Les meilleurs anti-malware gratuits du moment

	Les meilleurs anti-malware gratuits du moment

Les menaces sont omnipresentes sur internet. La performance des antivirus est alors remise en question. En effet, dans certains cas, ils ne sont pas assez puissants pour bloquer ces malwares. Le recours aux meilleurs logiciels anti-malware s'avère alors indispensable.

L'IObit Malware Fighter : fiable et s'adapte bien

Ce logiciel est gratuit pour repérer et lutter contre les malwares. Utilitaire efficace contre les adwares, chevaux de Troie, vers, keyloggers, etc, il se complète parfaitement avec un antivirus. Il offre une protection instantanée, une analyse heuristique, et le choix de recourir à un scan manuel. Il n'existe qu'en version anglaise et s'adapte à tous systèmes d'exploitation Microsoft, allant de Windows XP à Windows 10.

Le Spybot – Search& Destroy : l'anti-malware recherche et destruction par excellence

Celui-ci, également gratuit a la même capacité que le précédent. Il a deux sortes d'interface, l'une pour les néophytes et l'autre pour les professionnels. Ce logiciel protège les navigateurs contre les menaces et permet une analyse manuelle du système. Disponible seulement en anglais, il s'adapte sur les mêmes systèmes d'exploitation quel' L'IObit Malware Fighter .

L'AdwCleaner : le suppléant fiable

L'AdwCleaner est un logiciel gratuit qui détecte et supprime les malwares. Il est efficace contre les adwares, toolbars, PUP/LPI ethijackers. C'est un utilitaire qui fonctionne uniquement par analyse manuelle mais il faut disposer de la dernière version. L'AdwCleaner est un excellent complément d'un antivirus ou un autre logiciel anti-malwares. Il est disponible en langue française et dispose d'une même adaptabilité de système que les deux premiers logiciels.

Emsisoft Anti-Malware : le bilingue

A la différence des trois premiers logiciels, celui-ci est payant. Sa validité est de 30 jours pour épargner votre système contre les menaces de types cheval de Troie, vers, spywares, etc. Il se complète à 100 % avec un antivirus classique. Il offre la possibilité de scanner manuellement le système et permet une surveillance instantanée, de même qu'une analyse heuristique. Il est disponible à la fois en anglais et en français. Cet anti-malware s'adapte sur tous systèmes de Windows XP à Windows 10.

Le Malwarebytes Anti-Malware : bref, mais efficace

Ce logiciel possède un arsenal complet pour tenir éloignés tous les malwares. Il est efficace contre les spamgiciels, les chevaux de Troie, les spywares, etc. Son scanner manuel et analyse heuristique constituent un appui optimal pour un antivirus. Il est également disponible en bilingue. Sa validité n'est que de 14 jours.

TDSS Killer : le tueur de malware

Le TDSS Killer est un anti-malware de Kaspersky. Sa fonction majeure est de détecter et supprimer les infections de type rootkit. Son analyse se fait uniquement en mode manuelle. Le savoir-faire de Kaspersky est une garantie chez le TDSS Killer pour déceler les malwares dissimulés. Son point faible est sa seule disponibilité en anglais.

En somme, même si les antivirus classiques sont conçus pour se parer aux menaces, il arrive que les malwares les contournent. C'est pourquoi il est mieux de se doter d'un logiciel anti-malware efficace. Il est même prudent d'en recourir à plusieurs.
Article original de Sekurigi

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Les meilleurs anti-malware gratuits du moment – @Sekurigi

---

Tor envahi par des mouchards ?

Tor envahi par des mouchards ?

Selon des chercheurs, 110 relais du réseau d'anonymisation Tor étaient à la recherche d'informations sur les services cachés auxquels ils permettent d'accéder.

Deux chercheurs de la Northeastern University (Boston), Guevara Noubir et Amirali Sanatinia, démontrent à leur tour que le réseau Tor est la cible d'espions. Cette fois, les chercheurs n'ont pas étudié des noeuds de sortie détournés pour mener des attaques de type « *Man In The Middle* ». Ils se sont intéressés à d'autres relais : ceux qui permettent d'accéder à des services cachés et référencent des éléments clés (adresse en .onion, clé publique, points d'introduction) .

Ces relais (HSDirs, *Hidden Service Directories*) font partie intégrante des services cachés et du dark web. Mais des entités (gouvernements, entreprises, hackers, etc.) peuvent en modifier le code pour obtenir des informations, découvrir une adresse ou exploiter une faille.

Pot de miel

Dans le cadre de leurs travaux, les chercheurs ont déployé 4500 services cachés (en .onion), 72 jours durant. « *Nos résultats expérimentaux montrent que, durant cette période, au moins 110 relais (HSDirs) étaient à la recherche d'informations sur les services cachés qu'ils accueillent* », soulignent les chercheurs dans une note. Ils ont également indiqué à *Motherboard* que la recherche de vulnérabilités n'est pas exclue des motivations de ceux qui pilotent ces relais. La plupart d'entre eux sont hébergés aux États-Unis, en Allemagne et en France. Mais il est toujours possible d'opérer un serveur à distance…

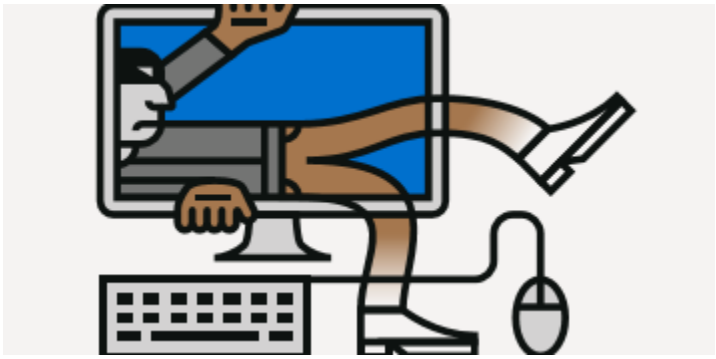
Roger Dingledine, cofondateur du projet Tor, a expliqué au magazine que peu, voire aucun de ces relais ne se trouvent dans le réseau Tor en ce moment. Le projet travaille, par ailleurs, à la mise en place d'une prochaine génération de services « *onion* ». Quant aux chercheurs, ils présenteront leurs travaux lors de la Defcon 24, qui se déroulera du 4 au 7 août prochains à Las Vegas.

Article original de Ariane Beky

Original de l'article mis en page : Tor envahi par des noeuds espions ?

---

77 % des entreprises totalement impuissantes face à des Cyberattaques



77 % des entreprises totalement impuissantes face à des Cyberattaques

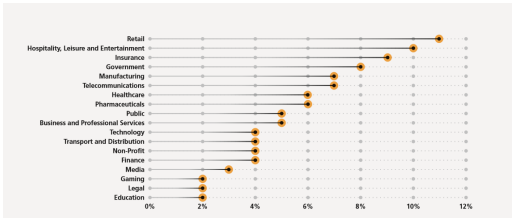
Pénurie de compétences et manque d'investissements : les entreprises sont non seulement vulnérables aux attaques, mais aussi impuissantes pour les résoudre seules. Décryptant les tendances de ces trois dernières années dans le monde, un rapport de NTT Com Security souligne le peu de progrès réalisés dans ce domaine, et note même un recul….

Le GTIR (« Global Threat Intelligence Report ») analyse une énorme masse de données issues de 24 centres d'opérations de sécurité (SOC), sept centres R&D, 3 500 milliards de logs et 6,2 milliards d'attaques. Ces résultats sont donc particulièrement intéressants pour suivre l'état des menaces dans le monde. Son édition 2016, qui décrypte les tendances de ces trois dernières années souligne le peu de progrès réalisés par les entreprises dans leur lutte contre les menaces, et note même une légère hausse du nombre d'entre elles mal préparées qui s'élève à 77 %. Face à des attaques d'envergure, elles doivent le plus souvent solliciter une intervention extérieure. Seules 23 % des organisations seraient donc en mesure de se défendre efficacement contre des incidents de sécurité majeurs.

Le retail le plus touché par les incidents

Après des années passées en tête des secteurs les plus touchés dans les précédents rapports GTIR, la finance cède sa place à la grande distribution qui enregistre 22 % des interventions sur incidents (contre 12 % l'année passée) de NTT Com Security. La grande distribution a été particulièrement exposée aux attaques de spear phishing. Parce qu'elles brassent d'importants volumes de données personnelles, dont des informations bancaires, les organisations de ce secteur constituent une cible particulièrement attractive, et ce au point d'enregistrer le plus fort taux d'attaques par client. Le secteur financier a représenté 18 % des interventions.

En 2015, le groupe NTT a également noté une augmentation des attaques à l'encontre du secteur de l'hôtellerie, des loisirs et du divertissement. Tout comme la grande distribution, ce secteur draine aussi de gros volumes d'informations personnelles, y compris des données de cartes bancaires. De même, le niveau relativement élevé des transactions dans le milieu (hôtels, stations touristiques…) suscitent la convoitise des attaquants. Avec sa palette de programmes de fidélité, l'hôtellerie est une vraie mine d'informations personnelles. Plusieurs violations de sécurité ont d'ailleurs défrayé la chronique en 2015 : Hilton, Starwood ou encore Hyatt.



Les attaques par secteur – 2015

Hausse de 17 % des menaces internes

A quels types d'incidents NTT Com Security a-t-il été confronté ? Les violations de sécurité ont représenté 28 % des interventions en 2015, contre 16 % en 2014. Un grand nombre d'incidents concernaient des vols de données et de propriété intellectuelle. Les menaces internes ont connu de leur côté une véritable envolée, passant de seulement 2 % en 2014 à 19 % en 2015. Elles résultent le plus souvent d'une utilisation abusive des données et ressources informatiques par des salariés ou prestataires externes.

En 2015, 17 % des interventions de NTT Com Security se sont produites sur des attaques par spear phishing, alors qu'elles représentaient moins de 2 % auparavant. Basées sur des tactiques sophistiquées d'ingénierie sociale, comme l'utilisation de fausses factures, ces attaques visaient principalement des dirigeants et autres personnels de la fonction comptabilité-finance.

Enfin, le GTIR 2016 a enregistré un recul des attaques DDoS par rapport aux années précédentes. Elles ont reculé de 39 % par rapport à 2014. Le rapport attribue cette baisse aux investissements réalisés dans les outils et services de défense contre ce type d'agression.

A noter cependant une augmentation des cas d'extorsion, où les victimes d'acquittent d'une rançon pour lever les menaces ou stopper une DDos en cours.

Top 10 External Vulnerabilities	
Outdated PHP Version	8%
Cross-Site Scripting (CSS/XSS)	7%
Outdated Apache Web Server	7%
SSL/TLS Information Disclosure	6%
Web Clear Text Username/Password	5%
Weak SSL/TLS Ciphers/Certificate	5%
Outdated Apache Tomcat Server	4%
Weak/No HTTPS cache policy	4%
Cookie without HTTPOnly attribute set	3%
SSL Certificate Signed using Weak Hashing Algorithm	3%

Top 10 Internal Vulnerabilities	
Outdated Java Version	51%
Outdated Adobe Flash Player	11%
Outdated Adobe Reader and Acrobat	5%
Outdated Microsoft Windows	3%
Outdated Microsoft Internet Explorer	3%
Outdated Mozilla Firefox	2%
Outdated Microsoft Office	1%
Outdated Linux Kernel	1%
Outdated Novell Client	1%
Outdated OpenSSH Version	1%

Top 10 des vulnérabilités internes et externes – 2015. Parmi l'ensemble des vulnérabilités externes identifiées, le top 10 compte pour 52 % des cas recensés. Les 48 % restants étaient composés de milliers de vulnérabilités. Parmi l'ensemble des vulnérabilités internes identifiées, le top 10 compte pour 78 % des cas recensés. Ces 10 vulnérabilités internes étaient directement liées à la présence d'applications obsolètes sur les systèmes visés.

Le rapport ici

Article original de Juliette Paoli

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Cyberattaques : 77 % des entreprises totalement impuissantes | Solutions Numériques

Détecter les futurs terroristes sur Internet ? L’Europe veut s’inspirer d’Israël

Détecter les futurs terroristes sur Internet ? L’Europe veut s’inspirer d’Israël

Le coordinateur de l'anti-terrorisme pour lUnion européenne, Gilles de Kerchove, s'est rendu en Israël pour trouver des solutions technologiques qui permettraient de détecter automatiquement des profils suspects sur les réseaux sociaux, grâce à des algorithmes de plus en plus intrusifs.

Plus les attentats en Europe se multiplient, plus on découvre que les profils psychologiques et sociaux des kamikazes et de leurs associés sont très divers, jusqu'à paraître indétectables. Le cas de Mohamed Lahouaiej-Bouhlel, dont on ne sait pas toujours très bien s'il s'agit d'un déséquilibré qui se cherchait un modèle ultra-violent à imiter, ou d'un véritable djihadiste islamiste radicalisé à une vitesse inédite, laisse songeur. Bisexuel, amant d'un homme de 73 ans, mangeur de porc, aucune connexion connue avec des réseaux islamistes… l'auteur de l'attentat de Nice était connu des services de police pour des faits de violence de droit commun, mais n'avait rien de l'homme que l'on pourrait soupçonner d'organiser une tuerie motivée par des considérations idéologiques.
Or c'est un problème pour les services de renseignement à qui l'on demande désormais l'impossible, à la Minority Report, c'est-à-dire de connaître à l'avance le passage à l'acte d'un individu, pour être capable de l'appréhender avant son méfait, même lorsqu'objectivement rien ne permettait de présager l'horreur.

C'EST POUR ÇA QUE JE SUIS ICI. NOUS SAVONS QU'ISRAËL A DÉVELOPPÉ BEAUCOUP DE MOYENS DANS LE CYBER

Néanmoins, l'Union européenne ne veut pas se résoudre à la fatalité, et va chercher en Israël les méthodes à appliquer pour détecter sur Internet les terroristes susceptibles un jour de passer à l'acte. « C'est un défi », explique ainsi à l'agence Reuters Gilles de Kerchove, le coordinateur de l'UE pour l'anti-terrorisme, en marge d'une conférence sur le renseignement à Tel Aviv. « Nous allons trouver bientôt des moyens d'être beaucoup plus automatisé » dans la détection des profils suspects sur les réseaux sociaux, explique-t-il. « C'est pour ça que je suis ici ».
« Nous savons qu'Israël a développé beaucoup de moyens dans le cyber », pour faire face aux attaques d'Israéliens par des Palestiniens, ajoute le haut fonctionnaire européen, et l'UE veut s'en inspirer.

ÉTABLIR DES PROFILS SOCIOLOGIQUES ET SURVEILLER LES COMMUNICATIONS

Selon un officiel israélien interrogé par l'agence de presse, il s'agit d'établir constamment des profils types de personnes à suspecter, en s'intéressant non plus seulement aux métadonnées qui renseignent sur le contexte des communications et les habitudes d'un individu, mais bien sur le contenu-même des communications sur les réseaux sociaux.
Mis à jour quotidiennement au gré des nouveaux profils qui émergent, des paramètres comme l'âge de l'internaute, sa religion, son origine socio-économique et ses liens avec d'autres suspects, seraient aussi pris en compte par les algorithmes israéliens – ce qui semble difficilement compatible en Europe avec les textes internationaux protégeant les droits de l'homme, que l'Union européenne s'est engagée à respecter.

DES BOÎTES NOIRES TOUJOURS PLUS INTRUSIVES ?

En somme, c'est exactement ce que nous redoutions avec les fameuses boîtes noires permises par la loi Renseignement en France, dont le Conseil constitutionnel n'a su que dire, et qui se limitent officiellement aux métadonnées. Là aussi, il s'agit d'utiliser des algorithmes, dont on ne sait pas du tout sur quoi ils se basent, pour détecter des profils suspects.

Eagle Security & Defense, une société israélienne proposant des solutions de surveillance sur Internet, a reçu la visite de Christian Estrosi en début d'année.
Il n'est toutefois pas dit que la technologie israélienne soit importée telle quelle, d'autant que M. De Kerchove a lui-même rappelé que le droit européen n'autoriserait pas un tel degré d'intrusion dans la vie privée. Mais le mécanisme décrit par l'officiel d'Israël est très proche.
Il vise tout d'abord à réaliser une première détection sommaire des profils suspects, puis à déterminer parmi eux ceux qui doivent faire l'objet d'une surveillance individualisée. C'est exactement ce que prévoit la loi Renseignement, qui autorise l'installation de boîtes noires chez les FAI ou les hébergeurs et éditeurs pour détecter des comportements suspects d'anonymes, avant de permettre une identification des personnes dont il est confirmé qu'elles méritent une attention particulière.
En Israël, le ratio serait d'environ 20 000 personnes considérées suspectes pour 1 million d'internautes, sur lesquelles ressortiraient entre 10 et 15 profils nécessitant une surveillance étroite.

CHRISTIAN ESTROSI DÉJÀ INTÉRESSÉ

L'information de Reuters confirme ce qu'indiquaient Les Échos le week-end dernier dans un reportage bien informé. « L'Etat hébreu, dont la population a connu sept guerres et deux Intifada depuis sa création, est bel est bien devenu un cas d'école, dans sa façon de gérer une situation d'insécurité permanente. Une expertise dans la mire des décideurs européens », écrivait le quotidien,
Il précisait qu'en février dernier, l'ancien maire de Nice et actuel président de la région Provence-Alpes-Côte d'Azur, Christian Estrosi, s'était déjà rendu en Israël, où il aurait rencontré le PDG de la société Eagle Security and Defense, Giora Eiland, qui est aussi ex-directeur du Conseil de sécurité nationale israélien.
Lors de cette visite, Christian Estrosi aurait insisté sur la nécessité « d'être à la pointe de la lutte par le renseignement contre la cybercriminalité lorsqu'on sait que la radicalisation se fait par le biais des réseaux sociaux ». On imagine que cette conversation lui est revenue en mémoire lorsque sa ville a été meurtrie.
Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : Détecter les futurs terroristes sur Internet ? LEurope veut sinspirer dIsraël – Politique – Numerama

---

Les campagnes de sensibilisation à la cybersécurité portent (petit à petit) leurs fruits

Les campagnes de sensibilisation à la cybersécurité portent (petit à petit) leurs fruits

---

Une étude souligne que les primo-adoptants de nouvelles technologies demandent l'autorisation avant d'amener de nouveaux équipements au travail.

Sachant que plus de 25 % des attaques identifiées en entreprise devraient associer l'Internet des objets d'ici à 2020 [1] et, pour nombre d'entre elles, s'inviter sur le lieu de travail, les conclusions de cette étude marquent une évolution significative dans la bonne direction et prouvent que les collaborateurs cernent mieux le rôle qui leur incombe dans le domaine de la cybersécurité.
Néanmoins, les résultats de cette enquête menée auprès de cadres en entreprise – les plus susceptibles, de par leur rémunération et leur état d'esprit, à être des primo-adoptants des nouvelles technologies – sont contrastés puisque 39 % d'entre eux auraient tendance à se soustraire au contrôle du service informatique. Ce qui laisse une énorme marge de risque.
Pire, parmi les collaborateurs qui se disent prêts à court-circuiter le service informatique, un sur huit « ne révélerait à personne » son intention d'introduire un nouvel appareil au sein de l'entreprise ou d'installer un outil professionnel, messagerie électronique par exemple, sur un équipement non sécurisé.

L'attitude a une incidence sur le respect des règles
L'étude révèle que le respect des règles de cybersécurité, telles que celles concernant l'introduction d'un nouvel équipement, est largement fonction des attitudes et opinions de chacun vis-à-vis de la technologie. Les professionnels ayant dérogé, dans le passé, aux règles de cybersécurité de leur entreprise justifient essentiellement leur geste par leur volonté de recourir à un outil ou un service plus efficace, ou considéré à l'époque comme le meilleur sur le marché. Les entreprises doivent élargir, et non restreindre, le choix de leurs collaborateurs, en s'appuyant sur la technologie et la formation pour gérer les risques.

Les intérimaires exigent une surveillance à temps complet
Les sous-traitants constituent le groupe contournant le plus souvent les règles de cybersécurité, 16 % des participants affirmant avoir vu un intérimaire se soustraire à celles-ci.
« Le concept BYOD a beau aujourd'hui avoir fait ses preuves, nombre d'individus continuent à éprouver des difficultés à dissocier clairement l'accès aux données personnelles de celui aux données professionnelles sur les appareils leur appartenant. Quantité d'entreprises ont déployé des solutions d'administration pour leur parc d'équipements, mais c'est la connectabilité de ces derniers qui pose véritablement problème, d'autant que la ligne de démarcation entre les services cloud orientés métier et les services personnels s'estompant, des passerelles méconnues sont jetées entre les réseaux d'entreprise et l'Internet en général. Une sécurité dernier cri doit être en mesure d'empêcher que toute communication à partir d'un équipement ne se transforme en faille et diminuer le plus possible les risques encourus par l'entreprise. » Greg Day, vice-président et responsable de la sécurité (CSO) pour la zone Europe, Moyen-Orient et Afrique (EMEA) chez Palo Alto Networks

Recommandations
Les entreprises doivent poursuivre leurs actions de sensibilisation auprès de leurs collaborateurs afin de faire en sorte que ceux positionnés en première ligne défensive possèdent les compétences nécessaires pour déceler les menaces.
Les professionnels de la sécurité doivent encadrer étroitement les activités des collaborateurs non permanents ou des sous-traitants, et veiller à ce que leur soient communiquées les mêmes informations que celles dispensées au personnel à temps complet.
Les entreprises doivent intégrer des solutions de sécurité modernes, en harmonie avec les nouvelles évolutions technologiques, afin d'écarter les fragilités inhérentes à un environnement informatique en constante évolution.
Les entreprises doivent réfléchir à la façon dont elles recensent et favorisent l'utilisation, dans de bonnes conditions de sécurité, d'applications et de services cloud dignes de confiance ou approuvés par leurs soins, et gèrent celle de ceux qu'elles ne jugent pas dignes de leur confiance ou n'avalisent pas.
Méthodologie de recherche
L'enquête a été menée en ligne, par Redshift Research en octobre 2015, auprès de 765 décideurs d'entreprises comptant plus d'un millier de salariés au Royaume-Uni, en Allemagne, en France, aux Pays-Bas et en Belgique.
Article original de edubourse.com

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Les campagnes de sensibilisation à la cybersécurité portent (petit à petit) leurs fruits

---

Directive européenne sur la sécurité des réseaux et des systèmes d'information

Directive européenne sur la sécurité des réseaux et des systèmes d'information

Les entreprises qui fournissent des services essentiels, par exemple l'énergie, les transports, les services bancaires et de santé, ou numériques, tels que les moteurs de recherche et les services d'informatique en nuage, devront améliorer leur capacité à résister à des cyber-attaques, selon les premières règles de cybersécurité à l'échelle européenne, approuvées par les députés mercredi.

L'établissement de normes de cybersécurité communes et renforcer la coopération entre les pays de l'Union aidera les entreprises à se protéger elles-mêmes, et aussi à prévenir les attaques contre les infrastructures interconnectées des pays européens, estiment les députés.

« Des incidents de cybersécurité possède très souvent un aspect transfrontalier et concernent donc plus d'un État membre de l'Union européenne. Une protection fragmentaire de la cybersécurité nous rend tous vulnérables et pose un risque de sécurité important pour l'Europe dans son ensemble. Cette directive établira un niveau commun de sécurité de réseau et d'information et renforcera la coopération entre les États membres. Cela contribuera à prévenir à l'avenir les cyberattaques sur les infrastructures interconnectées européennes importantes », a déclaré le rapporteur du Parlement Andreas Schwab (PPE, DE).

La directive européenne sur la sécurité des réseaux et des systèmes d'information « est également l'un des premiers cadres législatifs qui s'applique aux plates-formes. En phase avec la stratégie du marché unique numérique, elle établit des exigences harmonisées pour les plates-formes et veille à ce qu'elles puissent observer des règles similaires quel que soit l'endroit de l'Union européenne où elles opèrent. C'est un énorme succès et une première étape importante vers l'établissement d'un cadre réglementaire global pour les plates-formes dans l'Union », a-t-il ajouté.

Les pays de l'UE devront lister les entreprises de « services essentiels »

La nouvelle législation européenne prévoit des obligations en matière de sécurité et de suivi pour les « opérateurs de services essentiels » dans des secteurs tels que ceux de l'énergie, des transports, de la santé, des services bancaires et d'approvisionnement en eau potable. Les États membres de l'UE devront identifier les entités dans ces domaines en utilisant des critères spécifiques, par exemple si le service est essentiel pour la société et l'économie, et si un incident aurait des effets perturbateurs considérables sur la prestation de ce service.

Certains fournisseurs de services numériques – les marchés en ligne, les moteurs de recherche et les services d'informatique en nuage – devront aussi prendre des mesures pour assurer la sécurité de leur infrastructure et devront signaler les incidents majeurs aux autorités nationales. Les exigences de sécurité et de notification sont, cependant, plus légères pour ces fournisseurs. Les micro- et petites entreprises numériques seront exemptées de ces exigences.

Mécanismes de coopération à l'échelle européenne

Les nouvelles règles prévoient un « groupe de coopération » stratégique pour échanger l'information et aider les États membres à renforcer leurs capacités en matière de cybersécurité. Chaque pays de l'Union devra adopter une stratégie nationale relative à sécurité des réseaux et des systèmes d'information.

Les États membres devront aussi mettre en place un centre de réponse aux incidents de sécurité informatique (CSIRT) pour gérer incidents et risques, discuter des questions de sécurité transfrontalière et identifier des réponses coordonnées. L'Agence européenne pour la sécurité des réseaux et de l'information (ENISA) jouera un rôle clé dans la mise en œuvre de la directive, en particulier en matière de coopération. La nécessité de respecter les règles de protection des données est réitérée tout au long de la directive.

Prochaines étapes

La directive sur la sécurité des réseaux et des systèmes d'information sera bientôt publiée au Journal officiel de l'Union européenne et entrera en vigueur le vingtième jour suivant sa publication. Les États membres auront alors 21 mois pour transposer la directive dans leur législation nationale et six mois supplémentaires pour identifier les opérateurs de services essentiels.

Directive sur la sécurité des réseaux et des systèmes d'information – texte approuvé par le Parlement et le Conseil
http://data.consilium.europa.eu/doc/document/ST-5581-2016-REV-1/fr/pdf
Procédure: codécision, seconde lecture
Source : Parlement européen

Réagissez à cet article

Original de l’article mis en page : Cybersécurité: les députés soutiennent les règles pour aider les entreprises de services clés à… – Linkis.com

---

Quel cadre pour l’État d’urgence et la copie des données informatiques ?

Quel cadre pour l’État d’urgence et la copie des données informatiques ?

Le gouvernement a entendu le Conseil constitutionnel, et fixé cette fois-ci un cadre très précis à la copie et l'utilisation des données informatiques saisies lors des perquisitions administratives réalisées dans le cadre de l'état d'urgence.

Ce mardi matin, nous expliquions que pour faire revenir la possibilité de saisir des données informatiques lors de perquisitions administratives organisées dans le cadre l'état d'urgence, le gouvernement aurait l'obligation de se conformer aux demandes d'encadrement fixées par le Conseil constitutionnel dans sa décision du 19 février 2016. Celui-ci avait en effet censuré le dispositif prévu à l'origine en novembre 2015, qui autorisait de copier les données accessibles sur place, sans aucun encadrement, ni sur la forme, ni sur le fond.

Nous avions ainsi résumé les préconisations des sages du Palais Royal :
• N'autoriser la copie que si une infraction est constatée lors de la perquisition administrative ;
• Limiter la copie aux données en lien avec l'infraction constatée ;
• Prévoir un cadre strict de conservation et d'exploitation des données saisies ;
• Faire entrer le juge dans la boucle.

Jean-Jacques Urvoas, ministre de la Justice, au Sénat

Or il faut reconnaître au gouvernement, sans doute influencé en ce sens par le ministre de la justice Jean-Jacques Urvoas, d'avoir su prendre parfaitement acte des demandes du Conseil constitutionnel. Tel que présenté en conseil des ministres et tel qu'il devrait être adopté par le Parlement, le projet de loi prorogeant l'état d'urgence fixe un cadre très précis, même s'il ne va pas aussi loin dans le filtrage que ce qu'ont souhaité les membres du Conseil.

PAS D'ACCÈS AU CLOUD, CONSULTATION OBLIGATOIRE D'UN JUGE…

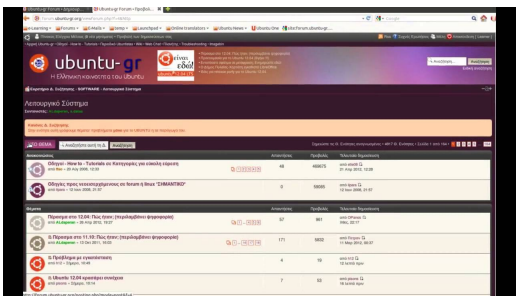
Nous avons mis en gras les éléments les plus importants du projet de loi, qui concernent notamment l'obligation de motiver la copie des données et de ne les consulter qu'après l'aval d'un juge administratif qui aura 48 heures pour se prononcer. On notera au passage que la copie est désormais limitée aux seules « données contenues dans tout système informatique présent sur les lieux de la perquisition », ce qui doit exclure en principe l'accès aux données stockées dans le Cloud – auparavant celle-ci était prévue par une référence aux « données accessibles à partir du système initial ou disponibles pour le système initial », qui a disparu.

« Si la perquisition révèle l'existence d'éléments, notamment informatiques, relatifs à la menace que constitue pour la sécurité et l'ordre publics le comportement de la personne concernée, les **données contenues dans tout système informatique ou équipement terminal présent sur les lieux** de la perquisition peuvent être saisies, soit par leur copie, soit par la saisie de leur support lorsque la copie ne peut être réalisée ou achevée pendant le temps de la perquisition.
La copie des données ou la saisie des systèmes informatiques ou des équipements terminaux est réalisée en présence de l'officier de police judiciaire, l'agent sous la responsabilité duquel est conduite la perquisition rédige un procès-verbal de saisie qui **en indique les motifs** et dresse l'inventaire des matériels saisis. Une copie de ce procès-verbal est remise aux personnes mentionnées au deuxième alinéa du présent I. Les données et les supports saisis sont conservés sous la responsabilité du chef du service ayant procédé à la perquisition. ***À compter de la saisie, nul n'y a accès avant l'autorisation du juge.***
L'autorité administrative **demande au juge des référés du tribunal administratif d'autoriser en tant sa partie leur exploitation.** Au vu des éléments révélés par la perquisition et, s'il l'estime utile, des données et matériels saisis, il **statue dans un délai de quarante-huit heures** à compter de sa saisine sur la régularité de la saisie et la demande de l'autorité administrative. **Sont exclus de l'autorisation les éléments déposrvus de tout lien avec la menace** que constitue le comportement de la personne concernée pour la sécurité et l'ordre publics. **En cas de refus** du juge des référés, et sous réserve de l'appel mentionné au dixième alinéa, **les données copiées sont détruites** et les supports saisis sont restitués à leur propriétaire.
Pendant le temps strictement nécessaire à leur exploitation autorisée par le juge des référés, les données et les supports saisis sont conservés sous la responsabilité du chef du service ayant procédé à la perquisition et à la saisie. Les systèmes informatiques ou équipements terminaux sont **restitués à leur propriétaire**, le cas échéant après qu'il a été procédé à la copie des données qu'ils contiennent, **à l'issue d'un délai maximal de quinze jours** à compter de la date de leur saisie ou de celle à laquelle le juge des référés, saisi dans ce délai, a autorisé l'exploitation des données qu'ils contiennent. **À l'exception de celles qui caractérisent la menace que constitue pour la sécurité et l'ordre publics le comportement de la personne concernée, les données copiées sont détruites à l'expiration d'un délai maximal de trois mois** à compter de la date de la perquisition ou de celle à laquelle le juge des référés, saisi dans ce délai, en a autorisé l'exploitation.
En cas de difficulté dans l'accès aux données contenues dans les supports saisis ou dans l'exploitation des données copiées, lorsque cela est nécessaire, les délais prévus à l'alinéa précédent peuvent être prorogés, pour la même durée, par le juge des référés saisi par l'autorité administrative au moins quarante-huit heures avant l'expiration de ces délais. Le juge des référés statue dans un délai de quarante-huit heures sur la demande de prorogation présentée par l'autorité administrative. **Si l'exploitation ou l'examen des données et des supports saisis conduisent à la constatation d'une infraction, ils sont conservés selon les règles applicables** en matière de procédure pénale.
Pour l'application des dispositions du présent article, le juge des référés est celui dans le ressort duquel se trouve le lieu de la perquisition. Il statue dans les formes prévues au livre V du code de justice administrative, sous réserve des dispositions du présent article. **Ses décisions sont susceptibles d'appel** devant le juge des référés du Conseil d'État dans un délai de 48 heures à compter de leur notification. Le juge des référés du Conseil d'État statue dans le délai de 48 heures. En cas d'appel, les données et les supports saisis demeurent conservés dans les conditions mentionnées au huitième alinéa du présent article. »
Dans ces conditions, il paraît vraisemblable qu'en cas de contestation, le Conseil constitutionnel ne trouvera rien à redire à la copie des données réalisées par les policiers.
Article original de Guillaume Champeau

Original de l’article mis en page : État d’urgence et copie des données informatiques : le cadre prévu par le gouvernement – Politique – Numerama

---

Deux millions de données d’utilisateurs Ubuntu dérobées



Deux millions de données d’utilisateurs Ubuntu dérobées

Le forum de la distribution Ubuntu a été victime d'une grave attaque informatique. Deux millions d'utilisateurs se sont fait voler leurs données.

Le butin du pirate est plus qu'impressionnant. Noms, mots de passe, adresse mails et IP, les données de deux millions d'utilisateurs du forum d'Ubuntu se sont envolées. La nouvelle a été annoncée jeudi dans un communiqué par Canonical l'éditeur d'Ubuntu. *« A 20h33 UTC le 14 Juillet 2016, Canonical et l'équipe ont été informés par un membre du Conseil Ubuntu que quelqu'un prétendait avoir une copie de la base de données des forums. Après enquête initiale, nous avons été en mesure de confirmer qu'il y avait bien eu une exposition des données et nous avons fermé les forums par mesure de précaution. »*

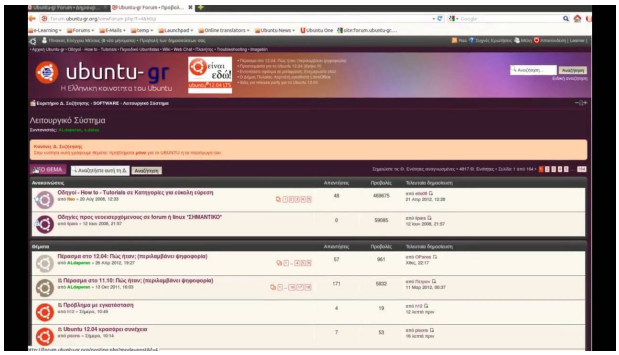
Une attaque par injection SQL

Une enquête plus poussée a révélé que la méthode employée est une injection SQL. Le pirate a pu injecter des requêtes SQL formatées dans la base de données des forums pour ensuite télécharger les datas.

Cependant, le communiqué précise que le hacker n'a pas pu accéder aux mots de passe utilisateur valides ni au référentiel de code Ubuntu ou au mécanisme de mise à jour. Moins certain, le rapport précise que normalement les services Canonical ou Ubuntu en sortent indemnes, comme certains forums.

Tout est plus ou moins rentré dans l'ordre

Des mesures correctives ont été prises et les forums restaurés. Les mots de passe du système et de la base de données ont été réinitialisés et ModSecurity, une Web Application Firewall vient renforcer le dispositif de sécurité. Selon Canonical, ça va mieux, même si après ce genre de vol il est légitime de penser que le mal est fait.



Article original de Victor Miget

Réagissez à cet article

Original de l'article mis en page : Ubuntu : les données de

deux millions d’utilisateurs dérobées

Les mots de passe disparaîtront progressivement d’ici 2025

Les mots de passe disparaîtront progressivement d’ici 2025

La technologie de biométrie comportementale et d'authentification à deux facteurs sont à la hausse comme des alternatives plus sûres, selon une étude.

Une étude de 600 professionnels en sécurité de l'opérateur de téléphonie mobile ID TeleSign a révélé que la protection du compte client est un souci majeur pour les entreprises, avec 72 % des personnes interrogées disant que les mots de passe seront éliminés progressivement d'ici à 2025. De plus en plus d'entreprises, selon le rapport, remplacent les mots de passe avec la biométrie comportementale et l'authentification à deux facteurs (2FA) avec 92 % des experts en sécurité affirmant que cela va améliorer la sécurité des comptes considérablement.

« La grande majorité des professionnels en sécurité ne font plus confiance aux mots de passe pour travailler », a déclaré Ryan Disraeli de TeleSign parce que 69 % des répondants ont dit qu'ils ne pensent pas que les noms d'utilisateur et mots de passe fournissent assez de sécurité. Les prises de contrôle de compte (ATO) étaient une préoccupation majeure pour 79 %, alors que 86 % sont préoccupés par l'authentification ID d'identité des utilisateurs du web et des applications mobiles avec 90 % étant touchées par des fraudes en ligne l'an dernier.

Plus de la moitié (54 %) des organisations disent qu'ils passeront à la biométrie comportementale en 2016 ou plus tard tandis que 85 % ont dit qu'ils mettraient en œuvre le 2FA dans les 12 prochains mois. Huit des 10 répondants croient que la biométrie comportementale ne dégradera pas l'expérience utilisateur.

Lire l'étude complète ici

https://iatranshumanisme.files.wordpress.com/2016/07/telesign-report-beyond-the-password-june-2016-1.pdf

Article original de Jaesa

Réagissez à cet article

Original de l'article mis en page : Les mots de passe disparaîtront progressivement d'ici 2025 | Intelligence Artificielle et Transhumanisme

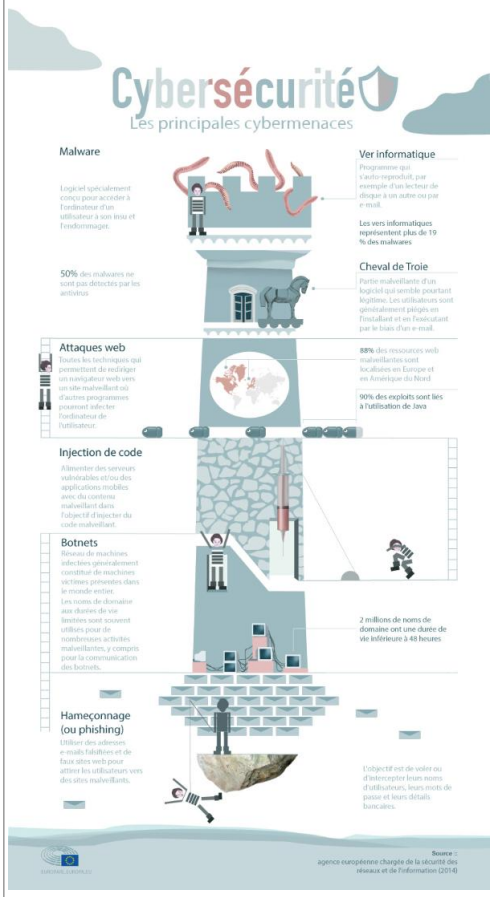
---

Directive sur la sécurité des

réseaux et des systèmes d’information

Directive sur la sécurité des réseaux et des systèmes d’information

Nos sociétés digitalisées reposent de plus en plus sur des réseaux électroniques qui peuvent faire l'objet de cyberattaques aux conséquences importantes. Afin de mieux faire face à ce type de menaces en ligne, le Parlement et le Conseil ont conclu en décembre dernier un accord sur les premières règles européennes en matière de cybersécurité. Celles-ci ont été soutenues par l'ensemble du Parlement réuni en session plénière ce mercredi 6 juillet.



Vols d'identité, faux sites web de banques, espionnage industriel ou inondation de données qui rendent un serveur incapable de répondre : les menaces en ligne sont nombreuses et visent tant les particuliers que les entreprises et les autorités publiques.
Les incidents et les attaques des systèmes d'information des entreprises et des citoyens pourraient représenter un coût de 260 à 340 milliards d'euros par an, selon les estimations de l'Agence européenne chargée de la sécurité des réseaux et de l'information.
Les cyberattaques menées contre certaines infrastructures clés de nos sociétés, comme les services bancaires, les réseaux d'électricité ou le secteur du contrôle aérien, peuvent avoir des conséquences particulièrement importantes sur notre quotidien.
Dans le cadre d'un Eurobaromètre publié en février 2015, les citoyens européens ont exprimé de fortes inquiétudes à propos de la cybersécurité : 89 % des internautes évitent de diffuser des informations personnelles en ligne. Selon 85 % des sondés, le risque d'être victime de cybercriminalité est de plus en plus important.

Vote en plénière
Les députés ont approuvé la directive sur la sécurité des réseaux et de l'information dans l'Union, qui définit une approche commune autour de la question de la cybersécurité.
Le texte prévoit une liste de secteurs dans lesquels les entreprises qui fournissent des services essentiels, liés par exemple à l'énergie, aux transports ou au secteur de la banque, devront être en mesure de résister aux cyberattaques.
La directive les oblige notamment à signaler les incidents de sécurité graves aux autorités nationales. Les fournisseurs de services numériques tels qu'Amazon ou Google devront également notifier les attaques majeures aux autorités nationales.
Ces nouvelles règles sur la cybersécurité visent également à renforcer la coopération entre États membres en cas d'incidents.

Téléchargez la directive sur la sécurité des réseaux et des systèmes d'information – texte approuvé par le Parlement et le Conseil :
http://data.consilium.europa.eu/doc/document/ST-5581-2016-REV-1/fr/pdf
Article original du Parlement Européen

Réagissez à cet article

Original de l’article mis en page : Cybersécurité : mieux faire face aux attaques en ligne