, c'est le moins que l'on puisse dire, d'autant que cela ne fera que creuser l'écart de compétences entre les enfants et leurs parents, au détriment de ces derniers.
En pratique, rien ne remplace l'éducation, mais encore faut-il maîtriser un domaine pour éduquer ses enfants à celui-ci, ce qui ramène encore une fois vers la transmission au plus grand nombre d'un ensemble de règles de base en matière de sécurité informatique, à la façon d'un permis de conduire qui permet à chaque automobiliste de se sécuriser et de sécuriser les autres par la même occasion, en appliquant à la lettre un ensemble de règles simples.
Le problème c'est que personne n'est véritablement responsable de cette transmission d'information. Ni l'école – le primaire, le secondaire comme le supérieur – ni l'entreprise ne se sont saisis de cette mission. Or, chacun de ces acteurs pourrait tout à fait mettre en œuvre des programmes pédagogiques simples qui permettrait à tout un chacun d'échapper à une large partie des pièges tendus par les cybercriminels. On pourrait enseigner cela dès l'école primaire. On pourrait intégrer cela dans la formation permanente des employés – ce serait du reste très rentable pour les entreprises qui perdent des fortunes du fait d'attaques informatiques qui tirent parti de l'ignorance de leurs employés… [Lire la suite]

Réagissez à cet article

Fabrice Epelboin est enseignant à Sciences Po et cofondateur de Yogosha, une startup à la croisée de la sécurité informatique et de l'économie collaborative.

Source : *Quand les sites pour enfants se transforment en pièges pour voler les données personnelles de leurs parents | Atlantico.fr*

2ème édition du Forum TAC, Technology Against Crime les 28 et 29 avril prochains à Lyon

INNOVER POUR UN MONDE PLUS SUR, Tel est le slogan de la 2ème édition du Forum TAC, Technology Against Crime qui réunit les acteurs mondiaux de la Sécurité à Lyon, les 28 et 29 avril prochains

Après le succès de la 1ère édition de 2013, le Forum international TAC, Technology Against Crime revient à Lyon en 2016, en présence du ministre de l'Intérieur, Bernard Cazeneuve, pour répondre à deux grands enjeux :
1/ Anticiper les menaces et répondre aux grands enjeux de sécurité
2/ Identifier et mettre en lumière les solutions de demain
Organisé autour de 3 menaces : cyber – crime organisé – terrorisme et de 3 solutions : l'innovation technologique – la coopération public/privé – la coordination internationale.
Le Forum TAC met en relation les besoins des donneurs d'ordres publics et privés et les solutions proposées par les entreprises et crée ainsi un dialogue de haut niveau axé sur la performance et l'innovation en matière de sécurité. Un événement au format unique qui associe des rendez-vous d'affaires, un Forum Innovation, des démonstrations, un espace networking, des cas pratiques et des interventions de haut niveau.

500 participants sont attendus :
• ministres, représentants d'Interpol et délégations officielles de plus de 190 pays
• forces de police et de sûreté internationales
• dirigeants et responsables de la sécurité de grands groupes industriels
• fournisseurs de solutions et services
• représentants institutionnels

Parmi les nombreux sujets traités :
• La protection des avions face aux cyber-attaques
• Le trafic d'êtres humains
• Le maintien de l'ordre et l'utilisation des media sociaux
• La protection des sites sensibles

En savoir plus : www.forum-tac.com

Réagissez à cet article

Source : Denis JACOPINI

Que risquent les enfants sur les réseaux sociaux ?

Que risquent les enfants sur les réseaux sociaux ?

Avoir des profils dans les réseaux sociaux peut représenter de nombreux dangers pour les enfants.
Denis JACOPINI, expert Informatique assermenté spécialisé en cybercriminalité a souhaité couvrir le sujet et a collecté quelques informations bien utiles pour comprendre le phhénomène.

Quels sont les risques d'une trop grande exposition sur les réseaux sociaux?

Attardons nous rapidement sur quelques analyses bien inquiétantes :
• 38% des 9-12 ans ont un profil sur un réseau social, alors que la plupart de ces réseaux ne sont autorisés qu'à partir de 13 ans !
• 77% des 13-16 ans sont présents !
• 1/4 ont un profil public ;
• 1/5 y communique son adresse, son numéro de téléphone…
• Seulement 55% des jeunes discutent avec leurs parents de ce qu'ils font sur Facebook ;
• 92% des jeunes de 8 – 17 ans utilisent leur vraie identité sur Facebook et livrent des informations personnelles ;
• 25% des jeunes de 8 – 17 ans disent avoir déjà été victimes d'insultes ou rumeurs sur Facebook ;
• 36% ont déjà été choqués par certains contenus.

1°/ Les jeunes, trop peu sensibilisés, ont tendance à communiquer bien trop d'éléments (photos, éléments de leur vie). L'effet immédiat est que les cybercriminels auront tous les éléments dont ils auront besoin pour pouvoir usurper leur identité.

2°/ Sur Internet, tout peut être copié collé (et altéré dans le processus), il n'y a aucune garantie de confidentialité dans les échanges électroniques via les réseaux sociaux. Des photos prises lors de soirées ou dénudées peuvent facilement se retrouver à la vue de tout le monde, tout comme un message insultant, écrit dans un moment d'énervement. Les jeunes n'hésitent pas à « taguer » des amis sur les photos de groupe, sans se rendre compte que cette action impacte directement la vue privée des amis tagués.

3°/ Autre risque bien réel, s'exposer sur les réseaux sociaux augmente le risque de contact avec un pédophile cherchant avant tout à rencontrer des enfants ou des ados naïfs, crédules ou confiants.

4°/ Autre faits inquiétants, 25% des jeunes de 8 – 17 ans disent avoir déjà été victimes d'insultes ou rumeurs sur Facebook. Les cyberviolences, souvent initiée à l'école est souvent poursuivies sur les réseaux sociaux sont très courantes. Une publication d'albums de photos de vacances ou d'une soirée entre amis peut vite déraper et se transformer en détournement obscène en ligne avec un impact sur la vie réelle. Intimidations, insultes, piratage de compte, commentaires humiliants, création de groupes de discussion pour moquer la victime – la violence des rapports entre jeunes peut pousser la victime jusqu'au suicide.
Le phénomène d'entraînement peut conduire les plus influençables à imiter des comportements violents et à se lancer dans des campagnes d'insultes contre le bouc émissaire désigné par le leader du groupe.

5°/ Enfin, risque souvent méconnu, les cybercriminels rivalisent d'ingéniosité pour concevoir des messages séduisants qui invitent à « Liker » un post viral avec un lien corrompu, des applications contenant des virus, des campagnes de phishing pour soutirer les informations de connexion, etc.

A la suite d'une exposition trop massive sur les réseaux sociaux, est-ce qu'un nouveau type de criminalité est né ?
Je répondrais à celà qu'un nouveau terrain de jeu est né !
Un espace rempli de prédateurs ou les jeunes sont des proies potentielles.

Comment optimiser la sécurité sur les réseaux sociaux?
Limitez la navigation et les échanges dans un périmètre adapté à l'âge et aux besoins du jeune. Si besoin, bloquez les réseaux sociaux jusqu'à ce qu'il soit en mesure de comprendre l'impact de ses interactions en ligne.
Discutez régulièrement avec votre enfant ou ado de ce qu'il fait sur Internet : quels sites il aime consulter, avec qui il tchatte, ce qu'il ou elle a découvert de nouveau. Expliquez-lui la différence entre de vrais amis et des connaissances numériques.
Apprenez aux enfants l'importance de la protection des informations personnelles, que ce soit les leurs ou celles de leurs amis. Informer le monde que l'on est seul ce week-end n'est peut être pas l'action la plus prudente, tout comme « taguer » ses amis sur une photo peu valorisante.
Vérifiez que les paramètres de protection de vie privée sont activés sur toutes les plates-formes utilisées par l'enfant. Expliquez que les traces numériques resteront dans le temps et qu'ils seront un jour ou l'autre confrontés à leurs actions en ligne. Soulignez l'importance de mesurer ses propos et de ne pas participer aux chasses à l'homme digitales.
Expliquez au jeune que si jamais il (ou elle) est victime d'harcèlement, ou bien s'il voit ses camarades s'acharner contre quelqu'un, il doit avertir le plus rapidement un adulte, parents ou professeur.
Souvent les enfants n'osent pas avouer, par honte ou bien parce qu'ils sont manipulés par les harceleurs.
Pour plus d'informations, consultez le site du Ministère de l'Éducation Nationale Agir Contre le Harcèlement à L'École (http://www.agircontreleharcelementalecole.gouv.fr).

Réagissez à cet article

Sources :

Denis JACOPINI

http://www.e-enfance.org/actualite/enfants-et-reseaux-sociaux-prudence-_151.html

http://www.e-enfance.org/enfants-danger-reseaux-sociaux.php

http://www.witigo.eu/controle-parental/dangers-reseaux-sociaux

Comment limiter simplement

les risques de piratage informatique en entreprise ?

	**Comment limiter simplement les risques de piratage informatique en entreprise ?**

La plupart du temps, les entreprises redoutent les cyberattaques provenant de l'extérieur. Pourtant, le personnel opérant dans les murs disposent souvent de droits d'accès excessifs par rapport à leurs rôles, et constituent le vecteur le plus probable de défaillances de sécurité, que ce soit en s'impliquant activement dans des activités malveillantes ou, plus souvent, en devenant inconsciemment les fournisseurs de comptes piratés et des droits associés. Entre 50% et 70 % des attaques réussies sont attribués à des utilisateurs internes. D'où la nécessité d'adopter un système IAM pour gérer dans les règles de l'art les identités des utilisateurs, et surveiller en permanence leurs droits d'accès aux ressources informatiques.

En collectant l'ensemble des informations liées à la structure d'autorisations, les solutions d'Identity and Access Intelligence offrent une vue d'ensemble des droits d'accès et des risques associés. Ces solutions disposent d'une ergonomie moderne et intuitive pour explorer, manipuler et restituer les données. S'appuyer sur des analyses approfondies et exhaustives facilite très largement le contrôle et l'audit des risques, la prise de décision et la gouvernance.
Ce guide pratique revient sur les principes de base de l'Identity and Access Intelligence. Il fournit un cadre simple pour aider votre entreprise à identifier les risques associés aux utilisateurs et liés à leurs droits d'accès.

1. Analyser les données de droits d'accès et évaluer les risques associés
Les solutions d'Identity and Access Intelligence s'appuient sur les technologies de business intelligence pour collecter les données d'identités et d'accès existantes, et les convertir en informations qualitatives facilitant la prise de décision. Elles fournissent à leurs utilisateurs une vue à 360° de toutes les informations liées aux droits d'accès (utilisateurs, rôles, groupes, ressources…) qui permet de naviguer de manière active au sein de ces données. Ils pourront les analyser depuis de multiples angles et axes à l'aide d'une interface graphique optimisée. Les systèmes les plus avancés proposent des analyses prêtes à l'emploi ainsi que des analyses ad-hoc pour construire ses propres requêtes.
Les solutions d'Identity and Access Intelligence permettent également d'identifier les risques potentiels associés aux utilisateurs et liés à leurs droits d'accès : utilisateurs à haut risque, comptes orphelins, failles de sécurité… Grâce à des indicateurs de risque et de conformité, l'entreprise peut se concentrer sur l'essentiel et dispose d'une aide précieuse au pilotage. Elle est alors en mesure de corriger plus rapidement des incohérences et des erreurs d'attribution de droits, et de mieux protéger ses ressources informatiques contre des interventions non autorisées et potentiellement dangereuses. En s'appuyant sur des faits démontrés, l'entreprise dispose des moyens nécessaires pour prouver l'efficacité des procédures de contrôle mises en place.

2. Adapter les informations à chaque type d'utilisateur
Le plus souvent, les solutions d'Identity and Access Intelligence intègrent des fonctionnalités d'exploration des données, comme l'analyse verticale et transversale, qui facilitent la recherche d'information et l'obtention de réponses pertinentes. La présentation graphique et intelligible des informations est adaptée à toutes les populations de l'entreprise : administrateurs informatiques, équipes métiers, auditeurs, direction générale…
Les RSSI et les auditeurs souhaitent visualiser les données de sécurité dans le moindre détail. Ils disposent d'un outil de surveillance dynamique à 360 degrés qui leur permet de déterminer le niveau de risque et le type de risque associés à un utilisateur. Ils peuvent aussi créer des rapports ad-hoc personnalisés pour croiser les informations comme bon leur semble et visualiser les données de sécurité qui les intéressent.
Les responsables métiers ont besoin de rapports standards prêts à l'emploi pour identifier rapidement les risques liés aux habilitations de leurs équipes et se concentrer sur les zones à haut risque. Pour aller à l'essentiel, la direction générale peut accéder à des tableaux de bord reprenant les principaux indicateurs de risque pondérés et hiérarchisés. Ils offrent un point de départ synthétique vers une analyse en profondeur si nécessaire. En pilotant l'évolution des indicateurs dans le temps, les décideurs déterminent les actions correctives à mener pour réduire le niveau de risque et améliorer la gouvernance à l'échelle de l'entreprise.

3. Réaliser un examen historique complet des droits d'accès
Les systèmes les plus avancés permettent de reconstituer tous les changements de droits ayant eu lieu au préalable, grâce à une historisation des modifications. Les changements de droits sont alors identifiés, tracés et consultables en toute simplicité.
Cette fonctionnalité est précieuse pour les auditeurs, car elle leur donne les moyens d'établir des pistes d'audit et de réaliser des investigations forensiques approfondies et exhaustives. En fonction de leurs besoins, ils passent en revue les droits d'accès d'un utilisateur à une date spécifique dans le passé, ou contrôlent ses changements successifs d'habilitations pendant une période donnée. Ainsi, l'historisation des droits d'accès est une fonctionnalité nécessaire pour détecter toute modification suspecte, identifier la source d'un problème, et réduire l'impact d'une fraude.

4. Identifier les utilisateurs à haut risque
Les solutions d'Identity and Access Intelligence offrent une visibilité à la demande sur les données de droits d'accès. Les informations relatives aux risques et aux habilitations sont mises à disposition dans un format compréhensible et intelligible, ce qui facilite très largement l'identification des groupes d'utilisateurs présentant le plus haut niveau de risque.
Une des recommandations de base de l'IAM est d'appliquer le principe du moindre privilège qui consiste à limiter les droits d'accès des utilisateurs au minimum requis pour leurs fonctions dans l'organisation. C'est pourquoi l'entreprise devra se concentrer sur la surveillance des utilisateurs à risque et évaluer régulièrement la pertinence de leurs droits d'accès spécifiques… [Lire la suite]

Réagissez à cet article

Source : *Bastien Meaux, Beta Systems : Le guide pratique de l'Identity and Access Intelligence – Global Security Mag Online*

L'eau d'une station

d’épuration manipulée par des hackers – Sciencesetavenir.fr

L’eau d’une station d’épuration manipulée par des hackers

L'opérateur de télécommunications américain Verizon révèle dans un rapport une cyberattaque ayant touché à la composition et à la distribution d'eau potable d'une station. Le système informatique était perclus de failles.

Le bilan dressé par l'opérateur américain Verizon publié en mars 2016 et consacré aux fuites de données a de quoi faire frémir. Il recense pas moins de cinq cents incidents de cybersécurité dans quarante pays en 2015 (le rapport en anglais ici**).** Parmi eux, l'un attire tout particulièrement l'attention : il concerne la Kemuri Water Company (KWC), une station d'épuration bien réelle mais dont le nom a été changé et le pays d'implantation non divulgué pour éviter de la compromettre. Et pour cause ! Verizon relate la façon dont des hackers ont réussi, très facilement, à manipuler la composition chimique de l'eau qui est redistribuée aux habitants après traitement ! Le tout, sans même en avoir eu l'intention au départ…
L'affaire a été révélée lorsque la société a décidé de faire appel aux équipes chargées du cyber-risque de Verizon pour renforcer son système d'information afin d'anticiper tout problème éventuel. Or, une fois sur place, les experts ont constaté avec stupeur que la station d'épuration était déjà la proie de pirates informatique depuis deux mois ! Et que ses responsables s'en doutaient… Des mouvements suspects de valves et de tuyauteries avaient été remarqués. Beaucoup plus grave ! Les gestionnaires avaient constaté des modifications inexpliquées de dosage dans les produits injectés dans l'eau pour la rendre portable. Sans conséquence désastreuse heureusement…

« Pour tout dire, KWC était un candidat tout trouvé pour une fuite de données. Son interface Internet présentait plusieurs failles à haut risque dont on sait qu'elles sont souvent exploitées» mentionne le rapport de Verizon. Et son système opérationnel, qui commande les applications industrielles (traitement des eaux, gestion du débit), reposait quant à lui sur une infrastructure informatique vieille de plusieurs dizaines d'années.
En outre, de nombreuses fonctions de ce système cohabitaient avec des applications « business » de l'entreprise sur un même et unique serveur, un AS/400 d'IBM, ordinateur commercialisé en… juin 1988. En clair, si des hackers pénétraient le système, ils pouvaient sans peine passer du contrôle du traitement des eaux aux informations financières et aux données de facturation de la compagnie. Et c'est exactement ce qui s'est passé.

L'opérateur liste une série de failles assez confondantes

Au cours de son enquête, Verizon s'est rendu compte que des adresses IP de hackers déjà rencontrées dans trois autres affaires s'étaient connectées au système de paiement en ligne de la KWC, cette interface permettant aux clients d'accéder à leur compte à distance (depuis un ordinateur, un mobile) ; c'est a priori par cette voie que les hackers sont passés, comme d'autres l'ont fait lors du piratage en octobre 2015 de l'hydrolienne Sabella.

2,5 MILLIONS. L'opérateur liste ensuite une série de failles confondantes : l'accès aux données clients n'était protégé que par un login/mot de passe, sans double authentification ; une « *connexion directe par câble* » existait entre l'application de paiement en ligne et l'AS/400, ce dernier ayant un accès ouvert à Internet, avec une adresse IP et des données d'identification administrative disponibles sur le serveur web de paiement, écrites en clair dans un fichier ! Au final, les pirates ont pu sortir du système 2,5 millions de dossiers clients avec leurs données de paiement. Pour l'heure, il semble qu'ils n'en aient pas fait usage.

ALERTE. Mais le plus grave restait à venir. Une fois à l'intérieur du réseau, les pirates se sont en effet rendus compte qu'ils pouvaient accéder aux fonctions opérationnelles.
En se servant des données d'identification administrative, ils ont ainsi pu intervenir sur des fonctions clés : le débit de l'eau potable, son traitement chimique et le temps de remplissage des réserves. A priori – et c'est une chance – les hackers ne semblent pas avoir eu l'intention de nuire et ne poursuivaient pas un but précis, mais les autorités frémissent à l'idée des conséquences dramatiques qu'une telle ingérence aurait pu occasionner. « *Si les attaquants avaient eu un peu plus de temps et avaient été un peu plus familiers du système de contrôle industriel, la KWC et les populations locales auraient pu subir de sérieux dommages* » conclut le rapport… [Lire la suite]

Réagissez à cet article

Source : *L'eau d'une station d'épuration manipulée par des hackers – Sciencesetavenir.fr*

L’iPhone du tueur débloqué par le FBI. Fin des poursuites contre Apple

L’iPhone du tueur débloqué par le FBI. Fin des poursuites contre Apple

Les autorités américaines affirment avoir « accédé avec succès aux données contenues dans l'iPhone de Syed Farook » et ont demandé à la justice d'annuler l'injonction obligeant la firme à la pomme à assister les enquêteurs.

Ce déblocage a été rendu possible par *« l'assistance récente d'un tiers »* (ndlr Cellebrite), selon un communiqué de la procureure fédérale du centre de la Californie, Eileen Decker. Elle indique en conséquence avoir demandé à la justice d'annuler l'injonction obligeant Apple à aider les enquêteurs. La firme refusait de se plier aux demandes judiciaires, soutenant qu'aider à décrypter le téléphone de Syed Farook créerait un précédent, sur lequel les autorités risquaient de s'appuyer à l'avenir pour réclamer l'accès aux données personnelles de nombreux citoyens pour diverses raisons.

« Viabilité »

Lundi 21 mars, les autorités fédérales avaient annoncé être sur la piste d'une méthode qui pourrait leur permettre d'accéder aux données du téléphone. Une audience clé, qui devait avoir lieu mardi au tribunal de Riverside en Californie, avait été annulée, après le dépôt d'une motion demandant un délai pour tester *« la viabilité »* de cette solution alternative.

Le gouvernement expliquait avoir *« poursuivi ses efforts pour accéder à l'iPhone »* pendant la procédure judiciaire et annonçait que des *« tierces parties »* lui avaient présenté une manière de décrypter son contenu sans la coopération d'Apple. La police fédérale demandait un peu de temps pour s'assurer que la méthode ne *« détruit pas les données du téléphone ».*

Une semaine plus tard, il semble donc que la méthode fonctionne. Washington affirme à la cour fédérale avoir *« accédé avec succès aux données contenues dans l'iPhone de Syed Farook »* et *« ne plus avoir besoin de l'assistance d'Apple »*… [Lire la suite]

Réagissez à cet article

Source : *San Bernardino : Washington a débloqué l'iPhone du*

tueur et renonce à poursuivre Apple

Cinq questions importantes à se poser en matière de cybersécurité

	**Cinq questions importantes à se poser en matière de cybersécurité**

Pas un jour ou presque ne se passe sans que le sujet de la cybersécurité ne soit traité dans les médias. Entre les « cyberattaques », les « cybermenaces » et la nécessité de « connaître son adversaire », on pourrait croire que les entreprises sont en état de siège permanent.

Les cybermenaces revêtent plusieurs formes : États-nations qui se livrent à des activités d'espionnage, cybercriminels qui cherchent à dérober de précieuses informations en vue de les exploiter, ou encore groupes aux motivations diverses qui cherchent à perpétrer des vols ou à causer des perturbations.

Il peut même s'agir d'une personne interne de confiance qui vole des données de clients ou d'entreprise ou d'un employé bien intentionné qui, en effectuant son travail, perd sans le vouloir de précieuses données de clients ou d'entreprise. Nul doute que les cybercriminels peuvent être très adaptables et innovants, mais le contexte de menace est un fait établi. C'est la manière dont vous gérez le risque qui est importante.
Dans un environnement cacophonique, il est important que les dirigeants d'entreprise gardent les choses en perspective. L'environnement est inondé de toutes sortes de solutions techniques, promettant de vous donner un avantage en matière de détection et de prévention. Toutefois, il est essentiel que tous les dirigeants d'entreprise prennent du recul et se rappellent que le cyber risque n'est pas un risque informatique, mais un risque d'entreprise et, à l'instar de tout autre risque d'entreprise, il doit être géré.

La menace ne peut pas être éliminée, mais le risque peut être géré

Il est également important de comprendre que cette menace ne peut pas être éliminée, mais que le risque peut être géré. Il est facile de se laisser tenter par une « structure du risque », mais comme de nombreuses structures, elle peut nécessiter d'investir beaucoup de temps et d'efforts pour des résultats de sécurité négligeables.
Trop souvent, la cybersécurité est évoquée à l'aide de jargon technique ou militaire, mais cela ne fait que dissiper l'attention et la compréhension des dirigeants. Il est vital que les professionnels de la sécurité expliquent le contexte de menace et le défi de la cybersécurité dans un langage accessible. C'est pourquoi il est important de comprendre le cyber risque auquel votre entreprise est confrontée. Tous les dirigeants doivent pouvoir poser les questions simples et non techniques suivantes et obtenir des réponses.

1. **Connaissez la valeur de vos données :** savez-vous de quelles données de valeur dispose votre entreprise ? Sont à inclure les données qui ont de la valeur non seulement pour vous, mais aussi pour les cybercriminels qui peuvent vouloir les voler. Quelles sont les données qui vous causeraient le plus grand préjudice si vous deviez les perdre ? Vous devez avoir une liste de vos données de valeur.
2. **Sachez qui a accès à ces données de valeur :** qui possède les droits d'administration ou l'accès aux informations ? Toutes vos « personnes internes de confiance » ont-elles besoin d'avoir accès aux données de valeur pour effectuer leur travail ? Cette question est essentielle, car l'accès aux données de valeur doit être étroitement surveillé. Vous ne confieriez pas les clés de votre domicile à n'importe qui, alors surveillez de près les personnes qui ont accès à vos données de valeur.
3. **Sachez où se trouvent vos données de valeur :** vous devez savoir où elles sont stockées et comment vous y accédez. Vos données de valeur sont-elles délocalisées au loin, dans le pays, dans le cloud ou même stockées chez un tiers ? Allez plus loin et demandez-vous si vos fournisseurs ont partagé vos données de valeur avec des sous-traitants.
4. **Sachez qui protège vos données :** vous devez savoir qui protège vos données de valeur. Cet aspect est extrêmement important. Où se trouvent ces personnes ?
5. **Sachez dans quelle mesure vos données sont protégées :** vous devez savoir ce qui est fait par les professionnels de la sécurité pour protéger vos données 24 h/24 et 7 j/7. Les tiers qui ont accès à vos données les protègent-ils de manière adéquate ?

C'est seulement une fois que vous aurez la réponse à ces questions que votre entreprise sera préparée à comprendre le niveau de cyber risque et l'efficacité avec laquelle il est géré… [Lire la suite]

Réagissez à cet article

Source : *Cinq questions importantes à se poser en matière de cybersécurité – ZDNet*

Protégez-vous gratuitement du Virus Locky avant qu'il ne soit trop tard !

Protégez-vous gratuitement du virus Locky avant qu'il ne soit trop tard !

Voici une solution rapide et pratique et efficace uniquement avec les versions actuelles de Locky pour s'en protéger.
Rien ne garantit qu'une version ultérieure de Locky ne contournera pas le souci.

Comme Locky essaye de créer la clé **HKCUSoftwareLocky** dans la base de registre (regedit), il suffit de la créer avant lui…

et de refuser tous les droits d'accès sur celle-ci:

Et voilà ! Ainsi, en se lançant sur votre système, Locky se crashera comme une station Mir dans le jardin de Paco. Les autres solutions proposées par Lexsi sont un poil plus complexes, mais vraiment intéressantes. Je vous invite à les lire, ne serait-ce que pour votre culture personnelle.
Merci Korben d'avoir relayé et à Olivier pour le partage.

Réagissez à cet article

Source : *Locky – La solution pour s'en protéger – Korben*

Petya, le nouveau ransomware qui chiffre l’ensemble du disque

Petya, le nouveau ransomware qui chiffre l’ensemble du disque

Le G DATA Security Labs a détecté les premiers fichiers ce jeudi 24 mars, en Allemagne, d'un nouveau type de ransomware nommé Petya.

A la différence des codes actuels, tels que Locky, CryptoWall ou TeslaCrypt, qui chiffrent certains fichiers du système, Petya chiffre l'ensemble des disques durs installés.

.

La campagne actuellement en cours vise les entreprises

Dans un email au service des ressources humaines, il y a une référence à un CV se trouvant dans Dropbox. Le fichier stocké dans le partage Dropbox est un exécutable. Dès son exécution, l'ordinateur plante avec un écran bleu et redémarre. Mais avant cela, le MBR est manipulé afin que Petya prenne le contrôle sur le processus d'amorçage. Le système démarre à nouveau avec un message MS-Dos qui annonce une vérification CheckDisk. A défaut d'être vérifié, le système est chiffré et plus aucun accès n'est possible.

Le message est clair : le disque est chiffré et la victime doit payer une rançon en se connectant à une adresse disponible sur le réseau anonyme TOR. Sur la page concernée, il est affirmé que le disque dur est chiffré avec un algorithme fort. Après 7 jours, le prix de la rançon est doublé. Il n'y a pour le moment aucune certitude sur le fait que les données soient irrécupérables.

Il est donc recommandé aux entreprises et particuliers de redoubler de vigilance quant aux emails reçus… [Lire la suite]

Réagissez à cet article

Source : *Petya : un nouveau ransomware qui chiffre l'ensemble du disque*

La gendarmerie cherche un expert en « déprotection » logicielle et matérielle

	La gendarmerie cherche un expert en « déprotection » logicielle et matérielle

La gendarmerie recrute un expert de haut niveau pour « déprotéger » des matériels ou des données auxquels les enquêteurs cherchent à accéder.

La gendarmerie nationale a fait publier ce jeudi au Journal Officiel deux petites annonces d'emploi, dont l'intitulé résonne fortement avec le conflit qui oppose Apple au FBI aux États-Unis.
La première concerne un « *emploi d'expert de haut niveau en technologies numériques chargé de projet et développement de techniques de déprotection matérielle à la division ingénierie numérique* » de l'Institut de recherche criminelle, au pôle judiciaire de la gendarmerie nationale, à Pontoise (95).
La seconde est très proche dans son intitulé mais concerne les « *techniques de dé-protection logicielle* ».

Les deux postes sont ouverts aux titulaires d'un diplôme d'ingénieur ou au moins d'un master 2 en informatique, électronique cryptologie ou mathématique.

Selon le descriptif, « *le candidat retenu aura pour mission principale de développer des méthodes et outils nécessaires à la dé-protection matérielle (smartphones, disques durs…) et assurer la pertinence, la robustesse de ses méthodes* ». En clair, il s'agira par exemple d'essayer de contourner le chiffrement des iPhone ou lechiffrement sous Android, pour accéder au contenu des appareils bloqués. C'est une attente forte du parquet, et plus généralement des enquêteurs qui souhaitent obtenir toutes les preuves potentiellement accessibles sur les matériels saisis chez des suspects.

UN HACKER CHERCHEUR

Le candidat idéal, qui devra aussi « *disposer de capacités avérées à acquérir de nouvelles compétences* », doit déjà avoir dans ses bagages :
• maîtrise de la structure des systèmes électroniques ;
• expérience de conception et de rétro-conception de circuits électroniques ;
• capacités de développement (langages C/C++, Java, Python…) ;
• connaissance d'un ou plusieurs domaines innovants nécessaires au développement de l'activité du département ;
• excellente connaissance des technologies numériques ;
• maîtrise écrite et parlée de la langue anglaise ;
• une connaissance de la criminalité liée aux nouvelles technologies est également recherchée.

La personne recrutée « *devra mettre en place les outils d'analyse de données permettant au département INL d'exploiter au mieux les informations à sa disposition* ». « *Il devra pour ce faire être en mesure d'analyser les supports informatiques et réaliser des dossiers d'expertise comme soutenir techniquement les enquêteurs de la gendarmerie spécialisés en nouvelle technologie* », précise la gendarmerie.
Celle-ci attend par ailleurs de son expert de haut niveau qu'il s'engage dans la communauté internationale de la sécurité informatique, pour apporter ses propres travaux et bénéficier des avancées des autres. Ainsi, « *il sera également chargé de définir et conduire la politique de veille technologique dans son domaine de compétence et de valoriser son action à un niveau national ou international en participant à des publications dans des revues ou en recherchant des partenaires* ».
Enfin, précise l'annonce, « *il sera aussi chargé de l'animation de l'activité scientifique et technique du département en faisant preuve d'innovation et en suivant différents projets de recherches et de développement, en dispensant des cours et en développant des relations entre les acteurs français et étrangers du domaine de l'expertise en technologie numérique* ».

Il n'y a plus qu'à envoyer vos CV.
… [Lire la suite]

Réagissez à cet article

Source : *La gendarmerie cherche un expert en « déprotection » logicielle et matérielle – Tech – Numerama*