Techniques et astuces pour la robustesse de vos mots de passe

Techniques et astuces pour la robustesse de vos mots de passe

Les experts en cybersécurité ont tendance à être quelque peu cyniques envers les utilisateurs « lambda », particulièrement lorsqu'il s'agit du choix des mots de passe. Cependant, selon certains experts en sécurité informatique au sein du CyLab, l'Institut Security & Privacy de l'Université de Carnegie Mellon, les utilisateurs ordinaires ne semblent pas être aussi stupides qu'il n'y paraît. En effet les erreurs commises peuvent être classées en 4 catégories spécifiques. Le travail de sensibilisation nécessaire ne devrait pas être une tâche insurmontable.

La méthodologie de CyLab est la suivante : montrer aux gens des mots de passe par paires, et leur demander lesquels leur semblent les plus robustes. Ensuite, établir une corrélation entre leurs réponses et l'efficacité effective de ces derniers en utilisant *les méthodes les plus actuelles pour craquer les mots de passe*. Au final, sur 75 paires, les participants en ont correctement sélectionné 59. Il s'agit de 79%, soit en pratique un « B ».
Il est vrai que l'échantillon des 165 utilisateurs du CyLab est certainement un peu plus technique que d'autres utilisateurs : ils ont été recrutés en ligne via le système du Turc Mécanique d'Amazon. De plus, CyLab ne dit pas en substance que tous les utilisateurs atteindront ce score, mais seulement que certains peuvent y arriver. Enfin, pour conclure, ces scores ne sont pas alarmants.
Les personnes sondées par CyLab savaient que des mots de passe sont robustes lorsque :
• Les majuscules sont utilisées au milieu du mot, plutôt qu'au début.
• Des chiffres et des symboles sont situés au milieu du mot plutôt qu'à la fin.
• Des séquences de chiffres aléatoires sont insérées à la place d'autres plus évidentes, telles que l'année en cours par exemple.
• Des noms sont ajoutés, différents des traditionnels prénoms et noms.
• Des noms faisant parties de la vie privée ne sont pas utilisés, tels que les prénoms de vos enfants.
• Des mots faisant référence de manière évidente au site ou au compte que vous êtes en train de protéger ne sont pas utilisés.
Bien sûr, il en reste 21% qui n'ont pas réussi à faire la distinction. Cela laisse en effet de belles opportunités **aux cybercriminels pour craquer vos mots de passe**. Quelles ont donc été les plus grosses erreurs commises ? :
1. **Les participants ont ajouté des chiffres à leurs mots de passe, en plus des lettres, en pensant les renforcer**. Dommage ! Les hackers savent bien que les internautes très souvent rajoutent à la fin des chiffres, du coup « brooklynqy » est plus sécurisé que « brooklyn16 ».
2. **Les participants ont pensé que le fait de changer tout simplement des lettres en chiffres rendrait leurs mots de passe plus robuste.** Dommage ! Les craqueurs de mots de passe « exploitent de plus en plus la tendance des utilisateurs à faire des substitutions prévisibles », ainsi « punk4life » n'est pas plus sûr que « punkforlife ».
3. **Les participants ont surestimé la sécurité procurée par les séquences présentes au niveau de leur clavier.**Dommage ! Les hackers de nos jours recherchent très rapidement les séquences des claviers telles que « qwertyuiop », tout comme d'autres patterns classiques, et pas seulement à base de mots.
4. **Les participants ont mal appréhendé la popularité de certains mots ou de certaines phrases.** Selon le CyLab, par exemple, les utilisateurs ont pensé que « ieatkale88 » et « iloveyou88 » étaient équivalent d'un point de vue sécurité. Pas vraiment : les craqueurs de mots de passe ont besoin de plus d'un milliard de tentatives en plus pour en venir à bout de « ilovekale ». Il est plus sûr de choisir un mot isolé rare plutôt qu'une phrase intégrant « iloveyou » or « ilove ». Les mots de passe utilisant le mot « love » sont incroyablement répandus …ce qui est plutôt une bonne intention si vous n'êtes pas responsable de la cybersécurité d'un site.
Qu'est ce qui pourrait aider les utilisateurs pour éviter les mauvaises stratégies de choix des mots de passe ? Selon l'auteur de l'étude :
Une méthode qui semble être très efficace pour assister les utilisateurs dans l'évaluation de leurs mot de passe, vis-à-vis des pratiques courantes, est de leur fournir des feedbacks ciblés et explicites pendant la phase de création. Les calculateurs actuels de la force d'un mot de passe indiquent simplement aux utilisateurs si un mot de passe est faible ou fort, mais ne mentionne pas les raisons.
Les futurs travaux dans ce domaine pourraient s'inspirer d'une récente étude qui montrait la possibilité pour les utilisateurs de finir automatiquement le mot de passe partiel qu'ils viennent de taper … et pourrait également se baser sur une autre étude utilisant des arguments de motivation ou encore la pression de collègues pour inciter les utilisateurs à créer des mots de passe plus robustes.
Article original de Sophos France

Réagissez à cet article

Original de l’article mis en page : Robustesse des mots de passes : techniques et astuces

---

La double authentification de Google contournée par des hackers

La double authentification de Google contournée par des hackers

---

Alors que la double authentification semblait être la meilleure solution pour protéger les données personnelles des internautes, voilà que celle de Google a réussi à être contournée par des pirates. Autrement dit, les spécialistes de la sécurité vont encore devoir se creuser la tête pour trouver encore mieux !

La double authentification plombée par des pirates ?

Puisque la double identification implique qu'un utilisateur saisisse un mot de passe puis qu'il confirme son identité en saisissant un code préalablement reçu par SMS afin de pouvoir accéder à ses comptes, elle semblait être une solution fiable pour bien protéger les données des internautes.

Mais ça, c'était avant puisque des pirates ont réussi à contourner la double authentification de Google pour accéder aux comptes d'utilisateurs tiers.

Pour ce faire, les hackers ont mis en place une méthode plutôt astucieuse. En effet, s'ils disposent de l'adresse mail et du mot de passe, ils se font passer pour la firme de Mountain View, expliquent qu'une activité suspecte a été repérée et invitent l'utilisateur à renvoyer le code de sécurité qui leur a été envoyé.

Sans le savoir, les utilisateurs fournissent alors la clé de l'ultime protection aux pirates qui ont désormais le temps de commettre tous les actes malveillants qui désirent.

Une porte d'entrée vers les terminaux mobiles des utilisateurs ?

En s'offrant un accès aux comptes de messagerie des internautes, les pirates s'offrent une vraie porte d'entrée vers les terminaux mobiles de leurs propriétaires.

En effet, s'ils contrôlent le compte mail de leurs victimes, ils pourront facilement envoyer des mails sur Gmail incluant des pièces jointes frauduleuses qui peuvent être des applications malveillantes. Si le mail est ouvert depuis le mobile, le terminal sera alors automatiquement infecté.

Autrement dit, le hacker pourra avoir un accès complet à l'ensemble des données qu'il contient.

Incontestablement, la double authentification a donc ses limites…

Article original de Jérôme DAJOUX

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 : La double authentification de Google contournée par des hackers

---

Alerte nouveau ransomware : Le Javascript RAA est diffusé par spams

Alerte nouveau ransomware : Le Javascript RAA est diffusé par spams

---

Le ransomware RAA se propage à grande vitesse en Russie par le biais de campagnes de spams. Il prend la forme d'une pièce jointe en Javascript.

RAA, un ransomware entièrement écrit en Javascript

Si la plupart des logiciels malveillants qui ciblent des machines Windows est écrite en C++, voilà que RAA surprend puisque lui est intégralement écrit en Javascript, un langage destiné principalement à être interprété par les navigateurs web.

Pour les cybercriminels, le choix de ce langage n'est pas dû au hasard étant donné qu'ils tentent d'infecter les machines à distance via la diffusion de spams. Toutefois, tout utilisateur doit normalement agir avec méfiance avec les pièces jointes, d'autant plus si celles-ci sont dans un format Javascript. En effet, ce format doit inciter les utilisateurs à mettre le mail dans leur corbeille et surtout à ne pas ouvrir la pièce jointe.

Si tel est le cas, RAA peut faire des ravages puisqu'il est conçu pour chiffrer les documents disposant des extensions .doc, .xls, .rtf, .pdf, .dbf, .jpg, .dwg, .cdr, .psd, .cd, .mdb, .png, .lcd, .zip, .rar et .csv comme le révèlent nos confrères du Monde Informatique.

Autant dire donc que le téléchargement de la pièce jointe n'est pas sans conséquences.

Pas de vaccin disponible pour déchiffrer les contenus

S'il existe parfois des vaccins contre les ransomwares, RAA n'a pas encore le sien si bien qu'une fois vos fichiers chiffrés, vous n'aurez aucune autre alternative que payer la rançon si vous voulez débloquer de nouveau l'accès à vos documents.

Pour l'heure, ce rançongiciel se propage principalement en Russie puisqu'il semble que c'est depuis ce pays qu'opèrent les cybercriminels. Toutefois, il y a fort à parier que la diffusion de RAA va s'étendre dans les prochains mois et qu'une version « internationale » du rançongiciel sera développée par ces spécialistes du genre.

Article original de Fabrice Dupuis

Réagissez à cet article

Original de l’article mis en page : RAA : un nouveau ransomware diffusé par spams

---

Pourquoi vous ne devriez jamais publier de photos de vos jeunes enfants sur Facebook

Pourquoi vous ne devriez jamais publier de photos de vos jeunes enfants sur Facebook

---

Atlantico : Poster une photo de son enfant sur Facebook peut-il lui porter préjudice ? Si oui, quand ? Et pourquoi ?

Publier une photo de ses enfants sur Facebook – qui est de loin le leader des réseaux sociaux dans le monde – est un acte compréhensible mais qui fait surtout plaisir sur le moment aux parents. Les parents façonnent l'identité numérique de leurs enfants à l'insu de leur plein gré alors même que le droit à l'oubli n'existe pas sur Internet. Plus tard, certaines traces numériques (photos ou vidéos postées avec les commentaires et tags associés) peuvent être utilisées contre eux surtout si les paramétrages de confidentialités sont mal utilisés.

Et même en postant une photo accessible aux seuls amis, celle-ci peut ensuite être partagée plus largement. En outre les personnes qui vont réagir à la photo permettent de révéler l'écosystème relationnel de la personne. Il est facile d'établir des corrélations entre les personnes. Et en fonction du profil des personnes réagissant de déterminer quel est le profil potentiel de l'enfant sur la photo. Pour les préjudices, on pense avant tout à l'attitude d'un recruteur mais ce peut être aussi des amis potentiels de l'enfant qui le jugeront avec un autre regard. Déjà on google une personne avant de la rencontrer ce qui induit un prisme dans la première rencontre. Le préjudice peut intervenir à des périodes charnières de la vie : adolescence où l'individu se construit et est sensible au regard des autres, entrée dans la vie active, rencontre amoureuse, etc.

Comment fonctionne le système de tag ? Quelle est sa fonction ? Pourquoi l'utilise-t-on ?

Il s'agit d'un système mis en place par Facebook qui permet à un utilisateur de Facebook d'indiquer qu'une personne figure sur une photo. En quelque sorte, un traitement manuel du facebooknaute lui-même vient en complément de l'algorithme mis en place par Facebook pour collecter des données personnelles (en l'occurrence les photos des visages des personnes) de nature à faire grandir la base d'information relative à une personne. Facebook peut avec l'expérience lui-même déterminer les personnes reconnues sur les photos, ce qui est parfois bluffant. Facebook peut ensuite, en fonction des références à d'autres posts, déterminer le cercle probable de personnes autour de celle qui a été taguée. Ceci lui permet de faire des suggestions (par exemple amis que l'on pourrait connaître, voire produits ou services que l'on est susceptible d'aimer car les goûts de ses amis sont souvent plus proches des siens que ceux d'inconnus) avec des taux de retour plus pertinents.

L'objectif de Facebook est d'exploiter le *big data* constitué par les photos et leurs tags pour sans cesse améliorer les résultats pour les marques partenaires et qui paient ses services. Par ailleurs, les algorithmes qui permettent de reconnaître les visages et les techniques de bio-identification ne sont qu'à leur début. Demain, à partir d'une simple photo, il sera, avec des outils idoines, possible de dresser le portrait robot d'une personne en allant fouiller sur l'ensemble de la webosphère (pas seulement sur Facebook mais sur l'ensemble des réseaux sociaux et des sites) pour collecter les numéros de téléphone, les adresses mails et d'autres détails personnels associés. Ceci peut présenter des opportunités réelles pour mieux connaître rapidement une personne, mais présente des risques. Des garde-fous et une éthique sont à construire pour éviter que le numérique ne soit un facteur d'exclusion ou un moyen d'ostraciser les internautes. Alors que les États-Unis sont dans le mécanisme d'*opt-out* (utilisation *a priori* des données personnelles sans autorisation préalable), l'Europe préfère l'*opt-in* qui constitue un principe de précaution quant à l'exploitation des données personnelles. Mais force est de constater que les outils majoritairement utilisés en Europe sont Américains et que nous sommes GAFA-dépendant *(Ndlr : GAFA = Google, Apple, Facebook, Amazon)* et qu'en contrepartie de la gratuité d'utilisation d'un service, nous fournissons et souvent avec beaucoup de zèle des données personnelles que ces outils utilisent à la fois avec un traitement automatique et un traitement humain qui le perfectionne comme celui des tags.

Article original de David Fayon Lire la suite…

Réagissez à cet article

Original de l’article mis en page : Pourquoi vous ne devriez jamais publier de photos de vos jeunes enfants sur Facebook | Atlantico.fr

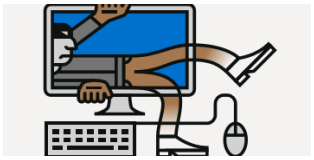
---

77 % des entreprises totalement impuissantes face aux cyberattaques

77 % des entreprises totalement impuissantes face aux 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….

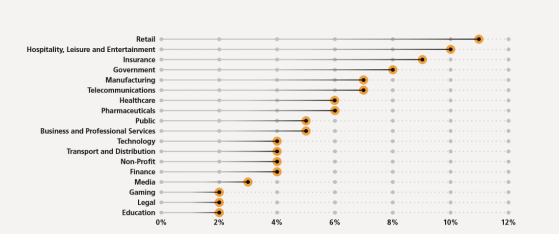


Le GTIR (« Global Threat Intelligence Report ») analyse une énorme masse de données issues de 24 centres d'opérations de sécurité (SOC), sept centres R&D, 3 500 milliards de logs et 6,2 milliards d'attaques. Ces résultats sont donc particulièrement intéressants pour suivre l'état des menaces dans le 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.

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

---

Trois étapes pour mieux protéger les données en mobilité

Trois étapes pour mieux protéger les données en mobilité

Pour mieux protéger les données en mobilités, la DSI doit connaître les spécificités de chaque système d'exploitation mobile, déterminer quels terminaux accepter dans l'environnement de travail, et comprendre les capacités natives de protection des données.

Protéger les données d'entreprise contre la perte et le vol est l'une des principales priorités. Les brèches de données sont douloureuses et onéreuses. Et leurs effets peuvent être étendus, entre atteinte à la marque et sanctions réglementaires.
Heureusement, l'industrie du mobile a progressé dans la prise en compte des préoccupations des entreprises en matière de sécurité, tout particulièrement pour ce qui est de la protection des données en mobilité. Par le passé, les smartphones manquaient de capacités même basiques de chiffrement des données. Mais ils ont depuis évolué en plateformes dotées de capacités de sandboxing avancées.
Parallèlement, les suites de gestion de la mobilité d'entreprise (EMM) ont amélioré le contrôle et la surveillance via le réseau, en OTA (over-the-air), ce qui donne aux DSI une pléthore d'outils de protections des données en mobilité, qu'elles transitent sur le réseau de l'entreprise ou via un point d'accès à Internet public.

Tout part du système d'exploitation mobile
La plupart des postes de travail des entreprises fonctionnent sous Windows, voire sous OS X. Cela offre aux DSI un environnement relativement cohérent et maîtrisé. Mais les terminaux mobiles exécutent des systèmes d'exploitation plus variés et évoluant plus rapidement, susceptibles d'ailleurs de changer d'un constructeur à l'autre, sinon d'un modèle à l'autre. Lorsque les utilisateurs amènent leurs propres appareils et applications mobiles, ils accroissent encore la diversité de l'environnement, et contournent les processus de la DSI. Dès lors, celle-ci ne peut pas compter sur la standardisation et le verrouillage des terminaux et de leurs applications pour sécuriser les données en mobilité.
Sécuriser les données en mobilité nécessite de comprendre ce que chaque système d'exploitation mobile peut ou ne peut pas faire. Les administrateurs peuvent alors pleinement tirer parti des technologies, applications et réglages supportés. Par exemple, la plupart des systèmes d'exploitation mobiles actuels supportent l'isolation native des applications – ou sandboxing –, et intègrent des capacités avancées de sécurisation du noyau.
Le support du chiffrement natif à l'échelle du terminal et de l'effacement à distance, varie toutefois. Pour cela, il est fréquent que les DSI choisissent une approche de sécurisation des données en mobilité en deux temps : elles commencent par établir et faire respecter des critères d'acceptation minimum, puis comblent les limitations des plateformes avec des outils tiers.

Déterminer quels terminaux accepter
Pour établir les critères d'acceptation des terminaux, il convient d'examiner l'architecture de sécurité de chaque plateforme pour étudier à quel point les applications utilisateur, opérateur et constructeur sont isolées les unes des autres, et du noyau du système d'exploitation.

Il convient également de savoir si les applications peuvent lire ou modifier les données d'autres applications et services en dehors du bac à sable – des fichiers partagés ou des messages, par exemple. L'examen doit également couvrir les permissions qui sont accordées – par défaut ou explicitement – aux applications, ainsi que le degré de contrôle que la DSI peut exercer pour détecter et bloquer des applications potentiellement dangereuses.
Comme leurs homologues pour le poste de travail, les systèmes d'exploitation mobiles souffrent de vulnérabilités susceptibles de mettre en danger les données. La question des mises à jour des applications et du système d'exploitation, leur délai de mise à disposition, s'avère particulièrement problématique dans un écosystème fragmenté.
La même considération s'applique à la provenance des applications mobiles. Le contrôle exercé par Apple s'avère efficace pour limiter la diffusion de logiciels malveillants pour iOS – sans toutefois l'empêcher complètement. C'est un facteur à prendre en compte dans l'établissement des critères d'acceptabilité. Par exemple, certaines entreprises interdisent les terminaux Android, ou n'en autorisent que certaines versions.
Pour beaucoup, les critères de base non négociables touchent à une version d'OS mobile minimum, le support matériel du chiffrement complet du terminal, des interfaces d'administration OTA, la possibilité d'imposer l'utilisation d'un mot de passe robuste, celle d'effacer le terminal à distance, d'enregistrer les activités, de détecter les opérations de jailbreak ou de rootage, voire de gérer dans une certaine mesure les applications installées. Les terminaux ne répondant pas à ces critères de base sont susceptibles d'être interdits d'accès aux réseaux et services de l'entreprise, ou bien autorisés dans une mesure limitée qui ne mette pas en danger les données.

Protection native des données : une base
Les smartphones et les tablettes sont appelés à être perdus, avec les données métiers qu'ils transportent. Le chiffrement complet du terminal peut souvent empêcher un appareil perdu d'être à l'origine d'une brèche de données.
Mais un tel chiffrement peut s'avérer d'une portée limitée sur certaines plateformes. Par exemple, l'effacement à distance est supporté par tous, mais son efficacité varie. Sur les appareils Apple et BlackBerry, les clés de chiffrement sont supprimées, ce qui rend les données chiffrées irrécupérables. Sur les anciens appareils Android sans chiffrement matériel, l'effacement n'est qu'une réinitialisation en conditions de sortie d'usine. Ce qui est susceptible de laisser les données exposées en cas de perte, de vol ou de revente du terminal.
De la même manière, un système de fichiers chiffré ne peut pas pleinement sécuriser les données sur un terminal compromis. Il ne peut pas non plus empêcher les utilisateurs de déplacer des données sur des emplacements non chiffrés. Lorsque des applications professionnelles et personnelles coexistent sur un même appareil, il y a plus de chances pour qu'une application malicieuse ou trop curieuse compromette des données d'entreprise présente sur le même système de fichiers. A moins que la DSI ne prenne des mesures préventives, un employé autorisé à accéder à un terminal chiffré peut aisément laisser fuir des données par e-mail ou transfert vers un service de stockage en mode Cloud.
La protection native des données en mobilité apparaît en fait comme un point de départ essentiel, mais pas suffisant. Pour profiter pleinement de ce que peuvent offrir les systèmes d'exploitation mobiles modernes, il convient d'utiliser une solution de gestion de la mobilité d'entreprise (EMM) pour enrôler les appareils acceptables et provisionner leurs réglages, en commençant par des points tels que la robustesse du mot de passe, le recours au lecteur d'empreintes digitales, ou encore le nombre de tentatives autorisées. Une authentification robuste est critique parce que des codes PIN faciles à deviner peuvent neutraliser un chiffrement fort. Il convient aussi d'activer l'effacement à distance et de recueillir le consentement explicite de l'utilisateur durant l'enrôlement à l'invocation de cette fonctionnalité en cas de dernier recours, et dans des conditions très précises.
Article original de Lisa Phife

Réagissez à cet article

Original de l’article mis en page : Trois étapes pour mieux protéger les données en mobilité

Sensibilisation au Phishing

Sensibilisation au Phishing

Vous feriez confiance à cet homme ? Sur Internet aussi, soyez vigilants: il arrive que des acheteurs ou vendeurs malhonnêtes essaient de vous arnaquer. Découvrez les bons réflexes sécurité avec PayPal. Acheter et vendre en ligne est simple et sécurisé avec PayPal, 7 millions de Français nous utilisent déjà.

Campagne Paypal France 2016

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

Sensibilisation aux Arnaques à la Loterie

Sensibilisation aux Arnaques à la Loterie

Vous feriez confiance à cet homme ? Sur Internet aussi, soyez vigilants: il arrive que des acheteurs ou vendeurs malhonnêtes essaient de vous arnaquer. Découvrez les bons réflexes sécurité avec PayPal. Acheter et vendre en ligne est simple et sécurisé avec PayPal, 7 millions de Français nous utilisent déjà.

Campagne Paypal France 2016

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

Les pays arabes mutualisent leurs forces pour faire face à la cybercriminalité

Les pays arabes mutualisent leurs forces pour faire face à la cybercriminalité

Un atelier sur la sécurité informatique réunit les pays arabes depuis lundi dernier à Tunis. La rencontre qui devrait être clôturée ce vendredi vise à évaluer la prédisposition des Etats concernés à faire face aux attaques informatiques d'après le président du Centre arabe régional de la cybersécurité cité par le webmanagercenter.com.

La rencontre qui devrait être clôturée vendredi dernier vise à évaluer la prédisposition des Etats concernés à faire face aux attaques informatiques d'après le président du Centre arabe régional de la cybersécurité.

(CIO Mag) – Un atelier sur la sécurité informatique réunit les pays arabes depuis lundi dernier à Tunis. La rencontre qui devrait être clôturée ce vendredi vise à évaluer la prédisposition des Etats concernés à faire face aux attaques informatiques d'après le président du Centre arabe régional de la cybersécurité cité par le webmanagercenter.com.

Le directeur général de l'agence tunisienne de sécurité informatique, lui, indique que Tunis a pris très tôt des initiatives pour lutter contre la cybercriminalité. Mohamed Naoufel Frikha, repris par nos confrères, rappelle qu'un travail important a été réalisé depuis 1999 avec la création du premier centre en Afrique, le troisième dans le monde arabe.

Le rendez-vous de Tunis entend amener les pays arabes à créer des centres de cyber-alerte. Leur nombre est très insuffisant dans l'espace arabophone puisque seuls dix pays en disposent. Des représentants de treize Etats prennent part aux échanges.

Article de Ousmane Gueye

Réagissez à cet article

Original de l'article mis en page : Cybercriminalité: les pays

arabes mutualisent leurs forces pour faire face au phénomène | CIO MAG

Denis JACOPINI présent à Abidjan pour le IT Forum 2016 les 7 et 8 juin 2016

	**Denis JACOPINI présent à Abidjan pour le IT Forum 2016 les 7 et 8 juin 2016**

Denis JACOPIN sera présent à l'IT Forum 2016 les 7 et 8 juin prochains, invité auprès des plus grands Experts en Cybersécurité. La 8ème édition de ce Forum aura pour thème Protection des Données, Gestion de l'identité numérique, Protection des transactions à l'ère du numérique : Risques, Enjeux et Stratégies de mise en oeuvre.

2 jours de networking organisés par CIO Mag et le Club DSI de côte d'Ivoire sous le parrainage de

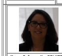
Bruno Nabagné KONE,
Ministre de l'Economie numérique et de la Poste – Côte d'Ivoire

Venez discuter, échanger et dialoguer avec des donneurs d'ordre, rencontrez-les en rendez-vous :

Freddy TCHALA, CEO MTN CI

Euloge SORO-KIPEYA, CEO ANSUT

Nongolougo SORO, CEO SNDI



Mme. Saloua K. BELKZIZ, Présidente de la Fédération APEBI – Maroc

Jean Kacou DIAGOU, Président du CGECI – Côte d'Ivoire

Une vingtaine d'experts partageant leurs retours d'expériences et les meilleures pratiques

Cdt Guelpétchin Ouattara, Directeur de l'Informatique et des Traces Technologiques – Côte d'Ivoire

Yann PILPRE, Expert Sécurité, CEO YPSI

Denis JACOPINI, Expert en Cybercriminalité et Protection des données personnelles

Ange DIAGOU, CEO NSIA Technologies

Frédéric MASSE, Vice-Président SAP

Alain DOLIUM, Expert Transformation numérique PDG SMS Group

vous souhaitez y participer ?
Entrée gratuite mais inscription obligatoire : Cliquez ici

PROGRAMME

Heures	Activités	Intervenants
Journée du Mardi 07 juin 2016		
08h00 – 09h00	Accueil et installation des invités	*Comité d'organisation*
09h00 – 09h05	Mot de Bienvenue	· **M. Mamadou NAON**, Président CDSI
09h05 – 09h15	Mot du Sponsor Officiel	· **M. Freddy TCHALA**, DG MTN
09h15 – 09h25	Mots des sponsors Leaders	· **M. Nongologou SORO**, DG SNDI · **M. Ange DIAGOU**, DG NSIA TECHNOLOGIES
09h25 – 09h35	Présentation du contenu de l'IT FORUM 2016	· **M. Mohamadou DIALLO**, Directeur de Publication CIO MAG
09h35 – 09h40	Mot du Pays Invité (Maroc)	· **Mme Saloua K. BELKZIZ**, Présidente de la Fédération APEBI
09h40 – 09h50	Mot du Président de l'IT FORUM 2016	· **M. Jean Kacou DIAGOU**, Président CGECI
09h50 – 10h05	Discours d'ouverture des travaux	· **M. Bruno KONE**, Ministre de la Poste et de l'Economie Numérique
10h05 – 10h20	REMISE DE TROPHEES	
10h20 – 10h45	Coupure de ruban – Visite des stands – Cocktail	
10h45 – 10h50	**TIRAGE TOMBOLA**	
10h50 – 11h05	Les principales tendances IT en Afrique occidentale et centrale	· **M. Mohamed ZIZI**, Directeur régional pour l'Afrique Francophone IDC
11h05 – 12h00	Plénière/Panel 01 **La protection des données, une nécessité pour le respect des libertés fondamentales**	· **Cdt Guelpétchin Ouattara**, Directeur de l'Informatique et des Traces Technologiques (DITT Côte d'Ivoire) · ***Ibrahima DIAGNE***, *Administrateur Délégué Gaindé 2000* ***Modérateur : Dr GUIBESSONGUI N'Datien Sévérin***, *ICT CONSULTING* ***Rapporteur : M. Auger SEOULOU***, *DSI Ministère de la Justice – Côte d'Ivoire*
12h00 – 12h05	**TIRAGE TOMBOLA**	
12h05 – 12H35	Atelier 01 **Optimisation des coûts en relation avec votre business model**	· **M. Christophe Thénégal**, Associé PWC
12h35 – 12h40	**TIRAGE TOMBOLA**	
12h40 – 14h20	Pause déjeuner	
14h30 – 14h35	**TIRAGE TOMBOLA**	
14h35 – 15h20	Plénière/Panel 02 **Fluidité des transactions : Comment mieux réglementer le secteur en vue de développer l'adoption de la monnaie électronique**	· ***M. Frédéric MASSE***, *Vice-Président SAP* · ***M. Francis Dufay***, *Directeur Général de JUMIA Côte d'Ivoire* · ***Représentant MTN MFS*** ***Modérateur : M. Lacina KONE***, *Conseiller NTIC –Président de la République* ***Rapporteur : M. Eric YAO***, *DSI CNCE*
15h20 – 15h30	**FIGHT 1 : Logiciel open source VS Logiciel Propriétaire (compétions des solutions IT)**	
15h30 – 15h35	**TIRAGE TOMBOLA**	
15h35 – 15h50	Atelier 01	· *SAP*
15h50 – 15h55	**TIRAGE TOMBOLA**	
15h55 – 16h10	Plénière **Méthode, technique et outils des transactions électroniques et leur sécurité**	· **M. Yann PILPRE**, Expert Sécurité, DG de YPSI
16h10 – 16h20	**FIGHT 2 : Approche de sécurisation de données à caractère personnel et des transactions électroniques : méthode et outils (compétition des approches IT)**	
16h20 – 17h05	Panel 03 **Données dans le Cloud public/privé: Comment et avec qui assurer la sécurité ?**	· ***M. Nongolougo SORO***, *DG de la SNDI* · ***M. Euloge SORO***, *DG de l'ANSUT* · ***AUSIM*** *(Maroc)* · ***M. Brice DEMONGE***, *Directeur de développement secteur public – GFI Informatique* · ***Camille AMEYAO / MTN Business*** · ***Denis JACOPINI***, *Expert Informatique assermenté spécialisé en Cybercriminalité et en Protection des données personnelles* · ***Modérateur : Conrad GBAGUIDI***, *DG MGT Conseils* ***Rapporteur : M. Aboadjé KOUADIO***, *DSI SNDI*
17h05– 17h10	**TIRAGE TOMBOLA**	
Fin de la première journée		

Journée du Mercredi 08 juin 2015		
08h30 – 09h15	Accueil et installation des invités	Comité d'organisation
09h15 – 09h30	Rappel des travaux de la journée du 07 juin	Club DSI
09h30 – 09h35	**TIRAGE TOMBOLA**	
09h35– 10h20	Panel 04 **Les entreprises et administrations ivoiriennes face à la cybersécurité** **–**	· **M. Freddy TCHALA**, DG MTN Côte d'Ivoire · ***M. Nongolougo SORO***, *DG de la SNDI* · ***M.Ange DIAGOU***, *DG NSIA Tech* · ***M. Bilé DIEMELEOU***, *DG ARTCI* ***Modérateur : Patrick M'BENGUE, Président GOTIC***
10h20 – 10h25	**TIRAGE TOMBOLA**	
10h25 –10h40		
10h40 – 10h45	**TIRAGE TOMBOLA**	
10h45– 11h00	Atelier 04 **Les services managés: garants d'une transformation numérique efficace, rentable et sécurisée**	*NSIA TECHNOLOGIES*
11h00 – 11h15	Atelier 05	*FEITAN France*
11h15 – 11h20	**Cloud privé VS Cloud Public (Compétition des technologies Cloud)**	
11h20 – 12h15	**Comment sécuriser ses infrastructures et plateformes de services pour la transformation numérique?**	· ***Représentant de l'ARTCI*** · ***Denis JACOPINI***, *Expert Informatique assermenté spécialisé en Cybercriminalité et en Protection des données personnelles* · ***Jean-François TESSERAUD***, *Chief Information Security Officer – Systemis* · ***Yves MIEZAN EZO, Conseil***, *Stratégie & Formation Open Source* · ***Modérateur : Ludovic MORINIERE***, *International Development BearinPoint*
12h15 – 12h20	**TIRAGE TOMBOLA**	
12h30 – 14h20	Pause déjeuner	
14h30 – 14h35	**TIRAGE TOMBOLA**	
14h35 – 14h50	Atelier 06	VEONE
14h50 – 15h00	**FIGHT 04**	
15h00 – 15h15	Atelier 07 **Pourquoi et Comment protéger efficacement vos données dans la transformation numérique ?**	· ***Marcial MONTHE***, *Ingénieur Avant-Vente, Responsable de la Business Unit Veritas –* ***SOCITECH***
15h15 – 15h20	**TIRAGE TOMBOLA**	
15h20 – 15h35		
15h35 – 16h40	**TIRAGE TOMBOLA**	
15h40 – 15h55	Récompense des Sponsors et Partenaires	***Club DSI***
15h55– 16h20	Restitution des travaux	
Fin de la 2ème journée		
Soirée de Gala		

Merci à l'auteur de cet article

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

Source : *Jour J-16*