Utilité et conformité des mesures de blocage de sites Internet faisant l’apologie du terrorisme dans le cadre de l’état d’urgence.

	Utilité et conformité des mesures de blocage de sites Internet faisant l’apologie du terrorisme dans le cadre de l’état d’urgence.

A ce jour, il existe certains exemples de moyens, usités par les terroristes, permettant de contourner une mesure de blocage d'un site, notamment, l'utilisation d'un « Virtual Private Network » (Réseau Privé Virtuel).

Ce dernier établi un réseau fictif, reliant un ordinateur (celui du client VPN) à un serveur (le serveur VPN), afin de permettre une connexion à Internet de manière anonyme.

De cette façon, les échanges de données sont cryptés et sont protégés par des clés de chiffrement. De plus, ce système permet d'utiliser une adresse IP différente de celle réellement utilisée par un ordinateur, ce qui complique considérablement la localisation de cette machine. De même, le logiciel « Tor » permet de se connecter à Internet par le biais de serveurs répartis dans le monde dans l'anonymat. Il convient de noter que ces procédés cryptologiques sont parfaitement légaux, effectivement, l'article 30 de la loi LCEN du 21 juin 2004 érige en principe que « l'utilisation des moyens de cryptologie est libre ». Dès lors, peut-on envisager l'introduction d'un contrôle par l'autorité administrative, sous forme d'autorisation préalable, lorsque l'utilisation de tels procédés est faite à des fins de provocation au terrorisme ?

Enfin, ces mesures de blocage de sites peuvent sembler illusoires étant donné que celles-ci ne s'appliquent qu'à des FAI et hébergeurs situés sur le territoire français. D'autant que de telles mesures drastiques ne sont pas exemptes de risques de « surblocage ». En 2013, l'Australie a pu en faire les frais en bloquant par accident 250 000 sites sur sa toile.

En conséquence, loin d'être la panacée, cette nouvelle disposition, faussement pragmatique, semble foncièrement superfétatoire.

Sur la conformité de la loi par rapport au bloc de constitutionnalité ?

A titre liminaire, il importe de se poser la question de savoir si la loi du 20 novembre 2015 est susceptible d'être déclarée non conforme à la constitution compte tenu de l'absence de consécration constitutionnelle du statut de l'état d'urgence. A cette fin, il conviendra d'appliquer mutatis mutandis le raisonnement adopté par le Conseil Constitutionnel dans deux décisions : celle du 10 juin 2009 concernant la loi HADOPI et celle relative à la loi sur la pédopornographie du 10 mars 2011.

Dans sa décision du 10 juin 2009, le Conseil en raison du caractère disproportionné du blocage et de sa contrariété avec l'article 11 de la DDHC censure la loi HADOPI soumise à son contrôle « considérant que les pouvoirs de sanction institués par les dispositions critiquées habilitent la commission de protection des droits, qui n'est pas une juridiction, à restreindre ou à empêcher l'accès à internet de titulaires d'abonnement ainsi que des personnes qu'ils en font bénéficier ; que la compétence reconnue à cette autorité administrative n'est pas limitée à une catégorie particulière de personnes mais s'étend à la totalité de la population ; que ses pouvoirs peuvent conduire à restreindre l'exercice, par toute personne, de son droit de s'exprimer et de communiquer librement, notamment depuis son domicile ; que, dans ces conditions, eu égard à la nature de la liberté garantie par l'article 11 de la Déclaration de 1789, le législateur ne pouvait, quelles que soient les garanties encadrant le prononcé des sanctions, confier de tels pouvoirs à une autorité administrative dans le but de protéger les droits des titulaires du droit d'auteur et de droits voisins ».

En substance, les Sages expliquent que l'octroie par la loi à une autorité administrative du pouvoir de suspendre l'accès à internet est une entorse à la « la libre communication des pensées et des opinions ». L'autorité administrative n'ayant pas le statut de juridiction, elle ne peut se voir octroyer ce pouvoir exorbitant de bloquer un site illicite.

A rebours, dans sa décision du 10 mars 2011, les Sages valident l'article 4 de la loi Loppsi 2 permettant de procéder au blocage administratif de sites pédopornographiques « considérant, en second lieu, que les dispositions contestées ne confèrent à l'autorité administrative que le pouvoir de restreindre, pour la protection des utilisateurs d'internet, l'accès à des services de communication au public en ligne lorsque et dans la mesure où ils diffusent des images de pornographie infantile ; que la décision de l'autorité administrative est susceptible d'être contestée à tout moment et par toute personne intéressée devant la juridiction compétente, le cas échéant en référé ; que, dans ces conditions, ces dispositions assurent une conciliation qui n'est pas disproportionnée entre l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public et la liberté de communication garantie par l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 ».

Dans cette décision, la mesure de blocage est déclarée conforme à l'article 11 de la DDHC de 1789 au motif qu'il existe un recours au fond ou en référé des décisions de blocage et qu'il est consacré un objectif à valeur constitutionnelle de sauvegarde de l'ordre public (ici l'exploitation sexuelle des mineurs).
En ce qui concerne la conformité du nouveau dispositif, il est à noter que ce nouvel article 11 de la loi de 1955 énonce que « le ministre de l'Intérieur peut prendre toute mesure » de blocage de sites faisant l'apologie du terrorisme. La large marge d'appréciation laissée à l'exécutif amène à s'interroger sur le caractère proportionné de cette disposition. Ainsi, un parallèle peut être opéré avec l'article L. 336-2 du CPI prévoyant des mesure de blocage en cas de violation d'un droit d'auteur ou d'un droit voisin. Celui-ci met en évidence l'éventuel caractère excessif du nouveau dispositif. Si ce dernier rend possible « toutes mesures », l'article L. 336-2 du CPI autorise seulement « toutes mesures propres » en vue de bloquer un site.

La référence au principe de proportionnalité, tangible dans cet article du CPI, ne l'est pas en ce qui concerne cette nouvelle mesure. Dans le cadre d'un raisonnement analogue à celui employé dans la décision du 10 juin 2009, on peut appréhender une potentielle censure par les Sages. En effet, la loi du 20 novembre 2015, compte tenu de sa rédaction large et générale, peut habiliter le ministre de l'Intérieur à « restreindre ou à empêcher l'accès à Internet ». De ce fait, un accroc à l'article 11 de la DDHC peut être redouté. D'ailleurs, le rapporteur au Sénat énonçait que « la disposition proposée [la loi lopssi 2] présente une portée beaucoup plus restreinte [que la loi HADOPI] puisqu'elle tend non à interdire l'accès à internet mais à empêcher l'accès à un site déterminé en raison de son caractère illicite ». Ainsi, le nouveau texte de 2015 risque de connaître le même sort que celui donné à la loi HADOPI, en ce que rien n'interdit au ministre de l'Intérieur de prendre des mesures bloquant l'accès à un site sans pour autant bloquer un site en particulier.
Par ailleurs, une autre incertitude juridique semble planer sur cette loi du 20 novembre 2015 au regard de la décision du 10 mars 2011. S'il est vrai que la suppression du délai de 24 heures ne semble pas impacter la conformité de ce texte, il en va autrement de l'éviction du rôle de contrôle de la CNIL. En effet, l'article 66 de la Constitution dispose que l'autorité judiciaire est « gardienne de la liberté individuelle ». Auparavant, la loi de 2014, chargeait la CNIL d'assurer ce rôle de gardien a posteriori, c'est-à-dire, en actionnant en aval les recours nécessaires devant la juridiction compétente. De même, la CNIL détenait la faculté de contrôler le bien fondé des demandes de retrait de l'autorité administrative. La nouvelle loi éludant cet encadrement exercé par la CNIL, peut laisser sceptique sur sa conformité au texte constitutionnel. D'autant que la loi ancienne (de 2014) n'a jamais fait l'objet d'un contrôle, que ce soit de manière a priori ou a posteriori, devant le Conseil Constitutionnel !

Sur le risque de contrariété de la loi avec la Convention Européenne des Droits de l'Homme ?

Dans un récent arrêt CEDH du 1er décembre 2015, la Cour censure des mesures de blocage de sites pratiquées par le gouvernement turc. En l'espèce, les autorités turques avaient ordonné le blocage de Youtube en raison de dix vidéos accusées de faire outrage à la mémoire d'Atatürk, fondateur de la République laïque turque. Des mesures de blocage ont été ordonnées entre 2008 et 2010.
La Cour reconnait une ingérence de l'autorité publique dans l'exercice des droits garantis par l'article 10 de la convention portant sur la liberté d'expression. De la même façon, la loi de novembre 2015 n'excluant pas la possible coupure d'un site Internet, elle encourt le risque d'être déclarée disproportionnée au regard de l'intérêt légitime poursuivi, à savoir, la lutte contre l'apologie du terrorisme.
Toutefois, l'article 15 de la CEDH autorise dérogation aux obligations de cette convention dans une situation d'état d'urgence, excepté pour les principes non dérogeables, dont ne fait pas partie l'article 10 de la CEDH. Mais un prolongement durable de l'état d'urgence posera nécessairement une difficulté relative à sa compatibilité avec l'article 15 de la CEDH. A moins, (ce que le gouvernement envisage) d'établir un socle juridique solide de l'état d'urgence, au sein de la constitution. En conséquence, de lege lata, la conformité de ce nouveau dispositif semble loin d'être évidente au regard d'un certain nombre de droits fondamentaux garantis.
Somme toute, est-ce qu'« à force de sacrifier l'essentiel pour l'urgence, on finit par oublier l'urgence de l'essentiel » ? (Edgar Morin)

Réagissez à cet article

Source : *Utilité et conformité des mesures de blocage de sites Internet faisant l'apologie du terrorisme dans le cadre de l'état d'urgence. Par Dan Scemama.*

Mobile strategies increase need for data loss prevention technology in Europe

Mobile strategies increase need for data loss prevention technology in Europe

Data loss prevention technology that covers all popular mobile platforms and is easy to use and implement is called for as mobile strategies evolve

Mobile has entered business strategy from two directions. The business wants to grab the opportunity to better serve the mobile masses, while employees want to mobile devices as part of their work
This has created an environment that security teams have had to come to terms with quickly.

Roman Foeckl, CEO at security supplier CoSoSys, says the increasing number of mobile devices in the enterprise, and new versions of an operating system, is forcing organisations to rethink ways of securing corporate data.
It is not just about mobile the applications, he says, but also how employees interact with other organisations and people. Mobile provides low-cost computing power that is available to everyone and enables staff to collaborate with others, but this is a recipe for security breaches in businesses.
Foeckl says traditional security is irrelevant in many cases. For example, he says the shift from open file systems (Windows 7) to application sandboxes (Android, iOS, Windows Phone/Pro/RT), is making traditional antimalware, especially antivirus, less relevant.
For example, on iOS, there is little need for antimalware or antivirus products because neither they, nor any other app on the device, can access another app's storage or memory.
According to Foeckl, when planning a mobile security strategy there is no one size fits all: "Every company has to choose a cross-platform solution that works on Apple iOS, Android mobile devices, Windows, Mac OS X and Linux computers to cover the entire fleet of workstations."
Sufficient resources for data loss protection
But what are companies doing to incorporate endpoint and mobile security tools in applications to make sure they are secure?
"This can be achieved by implementing data loss prevention (DLP) features into applications and more," says Foeckl. "However, the administrators have to be sure that IT resources under their control are ready to co-operate with advanced features like file tracing and file shadowing."

With DLP, the amount of data being monitored and the number of copies stored could quickly absorb a sizeable chunk of the available IT resources.
"In European countries, sometimes we are faced with the situation that a CIO or administrator evaluates resources as insufficient for DLP use," says Foeckl. "In such cases it is recommended to look at cloud-managed DLP and mobile device management [MDM] that offer easy evaluation, implementation and scalability. It's also a good way to safely reap the benefits of the cloud protecting data."
In central and eastern European countries, one obstacle is the fact that many companies still prefer their own datacentres or computing power over cloud services, says Foecki.

Authorisation and security awareness
The software being used in enterprises is changing, so security teams must understand different security features and their limitations.
Foeckl says CoSoSys increasingly supports Macs and iOS devices. It has experience with preventing data breaches that could happen with the use of Google Drive, One Drive, Dropbox, on Windows and Mac OS X computers, for example.

Réagissez à cet article

Source : *Mobile strategies increase need for data loss prevention technology in Europe*

Conférence sur la réponse aux incidents et l'investigation numérique 2016 | CECyF

Conférence sur la réponse aux incidents et l'investigation numérique 2016

Dans le cadre du FIC 2016 – Forum International sur la Cybersécurité, nous vous proposons de nous retrouver le lendemain de cet événement de référence (mercredi 27 janvier 2016), pour la seconde conférence de ce genre en France, dédiée aux techniques de la réponse aux incidents et de l'investigation numérique (retrouver la page de CoRI&IN 2015).

Cette journée, organisée dans les locaux d'Euratechnologies, permettra aux enquêteurs spécialisés, experts judiciaires, chercheurs du monde académique ou industriel, juristes, spécialistes de la réponse aux incidents ou des CERTs de partager et échanger sur les techniques du moment. L'ambition de cette conférence est de rassembler cette communauté encore disparate autour de présentations techniques ou juridiques de qualité, sélectionnées par notre comité de programme.
Si vous souhaitez être tenu informé de l'actualité quant à cette conférence, vous pouvez vous inscrire sur notre liste de diffusion.

Programme prévisionnel

L'accueil sera ouvert le 27 janvier 2015, à partir de 08h30 et la conférence commencera à 9h30, pour se terminer à 16h.
Au 23 décembre 2015, le programme prévisionnel est composé des interventions suivantes:

- Analyse de codes malveillants complexes, Paul Rascagnères et Sébastien Larinier
- La règle du boomerang, Eve Matringe

D'un point de vue juridique, lorsqu'une entreprise ou une institution est victime d'une attaque informatique, quelles sont les marges de manœuvre dont elle dispose pour répliquer? Est-il juridiquement possible de contre-attaquer? Le cas échéant, quels sont les points à envisager?

- De l'hameçonnage ciblé à la compromission totale du domaine, Johanne Ulloa
- Démonstration, état des lieux, limitation du risque et réponse à incident
- Retour d'expérience – gestion de crise SSI en environnement non préparé, Vincent Nguyen
- Surveillance de circonstance, Jean-Baptiste Galet et Alexandre Charlès
- Analyse forensique de dumps de RAM, Pierre Veutin et Nicolas Scherrmann
- Retour d'expérience audit inforensique, Vladimir Kolla

Investigation numérique dans les systèmes industriels : mythe & réalité, David Le Goff

Inscription

Merci de vous inscrire sur la page ci-après (participation aux frais de 10 € et gratuité pour les étudiants – inscription obligatoire):
Les inscriptions sont ouvertes depuis le 07 décembre 2015
https://www.helloasso.com/associations/cecyf/evenements/cori-in

---

Réagissez à cet article

Source : *Conférence sur la réponse aux incidents et l'investigation numérique 2016 | CECyF*

2700 sites Internet suspects passés à la loupe par le ministère de l'Intérieur

2700 sites Internet suspects passés à la loupe par le ministère de l'Intérieur

---

Le ministère de l'Intérieur a présenté au ministère des Technologies de la Communication et de l'Économie Numérique, 2700 requêtes sur des sites et des pages suspectés de prôner le terrorisme, a indiqué ce lundi 28 décembre sur les ondes de Mosaique FM, le ministre des TICS, Noômane Fehri.

Selon le ministre, plusieurs pages sur les réseaux sociaux ont été par ailleurs supprimées sur demandes présentées aux entreprises internationales comme Facebook.
Il a cependant précisé que des sites n'ont pas été supprimés ni masqués afin de pouvoir en extraire des renseignements et de suivre à la trace leurs administrateurs.

Réagissez à cet article

Source : *Cyberterrorisme : 2700 sites suspects ont été passés à la loupe par le ministère de l'Intérieur*

Cyber-attaque contre le ministère des Habous et des affaires islamiques

Cyber-attaque contre le ministère des Habous et des affaires islamiques

Le site du ministère des Habous et des affaires islamiques a été piraté ce Samedi 26 décembre par des hackers se faisant appelé « RxR Hackers. »

Le site du ministère des Habous et des affaires islamiques a été piraté ce Samedi 26 décembre par des hackers se faisant appelé « RxR Hackers. »
Une fois piraté, le site est devenu inaccessible pour les fonctionnaires ainsi que le grand public.
D'après « Le360 », l'attaque est confirmée, et l'ouverture d'une enquête est indispensable pour déterminer les raisons de ce piratage ainsi que l'identité des hackers à l'origine de cet acte qualifié d'irresponsable.

Réagissez à cet article

Source : *Cyber-attaque contre le ministère des Habous et des affaires islamiques – Article 19*

Les données personnelles de 191 millions d’électeurs en accès libre sur la Toile

Les données personnelles de 191 millions d’électeurs en accès libre sur la Toile

---

Un spécialiste en cybersécurité a découvert l’existence d’une base de données contenant les informations personnelles détaillées de 191 millions d’électeurs nord-américains. La fuite serait due à une erreur de configuration de la base de données.

Des données personnelles concernant près de 60% des citoyens des États-Unis se sont retrouvées en libre accès sur la Toile en raison d’un base de données mal configurée. C’est la découverte faite récemment par Chris Vickery, un expert en cybersécurité. La base de données en question n’était apparemment pas sécurisée et serait même toujours active.
Elle contient le nom complet de chaque personne, son sexe, sa date de naissance, son adresse, numéro de téléphone, numéro d’électeur, l’Etat dans lequel elle vote, l’affiliation politique ainsi qu’un historique de ses choix électoraux depuis 2010. Une véritable mine d’or en somme, et Vickery n’a pas indiqué où il avait déniché cette base de données, ni qui en était le créateur.

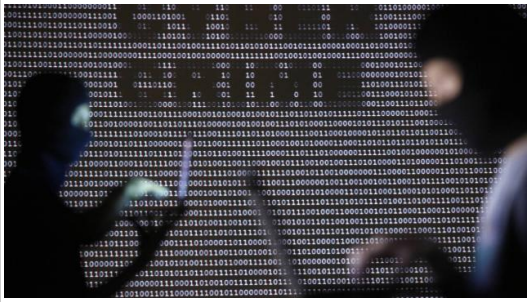
Réagissez à cet article

Source : *États-Unis : les données personnelles de 191 millions d'électeurs en accès libre sur la Toile*

Crainte d'attentats pilotés à partir d'Internet en 2016

Crainte d'attentats pilotés à partir d'Internet en 2016

Les experts en cybercriminalité craignent beaucoup pour l'année à venir. Notamment des attentats déclenchés à distance.



Multiplication des demandes de rançons, perfectionnement des attaques par e-mail, détournement des objets connectés… 2016 ne devrait pas faire chômer les experts de la cybercriminalité, qui craignent de plus en plus un attentat déclenché à distance.

Demandez au bureau du Cercle européen de la sécurité et des systèmes d'information, qui fédère les professionnels du secteur quelle est la plus grande menace planant sur nos têtes, et la réponse sera unanime: « Le #cyber-sabotage, ou #cyber-terrorisme. L'attaque informatique d'un système lourd, qui aura des impacts environnementaux ou humains : polluer l'eau, faire exploser une usine, faire dérailler un train… » Les hackers – États, mafias ou groupes militants – utilisent des méthodes de plus en plus sophistiquées pour « casser » les systèmes informatiques de leurs cibles. À l'exemple de ce haut-fourneau allemand mis hors service il y a un an, on peut tout à fait envisager une cyberattaque contre un équipement vital.

L'éditeur américain Varonis envisage une variante retentissante, une cyberattaque contre la campagne présidentielle américaine. « Elle aura pour conséquence une violation importante des données qui exposera l'identité des donateurs, leurs numéros de carte de crédit et leurs affinités politiques confidentielles », prévoit-il. De quoi provoquer un joyeux désordre.

« Cheval de Troie »

Pour atteindre leurs cibles, les pirates informatiques apprécient particulièrement la technique du « cheval de Troie », qui consiste à faire pénétrer un « malware » (logiciel malveillant) sur les appareils des employés, d'où il pourra progresser vers les unités centrales. Et pour ce faire, une méthode prisée est le « spear phishing », l'envoi de courriels de plus en plus personnalisés, pour amener le destinataire à ouvrir un lien corrompu ou une pièce jointe infectée.

Cette méthode est également utilisée pour faire chanter les gens, chefs d'entreprise ou particuliers, après avoir dérobé et/ou crypter des données – de la comptabilité d'une société aux photos de vacances– qui ne sont rendues et/ou décryptées que contre rançon.

La même méthode peut aussi permettre à une entreprise d'espionner un concurrent. « L'année prochaine, ou dans les deux prochaines années, je pense qu'il va y avoir des vraies affaires qui vont sortir sur le sujet », estime Jérôme Robert, directeur du marketing de la société de conseil française Lexsi.

Smartphones peu protégés

« Il y a beaucoup d'entreprises qui ont déjà utilisé des détectives privés, il n'y a pas de raison qu'elles ne le fassent pas dans le cybermonde », remarque-t-il. Autre préoccupation des spécialistes: le glissement de la vie numérique vers des smartphones qui pèchent parfois par manque de protections.

« Il y a quasiment plus maintenant de smartphones qu'il y a d'ordinateurs, des smartphones qui sont allumés quasiment 24 heures sur 24, qui nous suivent partout », note Thierry Karsenti chez l'éditeur d'antivirus israélien Check Point. « Or, ils ont finalement beaucoup plus de connectivité que les équipements informatiques traditionnels. Ils ont même des oreilles puisqu'il y a un micro, ils ont même une caméra, et ils stockent tout un tas d'informations à la fois professionnelles et personnelles. C'est beaucoup plus embêtant de se faire pirater son smartphone que se faire pirater son ordinateur ! »

« Paradoxalement, si vous regardez la sécurité, vous avez beaucoup plus de sécurité sur un ordinateur », poursuit M. Karsenti. « Alors que les smartphones ou les tablettes n'ont absolument rien en termes de sécurité. » Et le développement des paiements par smartphone devrait allécher les hackers, généralement motivés par l'argent.

Objets connectés détournés

Même préoccupation pour les objets connectés, dont le nombre devrait exploser ces prochaines années. Ceux-ci sont, selon Lam Son Nguyen, expert en sécurité internet chez Intel Security, « souvent conçus sans tenir compte des aspects sécurité ». « Ils vont être susceptibles d'être attaqués par des personnes développant des solutions malveillantes », prévient-il.

Jusqu'à présent, on a surtout vu des hackers s'emparer de données d'utilisateurs stockées sur des serveurs distants des fabricants – dans le « cloud » -, et pas les objets eux-mêmes détournés à distance. « Pour les objets destinés aux consommateurs, il devrait y avoir des attaques qui seront plus des galops d'essai, des jeux, pour se faire plaisir. Je ne vois pas de grosse activité cybercriminelle sur les objets connectés », car il n'y aura sans doute pas d'argent à en tirer dans l'immédiat, juge Jérôme Robert chez Lexsi.

Réagissez à cet article

Source : *Cybercriminalité. Crainte d'attentats déclenchés à distance en 2016*

Les super cartes bancaires débarquent

	Les super cartes bancaires débarquent

Pour lutter contre la fraude, les banques misent sur la technologie. Demain, on paiera avec une carte à code éphémère ou un smartphone à reconnaissance faciale.

Cette révolution est à portée de main. Dans quelques mois, tout devrait changer… dans votre portefeuille. Votre carte bancaire va s'offrir une deuxième jeunesse. Un relooking qui porte un nom barbare : «cryptogramme dynamique». Ce qui, en français, signifie que les trois petits chiffres, situés au verso de votre carte, changeront au bout de quelques minutes.
Les plus grands fabricants de cartes bancaires au monde, Gemalto et Oberthur, ont lancé ces derniers mois la commercialisation de cette technologie. BNP Paribas, la Banque postale, la Société générale… La quasi-totalité des établissements financiers français sont en train de la tester auprès de leurs clients.

Qui va payer ?
Objectif affiché : mieux lutter contre la fraude à la carte bancaire. Un fléau dont la finance aimerait bien se débarrasser. Pas question de laisser les arnaques et les fraudes nuire à l'engouement des Français pour ce mode de paiement. Imaginez, le 5 décembre dernier, la France a battu un record : 42 millions de transactions par carte bancaire en un week-end. Soit 12 % de plus que lors du premier samedi de décembre 2014 !
Un effet logique du boom du commerce en ligne. Pourtant, les banques se laissent encore quelques mois pour un développement à grande échelle de cette carte bancaire plus sécurisée. Car un petit détail reste encore à trancher. Ce bout de plastique bourré de technologies coûte plus cher à produire que la carte à puce classique. Qui va payer ? La banque, les commerçants ou le client ? Les réponses du milieu bancaire restent floues. Les banques trancheront ces prochains mois. Mais elles n'ont plus vraiment le temps de tergiverser. Des start-up dénommées FinTech (technologie financière) commencent déjà à les bousculer, notamment en utilisant le smartphone pour lancer de nouveaux modes de paiement. Et comme d'autres secteurs l'ont appris à leurs dépens, l'immobilisme face aux nouvelles technologies ne paye pas.
«2016 sera l'année des nouveaux modes de paiements», pronostique donc un cadre de banque. Nombre d'établissements ont, dans les cartons, de nouveaux produits qui n'attendent plus qu'une autorisation de la Cnil (Commission nationale de l'informatique et des libertés) pour passer des simples tests à la commercialisation. C'est le cas des technologies de biométrie utilisant des éléments du corps (empreinte digitale, vocale, etc.). Les bons vieux codes bancaires bientôt périmés ?

Un cryptogramme valable 20 minutes
Même largeur, agilité, finesse, robustesse, touché… A priori, rien ne la distingue de sa prédécesseur. A un détail près : la carte bancaire de nouvelle génération est équipée d'un écran. Tout petit. Pas de quoi regarder un film en haute définition. Non, mais tout de même assez large pour afficher, en noir et blanc, les trois chiffres du fameux cryptogramme visuel. Ce code de sécurité réclamé à chaque achat sur la Toile devient «dynamique». «Cette carte est équipée d'une horloge interne. Le code de sécurité sur l'écran change toutes les vingt minutes», explique Frédérique Richert, marketing manageur chez Gemalto, le leadeur mondial de la carte à puce, qui commercialise depuis quelques semaines cette nouvelle technologie. «Cette carte lutte mieux contre la fraude», ajoute-t-elle.

Réduire le coût des fraudes
A priori, rien ne change pour l'utilisateur. Pour effectuer un achat en ligne, il doit toujours remplir les mêmes formulaires en indiquant son nom, son numéro de carte bancaire, la date de validité et le cryptogramme. La différence, c'est que ces coordonnées ont une durée de vie limitée. Si un pirate informatique les vole, il ne peut alors les utiliser que pendant une vingtaine de minutes. Un laps de temps, a priori, trop court pour multiplier les achats sur le Web ou revendre ces informations à d'autres escrocs.
La plupart des grands réseaux bancaires sont en train de tester auprès de leurs clients cette nouvelle technologie. Ainsi, BPCE a équipé depuis plusieurs semaines un millier de clients. BPCE utilise la technologie d'Oberthur, concurrent de Gemalto. Avec un avantage, celui de réduire le coût des fraudes. Car les banques assument une partie du coût de l'arnaque : indemnisation du client pour les achats réalisés frauduleusement, coût du changement du support, etc. «Nous regardons à la fois l'effet de cette nouvelle technologie sur le coût lié à la fraude mais aussi sur la confiance des utilisateurs dans le paiement en ligne, dans l'usage des cartes bancaires», explique Nicolas Chatillon, directeur du développement fonctions transverses du groupe BPCE. Un point stratégique. Car un possesseur de carte bancaire en confiance, c'est un consommateur qui dépense !

Réagissez à cet article

Source : *Les super cartes bancaires débarquent*

Comment un cybercriminel peut infiltrer votre réseau ?

	Comment un cybercriminel peut infiltrer votre réseau ?

La sécurité est plus que jamais une priorité pour les entreprises, contribuant activement à sa réussite. Les RSSI doivent désormais s'assurer que leurs projets en matière de sécurité IT sont en phase avec les objectifs de l'entreprise.

Nous sommes tous connectés à Internet, ce qui est très positif. Mais ce lien permanent implique que nous sommes tous au cœur d'un écosystème de grande envergure. Il est essentiel de comprendre que tout ce qui touche une organisation impactera également de nombreuses autres entreprises, et notamment ses partenaires.
Ainsi, en cas de piratage d'une entreprise, ce sont des données personnelles identifiables qui sont détournées. Ces données peuvent être revendues à des spécialistes de l'usurpation d'identité ou constituer un terreau favorable aux attaques de phishing. Plus l'assaillant disposera d'informations sur vous, plus l'email qu'il vous enverra apparaîtra comme légitime et vous incitera à cliquer sur un lien malveillant.
Notons que les tactiques d'attaques actuelles sont similaires à celles d'il y a quelques années : récupération de mots de passe faibles, attaques de type phishing et téléchargement de logiciels malveillants à partir de sites web infectés ou de publicités malveillantes. Sauf qu'aujourd'hui, l'assaillant a gagné en furtivité et en efficacité lorsqu'il mène son attaque.

Penchons-nous, par exemple, sur les réseaux sociaux et les services en ligne. Nous sommes très nombreux à les utiliser, qu'il s'agisse de Facebook, de LinkedIn, ou encore des sites de rencontres en ligne. Les assaillants l'ont parfaitement compris et capitalisent sur la fibre émotionnelle de chacun. Ils établissent ainsi leur passerelle d'entrée vers les dispositifs des utilisateurs en s'aidant de ces sites et de techniques d'ingénierie sociale. Ainsi, si les méthodes d'ingénierie sociale restent les mêmes, les vecteurs et la surface d'attaque ont, en revanche, progressé. Parallèlement, ce sont les techniques de furtivité qui ont gagné en précision, avec des assaillants toujours plus aptes à se dissimuler. Se contenter d'utiliser les antivirus traditionnels n'est donc tout simplement plus suffisant.
Parmi les techniques utilisées, l'attaque de type phishing est la méthode principale pour s'immiscer au sein des réseaux d'entreprise.
Un email de phishing, conçu pour paraître le plus légitime possible, est envoyé avec un fichier joint ou une URL malveillante, et incitant l'utilisateur à ouvrir le fichier ou à cliquer sur l'URL. L'attaque par téléchargement furtif (ou drive–by attack) est une autre technique utilisée par les assaillants. Ces derniers piratent un site Web et y installent un script java malveillant qui redirigera l'utilisateur vers un autre site hébergeant un logiciel malveillant téléchargé en arrière-plan vers l'équipement de l'utilisateur. Dans le cas d'une attaque ciblée, les assaillants peuvent passer des mois à identifier les sites Web les plus consultées par les organisations ciblées, pour ensuite les infecter.
Le malvertising (publicité malveillante) compte également parmi les techniques utilisées. Cette attaque emprunte les codes des attaques drive-by, mais l'assaillant se focalisera sur l'infection des sites de publicités. Il devient possible d'infecter un seul de ces sites qui, à son tour, pourra infecter jusqu'à 1 000 autres sites Web. Ou l'art d'industrialiser son attaque.
Enfin, n'oublions pas l'attaque mobile. Nombre de ces attaques sont similaires à celles mentionnées plus haut, mais elles ciblent les dispositifs mobiles. Notons qu'il est possible d'infecter un dispositif mobile via un message SMS, ou à l'aide d'un logiciel malveillant qui se présente en tant qu'application ludique ou de contenu pour adultes.
Lorsque l'assaillant est rentré dans un réseau et qu'il réside sur le dispositif d'un utilisateur (ordinateur de bureau ou portable, équipement mobile), il doit désormais injecter de nouveaux logiciels malveillants et outils pour mener à bien sa mission. Généralement, les informations de valeur ne sont pas stockées sur les postes de travail, mais plutôt sur les serveurs et des bases de données.

Voici donc un aperçu des étapes supplémentaires pouvant être mises en œuvre par un cybercriminel déjà présent dans le réseau:
• Téléchargement d'autres outils et logiciels malveillants pour compromettre davantage le réseau.
• Exploration du réseau pour identifier les serveurs hébergeant les données ciblées.
• Recherche du serveur Active Directory contenant tous les identifiants d'authentification, dans l'objectif de pirater ces données, véritable sésame pour le cybercriminel.
• Une fois les données ciblées identifiées, recherche d'un serveur provisoire pour y copier ces données. Le serveur idéal est un serveur stable, à savoir toujours disponible, et disposant d'un accès sortant vers Internet.
• Exfiltration furtive et lente de ces données vers les serveurs des assaillants, généralement déployés dans le cloud, ce qui rend la neutralisation des communications plus complexe.

Les cybercriminels présents au sein du réseau sur une longue durée pourront obtenir tous types d'informations disponibles puisque les données d'entreprise, dans leur grande majorité, sont archivées sous format électronique. Plus le cybercriminel est présent sur le réseau, plus il en apprend sur les processus et les flux de données de votre entreprise. L'attaque Carbanak qui a ciblé de nombreuses banques dans le monde en est la parfaite illustration. Lors de cette exaction, les cybercriminels sont remontés jusqu'aux ordinateurs des administrateurs ayant accès aux caméras de vidéosurveillance. Ils ont ainsi pu surveiller de près le fonctionnement du personnel bancaire et enregistrer tous les processus dans le détail. Ces processus ont été reproduits par les cybercriminels pour transférer des fonds vers leurs propres systèmes.
Comme déjà souligné, une brèche dans le réseau s'initie généralement par un simple clic d'un utilisateur sur un lien malveillant. Après avoir investi le poste de l'utilisateur piraté, l'assaillant commence à explorer le réseau et à identifier les données qu'il souhaite détourner. C'est dans ce contexte que la notion de segmentation de réseau devient essentielle. Cette segmentation permet de maîtriser l'impact d'un piratage puisque l'entreprise victime peut isoler la faille et éviter tout impact sur le reste du réseau. D'autre part, elle permet de cloisonner les données sensibles au sein d'une zone hyper-sécurisée qui rendra la tâche bien plus complexe pour ceux qui souhaitent les exfiltrer. Pour conclure, gardons à l'esprit qu'il est impossible de protéger et de surveiller le réseau dans sa totalité, compte tenu de son périmètre étendu et de sa complexité. Il s'agit donc d'identifier les données les plus sensibles, de les isoler et de porter son attention sur les chemins d'accès vers ces données.

Réagissez à cet article

Source : *Comment un cybercriminel peut infiltrer votre réseau | Data Security Breach*

Que trouve-t-on dans le darknet ?

Que trouve-t-on dans le darknet ?

Sur le darknet, les pages Internet ne sont pas indexées. Vous ne pouvez donc pas les trouver via les moteurs de recherche classiques, comme Google ou Yahoo par exemple. Vous ne pouvez pas non plus y accéder par votre navigateur habituel, comme Internet Explorer ou Mozilla. Ces pages ne répondent pas au codage classique du genre « .fr » ou « .net ». Elles se terminent par « .oignon » : pour que les échanges soient anonymes sur cet Internet caché, il faut passer par une multitude de relais, comme plusieurs couches d'un oignon.

Tous ces relais expliquent pourquoi sur le darknet la connexion est plus longue. Au départ, cet Internet fantôme qui garantit l'anonymat a été créé pour aider à la liberté d'information dans des pays où tout est verrouillé, comme en Chine. Les dissidents pouvaient, via le darknet, communiquer de manière protégée. Un anonymat et une clandestinité largement détournés à des fins malhonnêtes : ventes d'armes, pédophilie ou drogues pullulent sur ce Web caché. L'un des logiciels les plus utilisés pour surfer sur le darknet s'appelle Tor (pour The Onion Router). On estime que les sites Internet sur le Web crypté sont 500 fois plus nombreux que sur le Web traditionnel.

Réagissez à cet article

Source : *Internet : que trouve-t-on dans le darknet ?*