Les entreprises ne sont pas prêtes pour la nouvelle législation européenne sur la protection des données | Denis JACOPINI

Les entreprises ne sont pas prêtes pour la nouvelle législation européenne sur la protection des données

Varonis a mené une enquête en mars auprès des informaticiens professionnels participant au CeBIT, le plus grand salon IT d'Allemagne, afin de recueillir leur opinion sur la nouvelle réglementation régissant la protection des données qui doit entrer en vigueur cette année ou l'année prochaine. Le constat est sans appel : les entreprises ne sont pas prêtes pour la nouvelle législation européenne sur la protection des données. Les professionnels interrogés par Varonis ne pensent pas que leurs entreprises soient en mesure de respecter les délais imposés par l'UE pour la notification des violations de données.

Il ressort de cette enquête que 80 % des personnes interrogées pensent qu'une banque sera très probablement la première entreprise à être frappée par l'amende maximale de 100 millions d'euros pour non-respect de la réglementation européenne sur la protection des données. À la question concernant le pays le plus probable de cette banque, les répondants indiquent l'Allemagne (30 %), les États-Unis (28 %) et 22 % mentionnent un autre pays européen. 48 % seulement des personnes interrogées pensent que leur entreprise pourrait signaler une violation dans le délai obligatoire de 72 heures.
Seuls 31 % disposent d'un plan leur permettant de se conformer à la nouvelle législation et seulement un tiers des personnes enquêtées a mis en place les processus et la technologie nécessaires pour empêcher leur entreprise de se voir infliger une amende importante dans le cadre de cette loi. 71 % des répondants sont incapables de dire ce que les entreprises doivent faire pour se conformer à la nouvelle réglementation.
Seuls 22 % des répondants savaient que l'amende maximale prévue par la nouvelle législation est de 100 millions d'euros, 41 % pensaient qu'elle ne serait que de 10 millions d'euros et 32 % l'estimaient à 1 million d'euros, avec un nombre réduit de personnes interrogées croyant qu'elle pouvait s'élever à un milliard d'euros. Un tiers a déclaré que la réglementation européenne sur la protection des données entrera en vigueur en 2015, 28 % ont indiqué que tel serait le cas en 2016, 7 % estiment que la loi ne verra jamais le jour et 32 % des personnes interrogées ont dit ne pas savoir quand la loi entrerait en vigueur.
« Nous pouvons attendre une refonte majeure de la loi européenne sur la protection des données au cours des prochains 12 à 24 mois », déclare David Gibson, vice-président du marketing de Varonis. « Les amendes devraient s'élever à 2 % du revenu annuel avec un plafond de 100 millions d'euros ou de dollars pour la non-protection des données personnelles des citoyens européens. Il pourrait également y avoir un nombre important de plaintes individuelles en plus des amendes et les sommes mises en jeu pourraient donc représenter des coûts substantiels, même pour les grandes entreprises. La nouvelle loi marquera aussi le passage d'un environnement autoréglementé à un régime d'application obligatoire qui aura une incidence sur toute entreprise stockant des informations d'identification personnelle concernant les citoyens européens (y compris sur les sociétés américaines menant des activités dans l'UE). Les entreprises doivent être préparées à protéger les données de leurs clients et prouver qu'elles le font avec le soin approprié, rendre compte de toute violation et supprimer les données à la demande des citoyens de l'UE. »
« Compte tenu de la vaste portée de la nouvelle réglementation et de l'importance accrue des amendes, cette enquête révèle des inquiétudes très importantes quant aux efforts que les entreprises sont prêtes à fournir pour se conformer aux conditions de la réglementation et gérer les scénarios de violation de données », indique Mark Deem, partenaire de Cooley LLP au Royaume-Uni. « En fait, l'échelle des amendes potentielles sera plus proche de celles infligées pour corruption ou violation antitrust, ou dans le secteur des services financiers. La conformité en matière de protection des données sera tout aussi importante que la conformité aux réglementations de la FCA. Même si la législation n'entre pas en vigueur avant 2017, un travail considérable doit être accompli par ceux qui souhaitent offrir des biens et des services aux habitants de l'UE et s'assurer qu'ils se trouvent dans la meilleure situation possible pour respecter la loi. »
Varonis propose 7 conseils pour garantir la conformité des données non structurées et permettre aux entreprises de se préparer à la réglementation européenne sur la protection des données :

1. Minimiser la collecte des données : la proposition de loi de l'UE comporte de fortes exigences en ce qui concerne la limitation des données recueillies auprès des consommateurs.

2. Favoriser le signalement des violations de données : la notification des atteintes à la protection des données constitue une nouvelle exigence que les entreprises européennes devront respecter.

3. Conserver les données avec attention : les règles de minimisation de la nouvelle loi concernent non seulement l'étendue des données collectées, mais aussi leur durée de rétention. En d'autres termes, une entreprise ne doit pas stocker les données plus longtemps que nécessaire aux fins prévues.

4. Nouvelle définition des identifiants personnels : l'UE a étendu la définition des identifiants personnels et ce changement s'avère important parce que les lois de l'UE portent sur la protection de ces identifiants.

5. Employez un langage clair : il faudra à une entreprise le consentement préalable et explicite des consommateurs lors de la collecte des données.

6. Bouton d'effacement : le « droit d'effacement » signifie qu'en cas de retrait du consentement accordé par les consommateurs, les sociétés devront supprimer les données concernées.

7. Le Cloud computing n'échappe pas à cette nouvelle loi de l'UE, car celle-ci suit les données.

Méthodologie de l'enquête
Les 145 personnes interrogées constituent un échantillon représentatif des participants du plus grand salon informatique d'Allemagne qui a compté 221 000 visiteurs en mars 2015. Parmi les répondants, 16 % sont issus de banques allemandes, 3 % de banques américaines, 3 % de banques européennes, 45 % d'entreprises allemandes hors du secteur financier, 26 % d'entreprises européennes hors du secteur financier et 7 % d'entreprises américaines.

Guide du Cloud Computing et des Datacenters à l'attention des collectivités locales | Denis JACOPINI

Guide du Cloud Computing et des Datacenters à l'attention des collectivités locales

A l'attention des collectivités locales
Les concepts de Cloud Computing et de Datacenters suscitent un fort intérêt de la part des collectivités locales, mais soulèvent également de nombreuses questions.
La Direction Générale des Entreprises, la Caisse des Dépôts et le Commissariat Général à l'Egalité des territoires proposent un guide pratique pour orienter les collectivités locales dans leurs réflexions.
• Comment répondre aux nouveaux besoins et disposer rapidement de nouvelles ressources informatiques ?
• Comment gérer et administrer facilement les ressources nécessaires à l'ensemble des services ?
• Comment assurer la disponibilité en continu de ces services ?
• Comment garantir l'interopérabilité des plateformes et la pérennité des solutions technologiques ?
• Comment gérer les problématiques de confidentialité et de sécurité des données ?
• Comment maîtriser les coûts de construction et d'exploitation des solutions ?
• Quels changements ces solutions imposent-elles dans le fonctionnement des Dsi et des services numériques ?
• Comment contractualiser avec les fournisseurs de services et maîtriser la relation client – fournisseur ?
• Quelles sont les contraintes liées à la construction et à la maintenance d'un Datacenter ?
• Comment mesurer la rentabilité d'un Datacenter ?
• Quelle est la pérennité des investissements dans les Datacenters locaux ou Datacenters de proximité implantés sur le territoire ?
• Quelle stratégie adopter pour mutualiser les projets et conserver la maîtrise des coûts ?

Ce guide a ainsi pour mission d'apporter un éclairage sur les différents concepts et de proposer aux collectivités un ensemble de solutions et de moyens pour réussir leurs projets.

Il s'adresse à la fois aux élus locaux, aux responsables du développement économique des territoires, aux responsables informatiques, aux opérationnels au sein des collectivités, associations et structures de mutualisation , ainsi qu'à tous les acteurs publics et privés de ces écosystèmes.

Source : http://www.entreprises.gouv.fr/secteurs-professionnels/guide-du-cloud-computing-et-des-datacenters

Comment bien choisir ses mots de passe ?

Comment bien choisir ses mots de passe ?

Les mots de passe sont une protection incontournable pour sécuriser l'ordinateur et ses données ainsi que tous les accès aux services sur Internet. Mais encore faut-il en choisir un bon.Un bon mot de passe doit être difficile à deviner par une personne tierce et facile à retenir pour l'utilisateur.

Qu'est ce qu'un bon mot de passe ?

Un bon de passe est constitué d'au moins **12 caractères** dont :

• des lettres majuscules
• des lettres minuscules
• des chiffres
• des caractères spéciaux

Un mot de passe est d'autant plus faible qu'il est court. L'utilisation d'un alphabet réduit ou de mot issu du dictionnaire le rend très vulnérable.
Les mots du dictionnaire ne doivent pas être utilisés.
Aussi à proscrire, les mots en relation avec soi, qui seront facilement devinables : nom du chien, dates de naissances…
Réseaux sociaux, adresses mail, accès au banque en ligne, au Trésor public, factures en ligne.
Les accès sécurisés se sont multipliés sur internet.
Au risque de voir tous ses comptes faire l'objet d'utilisation frauduleuse, il est impératif de **ne pas utiliser le même mot de passe**pour des accès différents.
Alors, choisir un mot de passe pour chaque utilisation peut vite devenir un vrai casse-tête.

Comment choisir et retenir un bon mot de passe ?

Pour créer un bon mot de passe, il existe plusieurs méthodes :

La méthode phonétique

Cette méthode consiste à utiliser les sons de chaque syllabe pour créer une phrase facilement mémorisable.
Exemple : « j'ai acheté huit cd pour cent euros ce après-midi» donnera : ght8CD%E7am

La méthode des premières lettres

Utiliser les premières lettres d'une phrase en variant majuscules, minuscules et caractères spéciaux.
Exemple : « un tiens vaut mieux que deux tu l'auras » donnera : 1TvmQ2tl'@

Diversifier facilement les mots de passe

Opter pour une politique personnelle avec, par exemple, un préfixe pour chaque type d'activité. Comme BANQUE-MonMotDePassz pour la banque, IMP-MonMotDePasse pour les impôts. Quelque chose de très facile à mémoriser qui complexifie votre mot de passe et, surtout, vous permet de le diversifier.

Diminuer les imprudences

Pour finir, il est utile de rappeler de **ne pas stocker ses mots de passe à proximité de son ordinateur** si il est accessible par d'autres personnes. L'écriture sur le post-it déposé sous le clavier est à proscrire par exemple, de même que le stockage dans un fichier de la machine.
En règle général, les logiciels proposent de **retenir les mots de passe**, c'est très **tentant mais imprudent**. Si votre ordinateur fait l'objet d'un piratage ou d'une panne, les mots de passe seront accessibles par le pirate ou perdus.

Que faire en cas de piratage ?

Il est recommandé de préserver les traces liées à l'activité du compte.
Ces éléments seront nécessaires en cas de dépôt de plainte au commissariat de Police ou à la Gendarmerie.
Exemple
Compte email piraté
Vos contacts ont reçu des messages suspects envoyés de votre adresse.
Contactez-les pour qu'ils conservent ces messages.
Ils contiennent des informations précieuses pour l'enquêteur qui traitera votre dépôt de plainte.
Récupérez l'accès à votre compte afin de changer le mot de passe et re-sécurisez l'accès à votre compte.

Changer de mots de passe régulièrement

Cette dernière règle est contraignante mais assurera un niveau supérieur de sécurité pour vos activités sur Internet.
Un **bon mot de passe doit être renouvelé plusieurs fois par an** et toujours en utilisant les méthodes décrites ci-dessus.

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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 : Comment choisir ses mots de passe ? / Cybercrime / Dossiers / Actualités – Police nationale – Ministère de l’Intérieur

---

Pourquoi, malgré le danger connu, cliquons nous sur des e-mails d’expéditeurs inconnus ?

Pourquoi, malgré le danger connu, cliquons nous sur des e-mails d’expéditeurs inconnus ?

Selon une enquête de la FAU (University of Erlangen-Nuremberg), près de la moitié des utilisateurs cliqueraient sur des liens d'expéditeurs inconnus (environ 56% d'utilisateurs de boite mails et 40% d'utilisateurs de Facebook), tout en étant parfaitement conscient des risques de virus ou d'autres infections.
Le site d'information Français Pure Player Atlantico à interrogé à ce sujet Denis JACOPINI, Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles

Atlantico :
Pourquoi donc, selon vous, le font-ils malgré tout ? Qu'est-ce qui rend un mail d'un inconnu si attirant, quitte à nous faire baisser notre garde ?

Denis JACOPINI :
Ça-vous est très probablement déjà arrivé de recevoir un e-mail provenant d'un expéditeur anonyme ou inconnu.
Avez-vous résisté à cliquer pour en savoir plus ? Quels dangers se cachent derrière ces sollicitations inhabituelles ? Comment les pirates informatiques peuvent se servir de nos comportements incontrôlables ?

Aujourd'hui encore, on peut comparer le courrier électronique au courrier postal.
Cependant, si l'utilisation du courrier postal est en constante diminution (-22% entre 2009 et 2014), l'usage des messages électroniques par logiciel de messagerie ou par messagerie instantanée a lui par contre largement augmenté.
Parmi les messages reçus, il y a très probablement des réponses attendues, des informations souhaitées, des messages de personnes ou d'organismes connus nous envoyant une information ou souhaitant de nos nouvelles et quelques autres messages que nous recevons avec plaisir de personnes connues et puis il y a tout le reste, les messages non attendus, non désirés qui s'appellent des spams.
En 2015, malgré les filtres mis en place par les fournisseurs de systèmes de messagerie, il y avait tout de même encore un peu plus de 50% de messages non désirés.
Parmi ces pourriels (poubelle + e-mail) se cachent de nombreux message ayant des objectifs malveillant à votre égard. Les risques les plus répandus sont les incitations au téléchargement d'une pièce jointe, au clic sur un lien renvoyant vers un site Internet piégé ou vous proposer d'échanger dans le but de faire « copain copain » et ensuite vous arnaquer.

La solution : ne pas cliquer sur un e-mail ou un message provenant d'un inconnu, de la même manière qu'on apprend aux enfants de ne pas parler à un inconnu…Pourtant, des millions de personnes en France se font piéger chaque année. Pourquoi ?

A mon avis, les techniques d'Ingenierie sociale sont à la base de ces correspondances. L'ingénierie sociale est une pratique qu exploite les failles humaines et sociales. L'attaquant va utiliser de nombreuses techniques dans le but d'abuser de la confiance, de l'ignorance ou de la crédulité des personnes ciblées.
Imaginez, vous recevez un message ressemblant à ça :
« Objet : changements dans le document 01.08.16
Expéditeur : Prénom et Nom d'une personne inconnue
Bonjour,
Nous avons fait tous les changements necessaires dans le document.
Malheureusement, je ne comprends pas la cause pour la quelle vous ne recevez pas les fichier jointes.
J'ai essaye de remettre les fichier jointes dans le e-mail. »
…
Dans cet exemple, on ne connaît pas la personne, on ne connaît pas le contenu du document, mais la personne sous-entend un nouvel envoi qui peut laisser penser à une ultime tentative. Le document donne l'impression d'être important, le ton est professionnel, il n'y pas trop de faute d'orthographe… Difficile de résister au clic pour savoir ce qui se cache dans ce mystérieux document.

Un autre exemple d'e-mail ou similaire souvent reçu :
« Objet : Commande – CD2533
Expéditeur : Prénom et Nom d'une personne inconnue
Madame, Monsieur,
Nous vous remercions pour votre nouvelle « Commande – CD2533″.
Nous revenons vers vous au plus vite pour les delais
Meilleures salutations,
VEDISCOM SECURITE »

En fait, bien évidemment pour ce message aussi, la pièce jointe contient un virus et si le virus est récent et s'il est bien codé, il sera indétectable par tous les filtres chargés de la sécurité informatique de votre patrimoine immatériel.
Auriez-vous cliqué ? Auriez-vous fais partie des dizaines ou centaines de milliers de personnes qui auraient pu se faire piéger ?

Un autre exemple : Vous recevez sur facebook un message venant à première vue d'un inconnu mais l'expéditeur a un prénom que vous connaissez (par exemple Marie, le prénom le plus porté en France en 2016). Serait-ce la « Marie » dont vous ne connaissez pas le nom de famille, rencontrée par hasard lors d'un forum ou d'une soirée qui vous aurait retrouvé sur Facebook ?
Dans le doute vous l'acceptez comme amie pour en savoir plus et engager pourquoi pas la conversation…
C'est un autre moyen utilisé par les pirates informatiques pour rentrer dans votre cercle d'amis et probablement tenter des actes illicites que je ne détaillerai pas ici.

Vous rappelez-vous avoir accepté une demande de mise en contact provenant d'un inconnu sur Facebook ? Peut-être que vous ne connaissiez pas les risques, mais qu'est-ce qui vous a poussé à répondre à un inconnu ? La politesse ? La curiosité ?

A mon avis, le principal levier utilisé pour pousser les gens à cliquer sur les emails pour en voir l'objet, cliquer sur les pièces jointes pour en voir le contenu ou cliquer sur les liens pour découvrir la suite, est une des nombreuses failles humaine : la curiosité.

Cette curiosité peut nous faire faire des choses complètement irresponsables, car on connait les dangers des pièces jointes ou des liens dans les e-mails. Malgré cela, si notre curiosité est éveillée, il sera difficile de résister au clic censé la satisfaire.

Il est clair que la curiosité positive est nécessaire, mais dans notre monde numérique où les escrocs et pirates oeuvrent en masse le plus souvent en toute discrétion et en toute impunité, la pollution des moyens de communication numériques grand public est telle que le niveau de prudence doit être augmenté au point de ne plus laisser de place au hasard. Le jeu vaut-il vraiment la chandelle face aux graves conséquences que peut engendrer un simple clic mal placé ?

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**.
Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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 Liberté) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : One in two users click on links from unknown senders › FAU.EU

Déplacements professionnels. Attention au Wi-Fi de l'hôtel…

Déplacements professionnels. Attention au Wi-Fi de l'hôtel…

De nos jours, qui réussirait à se passer d'Internet plus d'une journée, en vacances, en déplacement, lors d'une conférence ou au travail ? Nos vies aujourd'hui digitalisées nous poussent à nous connecter quasi automatiquement au premier réseau Wi-Fi disponible, quitte à mettre la confidentialité de nos données en danger.

Cela devient d'autant plus problématique lorsque nous voyageons : une étude Kaspersky Lab révélait récemment que 82% des personnes interrogées se connectent à des réseaux Wi-Fi gratuits non sécurisés dans des terminaux d'aéroports, des hôtels, des cafés ou des restaurants.
Dans la tribune ci-dessous, Tanguy de Coatpont, Directeur général de Kaspersky Lab France et Afrique du Nord analyse les vulnérabilités des réseaux Wi-Fi dans les hôtels, une mine d'or pour des cybercriminels en quête de données personnelles ou d'informations confidentielles.
Depuis 10 ans, le cyber crime s'est largement professionnalisé pour devenir une véritablement industrie, portée sur la rentabilité. Les cybercriminels sont en quête permanente de victimes qui leur assureront un maximum de gains pour un minimum d'investissements techniques.
De son côté, l'industrie hôtelière a passé la dernière décennie à se transformer pour répondre aux nouvelles attentes digitales de ses clients. Alors que plus d'un quart d'entre eux annoncent qu'ils refuseraient de séjourner dans un hôtel ne proposant pas de Wi-Fi, la technologie n'est plus un luxe mais bien une question de survie pour les établissements hôteliers. Face aux ruptures liées à la numérisation, il a donc fallu repenser les modèles existants et s'équiper, parfois en hâte, de nouvelles technologies mal maîtrisées. Il n'était donc pas surprenant de voir émerger rapidement des problèmes de sécurité, dans les hôtels bon marché comme dans les 5 étoiles.
Par Tanguy de Coatpont, Directeur général de Kaspersky Lab France et Afrique du Nord

Le paradoxe du Wi-Fi à l'hôtel : privé mais public
Ils ont beau être déployés dans des établissements privés, les Wi-Fi d'hôtels restent des points d'accès publics. Ils sont même parfois complètement ouverts. Le processus de connexion, qui nécessite le plus souvent de confirmer son identité et son numéro de chambre, limite l'accès au réseau mais ne chiffre pas les communications. Il ne garantit pas non plus leur confidentialité. Est-ce que cela signifie que nos informations sont à la portée de tous ? La réalité n'est pas aussi sombre, mais elles sont à la portée de n'importe quel criminel équipé d'un logiciel de piratage, dont certains sont disponibles gratuitement en ligne, et disposant de connaissances techniques de base.
Concrètement, il suffit à un criminel de se positionner virtuellement entre l'utilisateur et le point de connexion pour récupérer toutes les données qui transitent par le réseau, qu'il s'agisse d'emails, de données bancaires ou encore de mots de passe qui lui donneront accès à tous les comptes de l'internaute.
Une approche plus sophistiquée consiste à utiliser une connexion Wi-Fi non sécurisée pour propager un malware, en créant par exemple des fenêtres pop-up malveillantes qui invitent faussement l'utilisateur à mettre à jour un logiciel légitime comme Windows.

Le mythe de la victime idéale
En 2014, le groupe de cybercriminels Darkhotel avait utilisé une connexion Wi-Fi pour infiltrer un réseau d'hôtels de luxe et espionner quelques-uns de leurs clients les plus prestigieux. Un an plus tard, les activités de ce groupe étaient toujours en cours, continuant d'exfiltrer les données des dirigeants d'entreprises et dignitaires. Pour autant, les cybercriminels ne ciblent pas que des victimes à hauts profils. Beaucoup d'utilisateurs continuent de penser qu'ils ne courent aucun risque car les informations qu'ils partagent sur Internet ne méritent pas d'être piratées. C'est oublier que la rentabilité d'une attaque repose aussi sur le nombre de victimes. Parmi les 30 millions de clients pris en charge par l'hôtellerie française chaque année, seuls 20% sont des clients d'affaires. Les 80% de voyageurs de loisirs représentent donc une manne financière tout aussi importante pour des cybercriminels en quête de profit.
Dans certains cas, une faille Wi-Fi peut même exposer l'hôtel lui-même, en servant de porte d'entrée vers son réseau. Si l'on prend le cas d'une chaîne d'hôtellerie internationale qui disposerait d'un système de gestion centralisé et automatisé, une intrusion sur le réseau pourrait entrainer le vol à grande échelle d'informations confidentielles et bancaires sur les employées, le fonctionnement de l'hôtel et ses clients.

Hôtels indépendants vs. chaînes hôtelières : des contraintes différentes pour un même défi
Pour une industrie aussi fragmentée que celle de l'hôtellerie, la sécurité est sans aucun doute un défi. Les hôtels indépendants ont une capacité d'accueil réduite et traitent donc moins de données. Le revers de la médaille est qu'ils disposent souvent d'une expertise informatique limitée et leur taille ne permet pas de réaliser les économies d'échelle qui rentabiliseraient un investissement important dans la sécurité informatique. Quant aux grands groupes, qui comptent des ressources humaines et financières plus importantes, ils sont mis à mal par l'étendue de leur écosystème, qui rend difficile l'harmonisation d'une politique de sécurité sur des centaines, voire des milliers de sites.
Il est important que tous les hôtels, quelle que soit leur taille ou leur catégorie, respectent quelques règles simples à commencer par l'isolation de chaque client sur le réseau, l'utilisation de technologies de chiffrement et l'installation de solutions de sécurité professionnelles. Enfin, le réseau Wi-Fi offert aux clients ne doit jamais être connecté au reste du système informatique de l'hôtel, afin d'éviter qu'une petite infection ne se transforme en épidémie généralisée. En respectant ces règles, la sécurité pourrait devenir un argument commercial au moins aussi efficace que le Wi-Fi.
Article original de Robert Kassous

Denis JACOPINI est Expert Informatique et aussi **formateur en Cybercriminalité** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous pouvons vous animer des **actions de sensibilisation ou de formation** à la Protection des Données Personnelles, au risque informatique, à l'hygiène informatique et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-en-cybercriminalite-et-en-protection-des-donnees-personnelles
Denis JACOPINI

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 : Etude Kaspersky sur le Wi-Fi à l'hôtel… | InfoTravel.fr

Sensibilisations et Formations à la Cybercriminalité et au RGPD (Protection des données personnelles) – Redirect

Parce que la Cybercriminalité et la Protection des données personnelles sont liés, nous couvrons ces sujets concomitamment (Intervention en France et étranger)

Nos formations sont personnalisées en fonction du type de publics présent (Dirigeants, cadres , informaticiens, responsable informatique, RSSI, utilisateurs).

Contactez-nous

PROGRAMME

CYBERCRIMINALITÉ
COMMENT PROTÉGER VOTRE ORGANISME DE LA CYBERCRIMINALITÉ

Présentation

La France a rattrapé sont retard en matière d’équipement à Internet mais à en voir les dizaines de millions de français victimes chaque année, les bonnes pratiques ne semblent toujours pas intégrées dans vos habitudes.

Piratages, arnaques, demandes de rançons sont légions dans ce monde numérique et se protéger au moyen d’un antivirus ne suffit plus depuis bien longtemps.

Avons-nous raison d’avoir peur et comment se protéger ?

Cette formation couvrira les principaux risques et les principales solutions, pour la plupart gratuites, vous permettant de protéger votre informatique et de ne plus faire vous piéger.

Objectifs

Découvrez les règles de bonnes pratiques et des attitudes responsables qui sont les clés permettant de naviguer sur Internet en toute sécurité.

Demande d’informations

CYBERCRIMINALITÉ
LES ARNAQUES INTERNET A CONNAÎTRE POUR NE PLUS SE FAIRE AVOIR

Présentation

Que vous vous serviez d’Internet pour acheter, vendre, télécharger ou communiquer, un arnaqueur se cache peut-être derrière votre interlocuteur.

Quels sont les signes qui ne trompent pas ? Comment les détecter pour ne pas vous faire piéger ?

Objectifs

Découvrez les mécanismes astucieux utilisés par les arnaqueurs

d’Internet dans plus d’une vingtaine cas d’arnaques différents. Une fois expliqués, vous ne pourrez plus vous faire piéger.

Demande d’informations

PROTECTION DES DONNÉES

RGPD (RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES) – CE QU’IL FAUT SAVOIR POUR NE PAS LE PAYER CHER

Présentation

Le Règlement Général sur la Protection de Données (RGPD) est entré en application le 25 mai 2018 et toutes les entreprises, administrations et associations ne se sont pas mises en conformité. Or, quelle que soit leur taille, elles sont toutes concernées et risqueront, en cas de manquement, des sanctions financières jusqu’alors inégalées.

Au delà de ces amendes pouvant attendre plusieurs millions d’euros, de nouvelles obligations de signalement de piratages informatiques risquent désormais aussi d’entacher votre réputation. Quelle valeur lui donnez vous ? Serez-vous prêt à la perdre pour ne pas avoir fais les démarches dans les temps ?

Cette formation non seulement répondra la plupart des questions que vous vous posez, vous offrira des éléments concrets non seulement pour initier la mise en conformité de votre établissement mais surtout pour transformer ce qui peut vous sembler à ce jour être une contrainte en une véritable opportunité.

Objectifs

Cette formation a pour objectif de vous apporter l’essentiel pour comprendre et démarrer votre mise en conformité avec le

RGPD dans le but à la fois de répondre à la réglementation et de prévenir en cas de contrôle de la CNIL.

Informations complémentaires

Demande d'informations

PROTECTION DES DONNÉES

RGPD (RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES) – ANALYSONS CE QUE VOUS AVEZ COMMENCÉ

Présentation

Après avoir suivi notre formation vous permettant de comprendre l'intérêt d'une telle réglementation et de savoir ce qu'il faut mettre en place pour bien démarrer, vous souhaitez aller plus loin dans la démarche de mise en conformité avec le RGPD.

Après un retour éclair sur les règles de base, nous ferons un point sur la démarche de mise en conformité que vous avez initiée ces derniers mois dans votre établissement. Nous détaillerons ensuite les démarches à réaliser en cas de détection de données sensibles et d'analyse d'impact. Enfin, nous approfondirons des démarches périphériques essentielles pour répondre à vos obligations.

Objectifs

Après avoir déjà découvert l'essentiel pour comprendre et démarrer votre mise en conformité avec le RGPD, cette formation aura pour objectif de vous perfectionner afin de devenir référent protection des données ou DPO (Data Protection Officer = Délégué à la Protection des Données).

Demande d'informations

CYBERSÉCURITÉ

DÉTECTER ET GÉRER LES CYBER-ATTAQUES

Présentation

Que vous ayez déjà été victime d’une cyber-attaque ou que vous souhaitiez l’anticiper, certaines procédures doivent absolument être respectées pour conserver un maximum de preuves et pouvoir les utiliser.

Objectifs

Que votre objectif soit de découvrir le mode opératoire pour savoir quelles sont les failles de votre système ou si vous avez été victime d’un acte ciblé avec l’intention de vous nuire, découvrez les procédures à suivre.

Demande d’informations

CYBERSÉCURITÉ

APPRENEZ À RÉALISER DES AUDITS SÉCURITÉ SUR VOTRE SYSTÈME INFORMATIQUE

Présentation

Votre système informatique a très probablement de nombreuses vulnérabilités présentées aux pirates informatiques comme de nombreux moyens de nuire à votre système informatique.

Avant de procéder à un test d’intrusion, apprenez à réaliser l’indispensable audit sécurité de votre système informatique afin d’appliquer les mesures de sécurité de base présentes dans les référentiels internationalement utilisés.

Objectifs

Vous apprendrez au cours de cette formation la manière dont doit être mené un audit sécurité sur un système informatique, quelques référentiels probablement adaptés à votre organisme et nous étudierons ensemble le niveau de sécurité informatique de votre établissement.

Demande d'informations

CYBERSÉCURITÉ

APPRENEZ À RÉALISER DES TESTS D'INTRUSION SUR VOTRE SYSTÈME INFORMATIQUE

Présentation

Cette formation vous apporte l'essentiel de ce dont vous avez besoin pour adopter l'approche du Hacker pour mieux s'en protéger en élaborant vos tests de vulnérabilité, mettre en place une approche offensive de la sécurité informatique permettant d'aboutir à une meilleure sécurité et réaliser des audits de sécurité (test d'intrusion) au sein de votre infrastructure.

La présentation des techniques d'attaques et des vulnérabilités potentielles sera effectuée sous un angle « pratique ».

Objectifs

Cette formation vous apportera la compréhension technique et pratique des différentes formes d'attaques existantes, en mettant l'accent sur les vulnérabilités les plus critiques pour mieux vous protéger d'attaques potentielles.

Demande d'informations

QUI EST LE FORMATEUR ?

Denis JACOPINI est Expert Informatique assermenté, diplômé en Cybercriminalité, Droit, Sécurité de l'information, informatique Légale, Investigation numérique pénale, et en Droit de l'Expertise Judiciaire et a été pendant une vingtaine d'année à la tête d'une société spécialisée en sécurité Informatique.

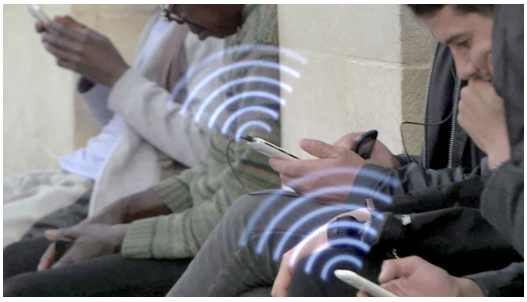
Il anime dans toute le France et à l'étranger des conférences et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles.
A ce titre, il intervient régulièrement sur différents médias et sur La Chaine d'Info LCI pour vulgariser les sujets d'actualité en rapport avec ces thèmes.

Spécialisé en protection des données personnelles, il accompagne les établissements dans leur mise en conformité CNIL en les accompagnant dans la mise en place d'un Correspondant Informatique et Libertés (CIL).

Enfin, il intervient en Master II dans un centre d'Enseignement et de Recherche en Informatique, en Master Lutte contre la Criminalité Financière et Organisée, au Centre National de la Fonction Publique Territoriale et anime le blog LeNetExpert.fr sur lequel il partage et publie de très nombreuses informations sur ses thèmes de prédilection.

Denis JACOPINI peut facilement être contacté sur :
http://www.leNetExpert.fr/contact

Comment se comporte notre cerveau surchargé par le numérique



Comment se comporte notre cerveau surchargé par le numérique

Samedi 3 septembre, ARTE a diffusé un excellent reportage sur la manière dont notre cerveau se comporte face à nos vies de plus en plus hyper connectées : « HYPERCONNECTÉS : LE CERVEAU EN SURCHARGE ».

Grâce aux smartphones, ordinateurs et autres tablettes, nous sommes reliés au monde en continu. Mais ce déluge d'informations menace notre bien-être. Alliant témoignages de cadres victimes de burn out et explications de chercheurs en neurosciences, en informatique ou en sciences de l'information et de la communication, ce documentaire captivant passe en revue les dangers de cette surcharge sur le cerveau. Il explore aussi des solutions pour s'en prémunir, des méthodes de filtrage de l'information aux innovations censées adapter la technologie à nos besoins et à nos limites.

Chaque jour, cent cinquante milliards d'e-mails sont échangés dans le monde. Les SMS, les fils d'actualité et les réseaux sociaux font également partie intégrante de notre quotidien connecté, tant au bureau qu'à l'extérieur. Nous disposons ainsi de tout un attirail technologique qui permet de rester en contact avec nos amis, nos collègues, et qui sollicite sans cesse notre attention. Comment notre cerveau réagit-il face à cette avalanche permanente de données ? Existe-t-il une limite au-delà de laquelle nous ne parvenons plus à traiter les informations ? Perte de concentration, stress, épuisement mental, voire dépression… : si les outils connectés augmentent la productivité au travail, des études montrent aussi que le trop-plein numérique qui envahit nos existences tend à diminuer les capacités cognitives.

Un documentaire de Laurence Serfaty (France, 52′), diffusé sur ARTE le samedi 3 septembre à 22h20

A voir et à revoir sur Arte +7 pendant encore quelques jours !

si vous ne voyez pas la vidéo, le lien

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 : Hyperconnectés : le

Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de passe » (à condition que…)| Denis JACOPINI

Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de passe » (à condition que…)| Denis JACOPINI

Une « phrase de passe » est beaucoup plus difficile à pirater qu'un « mot de passe ». Pour donner un ordre d'idée, les pirates du Web mettent quelques heures à quelques jours pour trouver un mot de passe de huit caractères complexes et mettraient… plusieurs millions d'années pour décoder un mot de passe complexe de 12 caractères.

Atlantico : Selon de nombreuses études menées par des chercheurs de l'Université américaine Carnegie-Mellon, un long mot de passe facile à retenir tel que « *ilfaitbeaudanstoutelafrancesaufdanslebassinparisien* » serait plus difficile à pirater qu'un mot de passe relativement court mais composé de glyphes de toutes sortes, tel que « *p8)J#&=89pE* », très difficiles à mémoriser. Pouvez-vous nous expliquer pourquoi ?

Denis Jacopini : La plupart des mots de passe sont piratés par une technique qu'on appelle « la force brute ». En d'autres termes, les hackers vont utiliser toutes les combinaisons possibles des caractères qui composent le mot de passe.

Donc, logiquement, plus le mot de passe choisi va avoir de caractères (majuscule, minuscule, chiffre, symbole), plus il va être long à trouver. Pour donner un ordre d'idée, les pirates du Web mettent quelques heures à quelques jours pour trouver un mot de passe de huit caractères complexes via la technique de « la force brute », et mettraient… plusieurs millions d'années pour décoder un mot de passe complexe de 12 caractères.

Un long mot de passe est donc plus difficile à pirater qu'un mot de passe court, à une condition cependant : que **la phrase choisie comme mot de passe ne soit pas une phrase connue de tous**, qui sort dès qu'on en tape les premiers mots dans la barre de recherche de Google. Les pirates du Net ont en effet des bases de données où ils compilent toutes les phrases, expressions ou mots de passe les plus couramment utilisés, et essayent de hacker les données personnelles en les composant tous les uns derrière les autres. Par exemple, mieux vaut avoir un mot de passe court et complexe plutôt qu'une « phrase de passe » comme « *Sur le pont d'Avignon, on y danse on y danse…* ».

Il faut également bien veiller à ce que cette « phrase de passe » ne corresponde pas trop à nos habitudes de vie, car les pirates du Web les étudient aussi pour arriver à leur fin. Par exemple, si vous avez un chien qui s'appelle « Titi » et que vous habitez dans le 93, il y a beaucoup de chance que votre ou vos mots de passe emploient ces termes, avec des associations basiques du type : « *jevaispromenermonchienTITIdansle93* ».

De plus, selon la Federal Trade Commission, changer son mot de passe régulièrement comme il est habituellement recommandé aurait pour effet de faciliter le piratage. Pourquoi ?

Changer fréquemment de mot de passe est en soi une très bonne recommandation, mais elle a un effet pervers : plus les internautes changent leurs mots de passe, plus ils doivent en inventer de nouveaux, ce qui finit par embrouiller leur mémoire. **Dès lors, plus les internautes changent fréquemment de mots de passe, plus ils les simplifient, par peur de les oublier, ce qui, comme expliqué plus haut, facilite grandement le piratage informatique.**

Plus généralement, quels seraient vos conseils pour se prémunir le plus efficacement du piratage informatique ?

Je conseille d'avoir une « phrase de passe » plutôt qu'un « mot de passe », qui ne soit pas connue de tous, et dont on peut aisément en changer la fin, pour ne pas avoir la même « phrase de passe » qui vérouille nos différents comptes.

Enfin et surtout, je conseille de ne pas se focaliser uniquement sur la conception du mot de passe ou de la « phrase de passe », parce que c'est très loin d'être suffisant pour se prémunir du piratage informatique. Ouvrir par erreur un mail contenant un malware peut donner accès à toutes vos données personnelles, sans avoir à pirater aucun mot de passe. Il faut donc rester vigilant sur les mails que l'on ouvre, réfléchir à qui on communique notre mot de passe professionnel si on travail sur un ordinateur partagé, bien vérrouiller son ordinateur, etc…

Article original de Denis JACOPINI et Atlantico

Réagissez à cet article

Original de l’article mis en page : Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de passe » (à condition que…) | Atlantico.fr

---

L’entreprise victime ou coupable de Cyberattaques ? | Le Net Expert Informatique

L’entreprise victime ou coupable de Cyberattaques ?

LES FAITS En avril 2015, TV5 Monde a été la cible d'une cyberattaque massive entraînant la paralysie de la chaîne, du site Internet et des réseaux sociaux de la société. Si les attaques informatiques visant les grands groupes sont médiatisées, Symantec soulignait dans son rapport annuel 2014 que 77 % d'entre elles concernaient en France les PME.
Ces failles informatiques d'origines internes ou externes doivent être appréhendées car elles s'accompagnent de sévères répercussions en termes de sécurité, de pertes économiques et de dégradation de l'image de l'entreprise. Or, la majorité d'entre elles ignorent qu'elles sont tenues, en application de l'article 34 de la Loi Informatique et Libertés, d'une obligation de moyen de mettre en œuvre les mesures conformes aux règles de l'art pour protéger leur système d'information. Au-delà du risque civil, des sanctions administratives et même pénales peuvent être prononcées allant jusqu'à 5 ans de prison et 300 000 € d'amende. Ainsi, de victime, l'entreprise qui n'aurait pas pris toutes les « précautions utiles » pour préserver « la sécurité des données » peut, indépendamment de son dommage, se voir reconnaître responsable, comme Orange qui a été sanctionnée par la CNIL à la suite d'une faille de sécurité concernant les données de près de 1,3 million de ses clients en août 2014.

LA PRÉVENTION POUR LIMITER LES RISQUES
La mise en place d'une #politique de cybersécurité adaptée aux besoins de l'entreprise comportant des mesures techniques de sécurité informatique ainsi qu'une #politique de gestion des incidents, dont la mise en œuvre est préconisée par la #norme ISO 27035, est indispensable. Il convient également de concevoir la sécurité des données dans les relations avec les prestataires, en insérant des clauses spécifiques dans les contrats qui les lient précisant clairement le partage de responsabilité entre les deux parties. Dans ce cadre, un état des lieux du patrimoine informationnel détenu par l'entreprise s'impose afin d'assurer aux données sensibles la sécurité adéquate, ainsi que la réalisation d'#audits techniques et de #correctifs réguliers du système d'information (typologie et quantité de données, protections, vulnérabilités, etc.).
Par ailleurs, une communication en interne sensibilisant les salariés sur ces risques est essentielle. Le recours à une #charte informatique précise annexée au règlement intérieur de l'entreprise fixant les droits, devoirs et obligations des salariés est un outil efficace. À cet égard, l'ANSSI vient de publier, en coopération avec la CGPME, un #guide de recommandation de bonnes pratiques simples qu'il convient de mettre en œuvre. Au-delà de ces mesures de prévention, il est conseillé de bien soigner les contrats d'assurance afin d'anticiper sur ces causes de pertes d'exploitation. Enfin, rappelons que depuis l'ordonnance du 24 août 2011, les opérateurs de communications électroniques sont tenus à une obligation de notification de la faille de sécurité, sans délai, à la CNIL et aux personnes concernées, prévue par l'article 34 bis de la Loi Informatique et Libertés, dont le défaut est sanctionné pénalement. À noter que le projet de réforme de règlement européen prévoit d'étendre cette obligation à toutes les entreprises, comme c'est le cas aux États-Unis.

CE QU'IL FAUT RETENIR
Le cyber-risque constitue une menace réelle que les entreprises doivent appréhender et anticiper pour ne pas voir, à titre de double peine, leur responsabilité engagée.

Source : http://www.itforbusiness.fr/services/juridique/item/6693-cyberattaques-l-entreprise-victime-ou-coupable

Comment les salariés peuvent lutter contre la cybercriminalité | Denis JACOPINI

	Comment les salariés peuvent lutter contre la cybercriminalité

Les entreprises -quels que soient leur taille économique et leur secteur d'activité- subissent des cyberattaques ciblées qui visent leurs actifs stratégiques. Ce qui entraîne des pertes de plusieurs millions de dollars. Au-delà des offres technologiques de sécurité et des discours méthodologiques qui fleurissent sur le marché, une véritable politique organisationnelle formée et informée face aux dangers doit être développée dans l'entreprise. Quel rôle pour les RH?

Le cybercrime est un phénomène complexe intégrant en son sein un spectre très large de méthodes, de cibles et de motivations. On assiste de moins en moins aux actions de l'hacker isolé uniquement motivé par la mise en lumière de ses exploits ou à celles de l'hacktiviste politique développant des attaques à des fins de sabotage. Le cybercrime est aujourd'hui de plus en plus organisé. Appâté par des gains financiers directs, il met en œuvre ses exactions via des mécaniques sophistiquées comme le spear fishing, l'ingénierie sociale ou encore les menaces furtives APT (Advanced Persistent Threats) au travers d'attaques ciblées, de grande envergure et de plus en plus dévastatrices. Et comme l'a dévoilé la retentissante affaire Edward Snowden aux Etats-Unis, les cyber armées misent en branle par les gouvernements à des fins de renseignement ou d'espionnage industriel sont également très actives.

Un contexte technologique propice aux failles mais pas uniquement …

Si les attaques cybercriminelles réussissent aujourd'hui, c'est que les évolutions technologiques majeures comme le Cloud, le BYOD (Bring Your Own Devive) ou encore les objets connectés… – en augmentant de manière exponentielle les données disponibles au niveau mondial – ont ouvert et donc fragilisé le réseau de l'entreprise. Ce contexte de démultiplication des périphériques, des utilisateurs et des usages génère des failles et des vulnérabilités, largement exploitées par les cyber assaillants. Mais même si leur impact est bel et bien réel, les transformations technologiques ne sont pas les seules au banc des accusés. En 2015, selon un rapport de sécurité Check Point, 81% des entreprises ont subi des fuites de données causées par des négligences humaines. L'humain, ce « maillon faible » est un élément clé de toute stratégie cyber défense même s'il n'est toujours pas appréhendé sérieusement par les entreprises. Et c'est là que les RH ont leur carte à jouer.

Le rôle déterminant des RH: transformer l'humain en un atout pour la sécurité de l'entreprise

Redoublant d'ingéniosité pour arriver à leurs fins, les cyber assaillants mettent en œuvre des attaques d'ingénierie sociale et d'hameçonnage qui exploitent les faiblesses humaines (vanité, reconnaissance, ignorance, gentillesse…) avec pour finalité le vol de données sensibles, le gain direct ou encore l'espionnage industriel. Ces attaques sont très difficiles à détecter par les entreprises car elles ne sont pas identifiées par leurs barrages technologiques et peuvent même passer inaperçues aux yeux de leurs victimes! Pour déjouer les manœuvres des cybercriminels, une culture « sécurité » portée par les RH doit être mise en œuvre pour sensibiliser et responsabiliser les employés de l'entreprise, à chaque couche fonctionnelle et dans le cadre d'une véritable démarche collaborative. Comment?

1/ En assumant la responsabilité des risques de sécurité posés par les collaborateurs de l'entreprise. La grande majorité des employés ne se sent pas vraiment concernée par les problématiques de sécurité de leur entreprise. Elle les considère comme seule responsabilité du département informatique et cette attitude rend les entreprises bien trop vulnérables. Une politique de sécurité interne ne sera efficace que si elle est comprise et intégrée par les collaborateurs via un véritable état d'esprit associé à une somme de comportements quotidiens. Les RH doivent mener des politiques de sensibilisation actives, sur la durée, portant sur les dangers, les techniques employées par les cyber délinquants et l'impact comportemental des employés sur la sécurité de l'entreprise.

2/ En identifiant le personnel vulnérable. Un des risques majeurs en matière de sécurité est l'accès des employés aux données sensibles de l'entreprise. Dans le cas du piratage de Sony Pictures, les experts ont évoqué l'implication d'un ou de plusieurs ex-employés du Groupe dont l'accès toujours actif au réseau a permis le vol d'informations critiques. En outre, les cybercriminels ont besoin du support de collaborateurs ou de partenaires de l'entreprise qui vont les aider volontairement ou non à arriver à leur fins. Ils utilisent ainsi les réseaux sociaux pour identifier leur cible/victime potentielle, celle qui aura une prédisposition à briser les systèmes de sécurité de l'entreprise, sera démotivée ou en désaccord avec sa hiérarchie. Au cœur de ces informations, les RH doivent ainsi redoubler de vigilance vis-à-vis de ressources à risques ou plus exposées comme les nouveaux arrivants, les employés sur le départ, des fonctions spécifiques (accueil/helpdesk, secrétariats, …) ou stratégiques tels que les directeurs financiers …

3/ En sensibilisant la Direction Générale. La mise en place d'une culture de la sécurité au sein de l'entreprise doit bénéficier du support du top management. Or les Directions Générales ne sont pas encore forcément sensibles à la mise en place de ces programmes de formations, orientant leurs investissements sécuritaires plutôt vers des dispositifs technologiques. Messieurs les Directeurs, comme l'a si justement souligné Derek Bok, Président de la prestigieuse université d'Harvard « Si vous pensez que l'éducation est chère, alors tentez l'ignorance » ! Il est aujourd'hui impératif pour les entreprises de mettre en place une vraie stratégie de sécurité basée sur une mobilisation interne transverse associant les métiers, le comité de direction, les RH et le RSSI.

Le cybercrime est bien réel, organisé, déterminé et atteint son but même pour les plus grandes organisations internationales aux murailles technologiques dites « infranchissables ». C'est aux entreprises maintenant de penser et de développer une organisation de sécurité en miroir, dotée d'un niveau de maturité technique et organisationnel tout aussi élevé que celui de leurs cybers assaillants. La sensibilisation de l'humain, clé de voûte d'une bonne stratégie de cyberdéfense ne doit pas être négligée et les RH devront vite s'emparer du sujet avant que l'ennemi ne soit dans la place !

Source : http://www.challenges.fr/tribunes/20150624.CHA7247/comment-les-salaries-peuvent-lutter-contre-la-cybercriminalite.html
par Emmanuel Stanislas, fondateur du cabinet de recrutement Clémentine.