Quoi et comment supprimer vos données si vous rendez votre ordinateur professionnel à votre employeur ?

	Quoi et comment supprimer vos données si vous rendez votre ordinateur professionnel à votre employeur ?

Est-il possible d'effacer toutes nos données présentes sur un ordinateur de fonction lorsque l'on quitte son travail et que l'on ne souhaite pas laisser de trace sur celui-ci ? Si oui, quels moyens préconisez-vous pour être sûr que ce type de données soit bien effacé (effacer l'historique de ses comptes mails et personnelles, formatage complet, logiciel d'aide à la suppression etc…) ?

La première étape consiste à identifier les données à supprimer et celles à sauvegarder avant de procéder au nettoyage.
Sur la plupart des ordinateurs professionnels, parfois sans le savoir, en plus de nos documents de travail nous stockons :
• Des programmes ajoutés ;
• Nos e-mails ;
• Nos traces de navigation ;
• Nos fichiers téléchargés ;
• Divers identifiants et mots de passe ;
• Les fichiers temporaires

Afin d'éviter l'accès à ces informations par le futur locataire / propriétaire / donataire de votre ordinateur, il sera important de procéder à leur suppression minutieuse.

Concernant les programmes ajoutés
Facile sur Mac en mettant le dossier d'un programme à la corbeille, n'utilisez surtout pas la corbeille pour supprimer des programmes sous Windows. La plupart des programmes apparaissent dans la liste des programmes installés. Pour procéder à leur suppression, nous vous conseillons de procéder :
• soit par le raccourcis de désinstallation que le programme a créé ;
• s'il n'y a pas de raccourci prévu à cet effet, passez par la fonction « Ajout et Suppression de Programmes » ou « Programmes et fonctionnalités » (ou fonction équivalente en fonction de votre système d'exploitation de sa version) ;
• Enfin, vous pouvez utiliser des programmes adaptés pour cette opération tels que RevoUninstaller (gratuit).

Concernant les e-mails
Selon le programme que vous utiliserez, la suppression du/des compte(s) de messagerie dans le programme en question suffit pour supprimer le ou les fichiers contenant les e-mails. Sinon, par précaution, vous pouvez directement les localiser et les supprimer :
• fichiers « .pst » et « .ost » de votre compte et archives pour le logiciel « Outlook » ;
• fichiers dans « » »% »'AppDataLocalMicrosoftWindows Live Mail » pour le logiciel « Windows Live Mail » ;
• les fichiers contenus dans ' » »% »'APPDATA%ThunderbirdProfiles » pour le programme Mozilla Thunderbird
• le dossier contenu dans « ..Local SettingsApplication DataIMIdentities » pour le programme Incredimail.

Concernant nos traces de navigation
En fonction de votre navigateur Internet et de sa version, utilisez, dans les « Options » ou les « Paramètres » la fonction supprimant l'Historique de Navigation » ou les « Données de Navigation ».

Concernant les fichiers téléchargés
En fonction de votre système d'exploitation l'emplacement de stockage par défaut des fichiers téléchargés change. Pensez toutefois à parcourir les différents endroits de votre disque dur, dans les lecteurs réseau ou les lecteurs externes à la recherche de fichiers et documents téléchargés que vous auriez pu stocker.

Concernant divers identifiants et mots de passe
Du fait que le mot de passe de votre système d'exploitation stocké quelque part (certes crypté), si vous êtes le seul à le connaître et souhaitez en conserver la confidentialité, pensez à le changer et à en mettre un basic de type « utilisateur ».
Du fait que les mots de passe que vous avez mémorisé au fil de vos consultations de sites Internet sont également stockés dans vote ordinateur, nous vous recommandons d'utiliser les fonctions dans ces mêmes navigateurs destinées à supprimer les mots de passes et les informations qui pré remplissent les champs.

Concernant les fichiers temporaires
En utilisant la fonction adaptée dans vos navigateurs Internet, pensez à supprimer les fichiers temporaires liés à la navigation Internet (images, cookies, historiques de navigation, autres fichiers).
En utilisant la fonction adaptée dans votre systèmes d'exploitation, supprimez les fichiers temporaires que les programmes et Windows génèrent automatiquement pour leur usage.

Pour finir
Parce qu'un fichier supprimé n'est pas tout à fait supprimé (il est simplement marqué supprimé mais il est toujours présent) et dans bien des cas toujours récupérable, vous pourrez utiliser une application permettant de supprimer définitivement ces fichiers supprimés mais pourtant récupérables telle que « Eraser », « Clean Disk Security », « Prevent Restore »…

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

---

Réagissez à cet article

Original de l’article mis en page : 5 applications pour effacer des données de façon sécurisée – ZDNet

---

Étape par étape : comment bien effacer et conserver vos données informatiques stockées sur votre ordinateur professionnel si vous changez de travail à la rentrée (et pourquoi c’est très important) ?

Étape par étape : comment bien effacer et conserver vos données informatiques stockées sur votre ordinateur professionnel si vous changez de travail à la rentrée (et pourquoi c’est très important) ?

Quitter son travail est souvent difficile, mais effacer des données présentes sur un ordinateur professionnel sur lequel on a travaillé pendant X années l'est encore plus. Il est donc nécessaire de savoir comment le faire sans laisser de données professionnelles ou personnelles derrière soi.

Atlantico : Quelles étapes faut-il suivre avant d'effacer nos données personnelles présentes sur notre futur ancien ordinateur de fonction ?

Denis Jacopini : L'ordinateur professionnel qui vous a été mis à disposition était probablement en état de marche. À moins d'avoir des circonstances ou des consignes particulières, vous devrez donc rendre cet appareil au moins dans l'état initial.
1. En premier lieu, pensez à identifier les données à sauvegarder dont il vous sera nécessaire de conserver copie. Attention aux données professionnelles frappées de confidentialité ou d'une clause de non concurrence, tel que les fichiers clients.
On pourrait bien vous reprocher d'en avoir conservé une copie et de l'utiliser contre votre ancien employeur.
2. Identifiez les données ayant un caractère confidentiel et qui nécessiteront une sauvegarde dans un format protégé par un procédé tel que le cryptage ou le hachage.
3. Identifiez les données devant être conservées pendant un grand nombre d'années tels que des justificatifs d'assurance, de sinistre…
4. Identifiez les données que vous ne devez absolument pas perdre car non reproductibles (contrats, photos de mariage, des enfants, petits-enfants…)
5. Identifiez les données que vous souhaitez rendre accessibles sur plusieurs plateformes (ordinateurs, téléphones, tablettes) que ça soit au bureau à la maison, en déplacement ou en vacances. Ensuite, en fonction des logiciels permettant d'accéder à vos données, identifiez les fonctions de « Sauvegarde », « Enregistrer sous » ou d' «Export ». Vous pourrez alors choisir le support adapté.
Enfin, en fonction des critères de sécurité choisis, vous pourrez sauvegarder sur des supports adaptée soit :
– à la confidentialité (tout support numérique en utilisant un logiciel de cryptage ou de hachage tel de Truecrypt, Veracrypt, ou AxCrypt…) ;
– à l'intégrité (multiplier le nombre de sauvegardes en réalisant plusieurs exemplaires de vos données à n'absolument pas perdre) ;
– à la longévité en utilisant des supports avec une durée de vie adapté à vos attentes. Sachez qu'à ce jour, il est difficile de garantir la lecture d'une information numérique au-delà de plusieurs dizaines d'années (en raison de l'altération des supports avec le temps, mais aussi de l'évolution des versions, des formations et des logiciels). Qui peut vous garantir de pouvoir visualiser vos photos numériques dans cinquante ans ?
– à la disponibilité sur plusieurs plateformes et sur plusieurs lieux, comme le proposent les solutions *cloud* qui sont éclos il y a quelques dizaines d'années seulement ;
– à la quantité (car vous devez rapidement stocker pour ensuite trier et choisir un support adapté) en choisissant par exemple un disque dur USB externe auto-alimenté (si le port USB de votre ordinateur l'autorise), ce support est actuellement celui ayant le meilleur rapport capacité / prix avec une bonne rapidité d'écriture.

Les risques :
Les clés USB sont des outils permettant de conserver une copie facilement accessible et aisément transportable. 100% des clés USB tomberont un jour ou l'autre en panne. Pensez-y pour ne pas leur confier les documents de votre vie.
Idem pour les disques durs. 100% des disques durs tomberont un jour en panne. Cependant, contrairement aux clés USB ou aux cartes mémoire, les disques durs (mécaniques et non SSD) permettront plus facilement de récupérer leur contenu en cas de panne.
Les supports de type lecteurs ZIP, lecteur JAZ, lecteurs magnéto-optiques, lecteurs de bandes etc. sont de plus en plus rares. Conserver des données importantes sur de tels supports peut s'avérer dangereux. En effet, imaginez un instant jour ou vous souhaitez y accéder mais que vous n'avez plus le lecteur pour les consulter et que le lecteur ne se vend même plus. Ne laissez pas la vies de vos données numériques entre les mains du *Bon Coin*…
Voilà, en fonction de tous ces critères et à partir de ces conseils, il ne vous reste plus qu'à sauvegarder vos données importantes avant de les effacer de l'appareil que vous allez rendre.

Comparatif :
Disque dur : Quelques Go à quelques To – Bon marché, rapide mais fragile.
Clé USB : Quelques Go – Rapide, léger mais quasiment impossible de récupérer des données en cas de panne.
Cloud : Quelques Mo à quelques To – Accessible de n'importe où mais aussi par tous ceux qui ont le mot de passe (risqué) – Dépend du fonctionnement et de la rapidité d'Internet – Les services de cloud gratuits peuvent s'arrêter du jour au lendemain et vous perdrez tout.
Disques optiques (CD, DVD,Magnéto Optique) : Bonne tenue dans le temps si conservés dans de bonnes conditions mais utilisables (pérennité des lecteurs de disques) jusqu'à quand ?
Supports spéciaux (ZIP/Jazz/QIC/DAT/DLT/DDS/SDLT) : Supports fragiles, lecteurs trop rares pour garantir une lecture au delà de 5 ans.

Est-il possible d'effacer toutes nos données présentes sur un ordinateur de fonction lorsque l'on quitte son travail et que l'on ne souhaite pas laisser de traces sur celui-ci ? Si oui, quels moyens préconisez-vous pour être sûr que ce type de données soit bien effacé ?

La première étape consiste à identifier les données à supprimer et celles à sauvegarder avant de procéder au nettoyage. Sur la plupart des ordinateurs professionnels, parfois sans le savoir, en plus de nos documents de travail nous stockons :
– Des programmes ajoutés ;
– Nos e-mails ;
– Nos traces de navigation ;
– Nos fichiers téléchargés ;
– Divers identifiants et mots de passe ;
– Les fichiers temporaires
Afin d'éviter l'accès à ces informations par le futur locataire / propriétaire / donataire de votre ordinateur, il sera important de procéder à leur suppression minutieuse.

Concernant les programmes ajoutés :
Facile sur Mac en mettant le dossier d'un programme à la corbeille, n'utilisez surtout pas la corbeille pour supprimer des programmes sous Windows. La plupart des programmes apparaissent dans la liste des programmes installés. Pour procéder à leur suppression, nous vous conseillons de procéder :
– soit par le raccourcis de désinstallation que le programme a créé ;
– s'il n'y a pas de raccourcis prévu à cet effet, passez par la fonction « Ajout et Suppression de Programmes » ou « Programmes et fonctionnalités » (ou fonction équivalente en fonction de votre système d'exploitation de sa version) ;
– Enfin, vous pouvez utiliser des programmes adaptés pour cette opération tels que RevoUninstaller (gratuit).
Concernant les e-mails :
Selon le programme que vous utiliserez, la suppression du/des compte(s) de messagerie dans le programme en question suffit pour supprimer le ou les fichiers contenant les e-mails. Sinon, par précaution, vous pouvez directement les localiser et les supprimer :
– fichiers « .pst » et « .ost » de votre compte et archives pour le logiciel « Outlook » ;
– fichiers dans « » « % %'AppDataLocalMicrosoftWindows Live Mail » pour le logiciel « Windows Live Mail » ;
– les fichiers contenus dans ' » «% «'APPDATA%ThunderbirdProfiles » pour le programme Mozilla Thunderbird
– le dossier contenu dans « _Local SettingsApplication DataIMIdentities » pour le programme Incredimail.
Concernant nos traces de navigation :
En fonction de votre navigateur Internet et de sa version, utilisez, dans les « Options » ou les « Paramètres » la fonction supprimant l'Historique de Navigation » ou les « Données de Navigation ».
Concernant les fichiers téléchargés :
En fonction de votre système d'exploitation l'emplacement de stockage par défaut des fichiers téléchargés change. Pensez toutefois à parcourir les différents endroits de votre disque dur, dans les lecteurs réseau ou les lecteurs externes à la recherche de fichiers et documents téléchargés que vous auriez pu stocker.
Concernant divers identifiants et mots de passe :
Du fait que le mot de passe de votre système d'exploitation stocké quelque part (certes crypté), si vous êtes le seul à le connaître et souhaitez en conserver la confidentialité, pensez à le changer et à en mettre un basic de type « utilisateur ».
Du fait que les mots de passe que vous avez mémorisé au fil de vos consultations de sites Internet sont également stockés dans votre ordinateur, nous vous recommandons d'utiliser les fonctions dans ces mêmes navigateurs destinées à supprimer les mots de passes et les informations qui pré remplissent les champs.
Concernant les fichiers temporaires :
En utilisant la fonction adaptée dans vos navigateurs Internet, pensez à supprimer les fichiers temporaires liés à la navigation Internet (images, cookies, historiques de navigation, autres fichiers).
En utilisant la fonction adaptée dans votre systèmes d'exploitation, supprimez les fichiers temporaires que les programmes et Windows génèrent automatiquement pour leur usage.
Pour finir :
Parce qu'un fichier supprimé n'est pas tout à fait supprimé (il est simplement marqué supprimé mais il est toujours présent) et dans bien des cas toujours récupérable, vous pourrez utiliser une application permettant de supprimer définitivement ces fichiers supprimés mais pourtant récupérables telle que « Eraser », « Clean Disk Security », « Prevent Restore »…

Ne pas effacer ses données personnelles sur so ordinateur de fonction est-il dommageable ? Si oui, pourquoi ?

Imaginez, votre ordinateur, protégé ou non, tombe entre les mains d'une personne malveillante. Il pourra :
– Accéder à vos documents et découvrir les informations qui peuvent soit être professionnelles et être utilisées contre vous, soit personnelles permettant à un voyou de les utiliser contre vous soit en vous demandant de l'argent contre son silence ou pour avoir la paix ;
– Accéder aux identifiants et mots de passe des comptes internet que vous utilisez (même pour des sites Internet commençant par https) et ainsi accéder à nos comptes facebook, twitter, dropbox… ;
– Avec vos identifiants ou en accédant à votre système de messagerie, le pirate pourra facilement déposer des commentaires ou envoyer des e-mails en utilisant votre identité.

Auteur : Denis JACOPINI

Denis Jacopini anime des **conférences et des formations** 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

Réagissez à cet article

Original de l'article mis en page : Étape par étape : comment bien effacer et conserver vos données informatiques stockées sur votre ordinateur professionnel si vous changez de travail à la rentrée (et pourquoi c'est très important) | Atlantico.fr

---

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

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

---

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

Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques

	Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques

Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques

1. CHOISISSEZ AVEC SOIN VOS MOTS DE PASSE

Entrer un mot de passe permettant de s'authentifier pour accéder à son ordinateur, sa tablette ou son téléphone portable est un geste quotidien de sécurité.
Choisir un mot de passe difficile à déceler par une tierce personne ou par du piratage informatique est ainsi un rempart efficace pour protéger ses données personnelles contre les intrusions frauduleuses.

Comment bien choisir son mot de passe ?

Définissez des mots de passe composés d'au moins 12 caractères

• mélangeant majuscules, minuscules, chiffres et caractères spéciaux
• n'ayant aucun lien avec vous comme votre nom, date ou lieu de naissance
• ne formant pas de mots figurant dans le dictionnaire

Comment faire en pratique ?

Pour cela 2 méthodes simples :
• la méthode phonétique : « J'ai acheté 5 CD pour cent euros cet après-midi » : ght5CD%E7am
• la méthode des premières lettres : « Un tiens vaut mieux que deux tu l'auras » : 1tvmQ2tl'A

Quelques recommandations supplémentaires

• n'utilisez pas le même mot de passe pour tout, notamment pour accéder à votre banque en ligne et votre messagerie personnelle ou professionnelle
• méfiez-vous des logiciels qui vous proposent de stocker vos mots de passe

2. ENTRETENEZ RÉGULIÈREMENT VOS APPAREILS NUMÉRIQUES

En mettant à jour régulièrement les logiciels de vos appareils numériques

Dans chaque système d'exploitation (Android, MacOS, Linux, Windows,…), logiciel ou application, des vulnérabilités existent. Une fois découvertes, elles sont corrigées par les éditeurs qui proposent alors aux utilisateurs des mises à jour de sécurité.
Sachant que bon nombre d'utilisateurs ne procèdent pas à ces mises à jour, les attaquants exploitent ces vulnérabilités pour mener à bien leurs opérations longtemps encore après leur découverte ou même leur correction. Il donc **nécessaire de procéder aux mises à jour régulières des logiciels.**

Comment faire ?

• configurez vos logiciels pour que les mises à jour de sécurité s'installent automatiquement chaque fois que cela est possible
• ou téléchargez les correctifs de sécurité disponibles en utilisant pour cela exclusivement les sites Internet officiels des éditeurs
• en effectuant couramment des sauvegardes

3. Effectuer des sauvegardes régulières (quotidiennes ou hebdomadaires par exemple) permet de disposer de ses données après un dysfonctionnement ou une panne d'ordinateur

Comment faire ?

• utilisez des supports externes tels qu'un disque dur externe, un CD ou un DVD enregistrable pour enregistrer et sauvegarder vos données.

4. PRENEZ SOIN DE VOS INFORMATIONS PERSONNELLES ET DE VOTRE IDENTITÉ NUMÉRIQUE

Les données que vous laissez sur Internet vous échappent instantanément.
Des personnes malveillantes récoltent vos informations personnelles, le plus souvent frauduleusement et à votre insu, afin de déduire vos mots de passe, d'accéder à votre système informatique, voire d'usurper votre identité ou de conduire des activités d'espionnage industriel.
Une grande prudence est conseillée dans la diffusion de vos informations personnelles sur Internet.

Voici quelques recommandations générales :

• soyez vigilant vis-à-vis des formulaires que vous êtes amenés à remplir : ne transmettez que les informations strictement nécessaires et pensez à décocher les cases qui autoriseraient le site à conserver ou à partager vos données, par exemple avec des partenaires commerciaux
• ne donnez accès qu'à un minimum d'informations personnelles sur les réseaux sociaux
• utilisez plusieurs adresses électroniques dédiées à vos différentes activités sur Internet : une adresse réservée aux activités dites sérieuses (banques, recherches d'emploi, activité professionnelle…) et une adresse destinée aux autres services en ligne (forums, jeux concours…)

5. PROTÉGEZ VOS DONNÉES LORS DE VOS DÉPLACEMENTS

L'emploi d'ordinateurs portables, d'ordiphones (*smartphones*) ou de tablettes facilite le quotidien lors des déplacements professionnels. Pourtant, voyager avec ces appareils nomades peut mettre en péril des informations sensibles sur l'entreprise ou vous travaillez.

Précautions à prendre avant de partir en mission

• utilisez le matériel dédié à la mission prêté par votre entreprise (ordinateur, clefs USB, téléphone)
• sauvegardez aussi vos données sur un support amovible pour les retrouver en cas de perte
• si vous comptez profiter des trajets pour travailler, emportez un filtre de protection écran pour votre ordinateur
• apposez un signe distinctif (comme une pastille de couleur) sur vos appareils pour vous assurer qu'il n'y a pas eu d'échange pendant le transport

Pendant la mission

• gardez vos appareils, supports et fichiers avec vous, pendant votre voyage comme pendant votre séjour (ne les laissez pas dans un bureau ou un coffre d'hôtel)
• si vous êtes contraint de vous séparer de votre téléphone, retirez la carte SIM et la batterie
• en cas d'inspection ou de saisie de votre matériel par des autorités étrangères, informez votre organisation
• n'utilisez pas les équipements que l'on vous offre si vous ne pouvez pas les faire vérifier par un service de sécurité de confiance
• évitez de connecter vos équipements à des postes qui ne sont pas de confiance. Par exemple, si vous avez besoin d'échanger des documents lors d'une présentation

6. SÉCURISEZ VOTRE WI-FI

Si l'utilisation du Wi-Fi est une pratique attractive, elle permet, lorsque le point d'accès n'est pas sécurisé, à des personnes malintentionnées d'intercepter vos données et d'utiliser votre connexion Wi-Fi à votre insu pour réaliser des opérations malveillantes.
C'est pour cette raison que l'accès à Internet par un point d'accès Wi-Fi est à éviter dans le cadre de l'entreprise.
Le Wi-Fi, solution pratique et peu coûteuse, peut cependant être le seul moyen possible d'accéder à Internet, il convient dans ce cas de sécuriser l'accès en configurant votre box. Pour ce faire, n'hésitez pas à contacter l'assistance technique de votre fournisseur d'accès.

Quelques recommandations générales :

• modifiez le nom d'utilisateur et le mot de passe par défaut (généralement « admin » et « 0000 ») de votre page de configuration accessible via votre navigateur Internet
• vérifiez que votre box dispose du protocole de chiffrement WPA2 et activez-le. Sinon, utilisez la version précédente WPA-AES (ne jamais utiliser le chiffrement WEP cassable en quelques minutes)
• modifiez la clé de connexion par défaut avec une clé (mot de passe) de plus de 20 caractères de types différents (cf. Choisissez des mots de passe robustes)
• ne divulguez votre clé de connexion qu'à des tiers de confiance et changez-la régulièrement
• activez et configurez les fonctions pare-feu / routeur.
• désactivez le Wi-Fi de votre borne d'accès lorsqu'il n'est pas utilisé

7. SÉPAREZ VOS USAGES PERSONNELS DES USAGES PROFESSIONNELS

Monsieur Paul, directeur commercial, rapporte souvent du travail chez lui le soir. Sans qu'il s'en aperçoive son ordinateur personnel a été attaqué. Grâce aux informations qu'il contenait, l'attaquant a pu pénétrer le réseau interne de l'entreprise de Monsieur Paul. Des informations sensibles ont été volées puis revendues à la concurrence.
Les usages et les mesures de sécurité sont différents sur les équipements de communication (ordinateur, ordiphone,…) personnels et professionnels.
Dans ce contexte, il est recommandé de séparer vos usages personnels de vos usages professionnels :
• ne faites pas suivre vos messages électroniques professionnels sur des services de messagerie utilisés à des fins personnelles
• ne stockez pas de données professionnelles sur vos équipements communicants personnels
En savoir plus sur le AVEC ou BYOD :
Le AVEC (Apportez Votre Equipement personnel de Communication) ou BYOD (Bring Your Own Device) est une pratique qui consiste, pour les collaborateurs, à utiliser leurs équipements personnels (ordinateur, ordiphone, tablette) dans un contexte professionnel. Si cette solution est de plus en plus utilisée aujourd'hui, elle est cependant très problématique pour la sécurité des données personnelles et professionnelles (vol ou perte des appareils, intrusions, manque de contrôle sur l'utilisation des appareils par les collaborateurs, fuite de données lors du départ du collaborateur).
De la même façon, il faut éviter de connecter des supports amovibles personnels (clés USB, disques durs externes) aux ordinateurs de l'entreprise.

8. SOYEZ AUSSI PRUDENT AVEC VOTRE ORDIPHONE (SMARTPHONE) OU VOTRE TABLETTE QU'AVEC VOTRE ORDINATEUR

Alexandre possède un ordiphone. Lors de l'installation d'une application, il n'a pas désactivé l'accès de l'application à ses données personnelles. Désormais, les éditeurs peuvent accéder à tous les SMS présents sur son téléphone.
Bien que proposant des services innovants, les ordiphones (smartphones) sont aujourd'hui très peu sécurisés. Il est donc indispensable d'appliquer certaines règles élémentaires d'hygiène informatique :
• n'installez que les applications nécessaires et vérifiez à quelles données elles peuvent avoir accès avant de les télécharger (informations géographiques, contacts, appels téléphoniques…). Certaines applications demandent l'accès à des données qui ne sont pas nécessaires à leur fonctionnement : il faut éviter de les installer
• en plus du code PIN qui protège votre carte téléphonique, utilisez un schéma ou un mot de passe pour sécuriser l'accès à votre terminal et configurez votre téléphone pour qu'il se verrouille automatiquement
• effectuez des sauvegardes régulières de vos contenus sur un support externe pour pouvoir les retrouver en cas de panne de votre ordinateur ou ordiphone

9. SOYEZ PRUDENT LORSQUE VOUS OUVREZ VOS MESSAGES ÉLECTRONIQUES

Suite à la réception d'un courriel semblant provenir d'un de ses amis, Madame Michel a cliqué sur un lien présent dans le message. Ce lien était piégé. Sans que Madame Michel le sache, son ordinateur est désormais utilisé pour envoyer des courriels malveillants diffusant des images pédopornographiques.
Les courriels et leurs pièces jointes jouent souvent un rôle central dans la réalisation des attaques informatiques (courriels frauduleux, pièces jointes piégées,…).

Lorsque vous recevez des courriels, prenez les précautions suivantes :
• l'identité d'un expéditeur n'est en rien garantie : vérifiez la cohérence entre l'expéditeur présumé et le contenu du message
• n'ouvrez pas les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que vous envoient habituellement vos contacts
• si un lien ou plusieurs figurent dans un courriel, vérifiez l'adresse du site en passant votre souris sur chaque lien avant de cliquer. L'adresse complète du site s'affichera alors dans la barre d'état en bas de la page ouverte. Si vous avez un doute sur l'adresse affichée, abstenez-vous de cliquer
• ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles (ex : code confidentiel et numéro de votre carte bancaire)
• n'ouvrez pas et ne relayez pas de messages de types chaînes de lettre, appels à la solidarité, alertes virales, etc.

10. SOYEZ VIGILANT LORS D'UN PAIEMENT SUR INTERNET

Lorsque vous réalisez des achats en ligne, vos coordonnées bancaires sont susceptibles d'être interceptées par des attaquants, directement sur votre ordinateur.
Ainsi, avant d'effectuer un paiement en ligne, il est nécessaire de procéder à des vérifications sur le site Internet :
• contrôlez la présence d'un cadenas dans la barre d'adresse ou en bas à droite de la fenêtre de votre navigateur Internet (remarque : ce cadenas n'est pas visible sur tous les navigateurs)
• assurez-vous que la mention « https:// » apparait au début de l'adresse du site Internet
• vérifiez l'exactitude de l'adresse du site Internet en prenant garde aux fautes d'orthographe par exemple
Si possible, lors d'un achat en ligne, privilégiez la méthode impliquant l'envoi d'un code de confirmation de la commande par SMS.
De manière générale, ne transmettez jamais le code confidentiel de votre carte bancaire.

11. TÉLÉCHARGEZ LES PROGRAMMES, LOGICIELS SUR LES SITES OFFICIELS DES ÉDITEURS

Si vous téléchargez du contenu numérique sur des sites Internet dont la confiance n'est pas assurée, vous prenez le risque d'enregistrer sur votre ordinateur des programmes ne pouvant être mis à jour, qui le plus souvent contiennent des virus ou des chevaux de Troie. Cela peut permettre à des personnes malveillantes de prendre le contrôle à distance de votre machine pour espionner les actions réalisées sur votre ordinateur, voler vos données personnelles, lancer des attaques, etc.

• C'est la raison pour laquelle il est vivement recommandé de télécharger vos programmes sur les sites officiels des éditeurs
• Enfin, désactivez l'ouverture automatique des documents téléchargés et lancez une analyse antivirus avant de les ouvrir, afin de vérifier qu'ils ne sont pas infectés par un quelconque virus ou spyware.

Réagissez à cet article

Original de l’article mis en page : Conseils aux usagers | Gouvernement.fr

---

Comment sécuriser Firefox efficacement en quelques clics de souris ?

Comment sécuriser Firefox efficacement en quelques clics de souris ?

Vous utilisez Firefox est vous souhaitez que cet excellent navigateur soit encore plus sécurisé lors de vos surfs sur Internet ? Voici quelques astuces qui supprimerons la géolocalisation, le profilage de Google ou encore que vos données offline disparaissent du regard d'espions locaux.

C'est sur le blog des Télécoms que j'ai vu pointer l'information concernant le réglage de plusieurs paramètres de Firefox afin de rendre le navigateur de la fondation Mozilla encore plus sécurisé. L'idée de ce paramétrage, empêcher par exemple Google de vous suivre à la trace ou de bloquer la géolocalisation qui pourrait être particulièrement big brotherienne.

Commençons par du simple. Il suffit de taper dans la barre de navigation de votre Firefox la commande about:config. Une alerte s'affiche, pas d'inquiétude, mais lisez là quand même. recherchez ensuite la ligne security.tls.version. Les valeurs affichées doivent osciller entre 1 et 3. Ensuite, recherchez la ligne geo.enabled pour annuler la géolocalisation. Passez le « true » en « False ». Pour que les sites que vous visitiez ne connaisse pas la dernière page que vous avez pu visiter, cherchez la ligne network.http.sendRefererHeader et mettre la valeur 1. Elle est naturellement placée à 2. Passez à False la ligne browser.safebrowsing.malware.enabled.

Ici, il ne s'agit pas d'autoriser les malwares dans Firefox, mais d'empêcher Google de vous tracer en bloquant les requêtes vers les serveurs de Google. Pour que Google cesse de vous profiler, cherchez la ligne browser.safebrowsing.provider.google.lists et effacez la valeur proposée.

Pour finir, vos données peuvent être encore accessibles en « offlire », en mode hors connexion. Cherchez les lignes offline-apps.allow_by_default et offline-apps.quota.warn. La première valeur est à passer en Fasle, la seconde valeur en 0.

Il ne vous reste plus qu'à tester votre navigateur via le site de la CNIL ou celui de l'Electronic Frontier Foundation.

Article original de Damien Bancal

Réagissez à cet article

Original de l'article mis en page : Sécuriser Firefox efficacement en quelques clics de souris – Data Security BreachData Security Breach

Victime d’une arnaque sur Internet ? Faites-nous part de votre témoignage

	Victime d’une arnaque sur Internet ? Faites-nous part de votre témoignage

Vous êtes victime d'une arnaque ou d'un piratage sur Internet ? Votre témoignage nous permettra peut-être de vous aider.

Devant une explosion de cas d'arnaques et de piratages par Internet et des pouvoirs publics débordés par ce phénomène, nous avons souhaité apporter notre pierre à l'édifice.
Vous souhaitez nous faire part de votre témoignage, contactez-nous.

Vous devez nous communiquer les informations suivantes (tout message incomplet et correctement rédigé ne sera pas traité) :

• une présentation de vous (qui vous êtes, ce que vous faites dans la vie et quel type d'utilisateur informatique vous êtes) ;
• un déroulé chronologique et précis des faits (qui vous a contacté, comment et quand et les différents échanges qui se sont succédé, sans oublier l'ensemble des détails même s'ils vous semblent inutiles, date heure, prénom nom du ou des interlocuteurs, numéro, adresse e-mail, éventuellement numéros de téléphone ;
• Ce que vous attendez comme aide (je souhaite que vous m'aidiez en faisant la chose suivante : ….)
• Vos nom, prénom et coordonnées (ces informations resteront strictement confidentielles).

Contactez moi
Conservez précieusement toutes traces d'échanges avec l'auteur des actes malveillants. Ils me seront peut-être utiles.

Réagissez à cet article

La sensibilisation des utilisateurs est la principale clé pour se protéger des pirates informatiques. Il n’est pas trop tard !

	La sensibilisation des utilisateurs est la principale clé pour se protéger des pirates informatiques. Il n’est pas trop tard !

La sensibilisation des utilisateurs est la clé pour se protéger des pirates informatiques

L'avis de Denis JACOPINI, Expert informatique assermenté spécialisé en cybercriminalité (arnaques, virus, phishing…) en Direct sur LCI le 23 mai 2016 dans l'émission « Ca nous Concerne » de Valérie Expert.

En mai 2016, Denis JACOPINI nous sensibilisait encore et déjà aux **cyber risques**.

Nos formations / nos sentibilisations
Toutes nos vidéos

LE NET EXPERT ET DENIS JACOPINI FONT DÉSORMAIS PARTIE DES PRESTATAIRES DE CONFIANCE DE LA PLATEFORME

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LE NET EXPERT

• **ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX ⇒ MISE EN CONFORMITÉ)**
- **ANALYSE DE VOTRE ACTIVITÉ**
- **CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES**
- **IDENTIFICATION DES RISQUES**
- **ANALYSE DE RISQUE (PIA / DPIA)**
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements

• **FORMATIONS / SENSIBILISATION :**
- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**

• **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES

• **EXPERTISES** & **AUDITS** (certifié ISO 27005)
- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Réagissez à cet article

Comment se préparer aux incidents de sécurité ?

	Comment se préparer aux incidents de sécurité ?

Les entreprises doivent être prêtes à agir face à des incidents de sécurité et à des attaques. Et cela passe notamment par sept points précis (par Peter Sullivan).

Un plan de préparation à la cybersécurité présente et détaille les objectifs fondamentaux que l'organisation doit atteindre pour se considérer comme prête à faire face à des incidents de sécurité informatique. La liste de contrôles qui va suivre n'est pas exhaustive, mais elle souligne des objectifs qui constituent un minimum requis pour donner un niveau raisonnable de sensibilisation à la cybersécurité et se concentrer sur la protection des actifs informationnels essentiels.
Ici, la préparation à la cybersécurité est définie comme l'état permettant de détecter et de réagir efficacement aux brèches et aux intrusions informatiques, aux attaques de logiciels malveillants, aux attaques par hameçonnage, au vol de données et aux atteintes à la propriété intellectuelle – tant à l'extérieur qu'à l'intérieur du réseau.
Un élément essentiel de cette définition est de « pouvoir détecter ». La détection est un domaine où une amélioration significative peut être atteinte en abaissant le délai de détection, couramment observé entre 9 et 18 mois. Une capacité de détection plus rapide permet de limiter les dommages causés par une intrusion et de réduire le coût de récupération de cette intrusion. Être capable de comprendre les activités régulières du réseau et de détecter ce qui diverge de la norme est un élément important de la préparation à la cybersécurité. Voici une sept objectifs que les entreprises devraient considérer.

Les objectifs à atteindre

1. Plan de cybersécurité
2. Gestion du risque
3. Gestion de l'identité
- **Contrôle d'accès**
- **Authentification**
- **Autorisation**
- **Responsabilité**

4. Surveillance de réseau
5. Architecture de sécurité
6. Contrôle des actifs, des configurations et des changements
7. Cartographie de la gestion des incidents
…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Se préparer aux incidents de sécurité*

Les bons réflexes contre les attaques informatiques | Denis JACOPINI

	Les bons réflexes contre les attaques informatiques

350 milliards d'euros par an : selon le McAfee Report on the Global Cost of Cybercrime publié en 2014, tel est le coût estimé des attaques informatiques à l'échelle mondiale.Depuis le début de l'année, les attaques se sont multipliées, notamment suite aux attentats de Charlie Hebdo, mettant plus que jamais en péril la sécurité des données des entreprises et des institutions. Un rapport publié le 16 février dernier par Kaspersky Lab a quant à lui révélé l'attaque d'une centaine de banques depuis 2013 par un gang organisé.

Afin d'appréhender au mieux ces offensives, il est important d'en comprendre les tenants et les aboutissants et d'avoir à l'esprit les réflexes qui permettent de s'en prémunir.

Des attaques aux motivations multiples

De plus en plus de sites internet sont victimes d'attaques dites de « défiguration » perpétrées par des hacktivistes revendiquant des convictions religieuses, politiques ou encore contestataires. On trouve également certains attaquants qui agissent uniquement pour l'amusement, mais ces scénarios se font de plus en plus rares. En général, seule la page d'accueil du site est modifiée pour signifier leur passage et évoquer leurs revendications.

On trouve également d'autres attaques qui, elles, sont plus furtives (ou en tout cas tentent de l'être) et consistent à voler des informations à des fins de rançonnage par exemple. Les vols de données bancaires (carte de crédit, numéros de comptes) permettent quant à eux du détournement d'argent, l'achat de services ou encore de matériels en ligne. Ces criminels, bien organisés, offrent des services de tout type à d'autres criminels : du kit d'infection, à l'envoi de spam massif, en passant par des serveurs de contrôle (c&c) pilotant des milliers de machines « zombies » permettant des attaques DDOS (Déni de service distribué). Tous n'ont pas le même niveau technique, certains ne sont d'ailleurs que des « presse-bouton », alors que d'autres ont la capacité de créer des virus, ou des programmes exploitant des failles de sécurité.

Mais comment s'y prennent-ils ? Ces malfaiteurs utilisent une faille de sécurité dans un programme qui peut provenir d'une erreur de conception (un protocole mal sécurisé par exemple), de programmation ou d'implémentation (failles connues comme shellshock, heartbleed ou ghost), de configuration (oubli du mot de passe par défaut après une installation) ou encore d'une erreur d'utilisation par une personne utilisant un mot de passe trop faible par exemple. L'humain est donc au centre de cette problématique.

Le plus souvent ces attaques débouchent sur du détournement d'argent ou la diffusion de données sur internet. Les conséquences financières pour les entreprises peuvent être considérables, sans compter l'impact que cela peut avoir sur l'image de l'entreprise victime d'un piratage. Dès lors, quels réflexes adopter face à ces diverses attaques et failles ?

Expert Informatique et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

Adopter les bonnes pratiques pour limiter les risques

Les attaques ne cessent de croître dans la mesure où l'enjeu financier pour les criminels est très important. Lorsque l'on sait que l'attaque par déni de service est accessible pour seulement 30 à 70 dollars la journée et qu'un spam ne revient qu'à 10 dollars par tranche d'1 million d'e-mails*, ce type de pratique n'est pas prêt de cesser. A ce premier enjeu s'ajoute le manque de vigilance dont font preuve les internautes. Le risque de s'infecter est en effet omniprésent : il suffit de cliquer sur un lien drainant un logiciel malveillant ou encore de partager un contenu infecté.

Quand bien même le risque zéro n'existe pas, la grande majorité de ces attaques pourrait être bloquée, dès lors que l'on adopte les bonnes pratiques pour se protéger et protéger autrui. Le maître mot est l'anticipation et la capacité à réagir rapidement en cas d'intrusion, la mise en œuvre d'un pare-feu ou d'un anti-virus pour se protéger n'étant pas suffisante. Le processus organisationnel de sécurisation est en effet plus important que les outils de protection eux-mêmes (on a en général un rapport de 80-20).

Pour ce faire, l'un des points majeurs est la gestion des mises à jour. Lorsqu'une faille tombe, celle-ci peut-être déjà exploitée plus ou moins massivement. S'en suit la douloureuse phase consistant à tester si le programme régresse ou non dans son fonctionnement avant une mise en production. Durant toute cette période, le programme est encore exposé à une potentielle exploitation de la faille. Cela sous-entend qu'il faut d'une part valider aussi vite que possible, et d'autre part essayer de se protéger temporairement avec des outils de type Firewall ou IPS. Il est aussi bon de rappeler que ces outils de protection sont aussi faillibles que les autres et qu'ils peuvent être contournés.

Dans le cas où l'attaque a déjà eu lieu, sur un site web par exemple, la première chose à faire est de bloquer le site. Cette phase est primordiale dans la mesure où un site piraté peut renvoyer des logiciels malveillants aux internautes le consultant. La deuxième étape est de sauvegarder tous les journaux, les données et programmes du site ainsi que la base de données, avant de procéder à une analyse du système pour connaître l'origine de l'attaque. Cette analyse est primordiale pour une remise en production du site. Elle permet de connaître par quel moyen les attaquants sont entrés dans le système et ce qu'il faut mettre à jour. Le mieux est de revenir sur une version de sauvegarde dont on est sûr qu'elle n'a pas été affectée par la compromission et de la mettre à jour. Parallèlement, il est également vivement conseillé de porter plainte afin que ces attaques soient référencées par les autorités et que des mesures soient prises.

S'il est crucial de prendre en compte la problématique de sécurité lors de la création d'un projet informatique, il est tout aussi indispensable d'en assurer la maintenance afin d'anticiper les attaques et de pouvoir les gérer efficacement, et ainsi minimiser leur impact sur l'activité de l'entreprise.

Expert Informatique et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.journaldunet.com/solutions/expert/60082/attaques-informatiques-decryptage-du-phenomene-et-reflexes-a-adopter.shtml
Par Sébastien Delcroix – NFrance

Les objets connectés représentent-ils un risque ? | Denis JACOPINI

Les #objets connectés représentent-ils un risque ?

Contrôler sa maison ou son appartement du bout des doigts, voici la promesse des fameux objets connectés. Des réfrigérateurs aux télévisions, en passant par les thermostats, les caméras de surveillance, les serrures, ou encore les éclairages… de plus en plus d'équipements du foyer peuvent être pilotés à distance à l'aide d'un smartphone via un réseau local et Internet. Mais derrière ce rêve de la maison intelligente et connectée, encore inimaginable il y a quelques années, se cachent d'inquiétants problèmes de sécurité. État des lieux.

Un marché en ébullition

Longtemps réservée aux technophiles fortunés, la domotique commence vraiment à se démocratiser grâce à l'émergence des appareils et objets connectés. Après les équipements multimédias (Smart TV, systèmes Hi-Fi, imprimantes…), les appareils électroménagers connectés – réfrigérateurs, lave-linge, cafetières, réveils, etc.– commencent à débarquer sur le marché. Mais ce sont surtout les systèmes prêts à l'emploi ou les modules adaptables permettant de connecter l'éclairage, les serrures de portes, les stores, les systèmes de surveillance (caméras, détecteurs de mouvements/fumée, alarmes…), ou encore le chauffage qui rencontrent un succès grandissant.
L'embellie du marché de la domotique s'explique notamment par la simplicité d'installation et d'usage de ces nouveaux produits, mais également par leur prix de plus en plus abordable. Toutefois, comme n'importe quel appareil qui se connecte à un réseau Wi-Fi et à Internet, ils s'exposent de fait à toutes sortes de risques. D'autant que pour la plupart, ils ne possèdent aucun système de protection de type antivirus, antimalware, etc. Des failles de sécurité, plus ou moins importantes en fonction de la nature des objets, ont été soit démontrées par des experts de sécurité, soit exploitées par des hackers. Nous verrons les cas les plus effrayants qui donnent matière à réflexion.

[-]

Des appareils sous haute surveillance

Outre les incidents révélés ici et là, la sécurité des objets connectés est devenue un sujet particulièrement sensible depuis la médiatisation d'un moteur de recherche public étonnant baptisé Shodan. Créé par un Américain du nom de John Matherly, ce dernier explore le Web en continu pour référencer et regrouper tous les appareils qui y sont connectés. Quelques clics suffisent pour trouver aussi bien des systèmes domotiques, que des imprimantes, des caméras, des alarmes, voire des installations industrielles sensibles telles que des centrales électriques, des raffineries, ou encore, des réacteurs.

Pas de quoi rassurer les utilisateurs, même si à l'origine Shodan n'aurait pas été créé pour nuire, mais au contraire pour aider les experts en sécurité à identifier les vulnérabilités des logiciels et infrastructures réseau des entreprises. Le service se targue de garder une trace de tous les faits et gestes de ses utilisateurs, qui doivent obligatoirement s'identifier et souscrire à un abonnement au-delà d'un certain nombre de recherches. Il n'en reste pas moins que désormais, tout objet connecté ayant une adresse IP peut être localisé, identifié, voire détourné.

Les promesses de la maison intelligente et connectée

Contrôler et gérer divers équipements de la maison à l'aide d'un smartphone, d'une tablette ou d'un ordinateur n'est plus une utopie. Inutile d'avoir à tirer des câbles partout et d'entreprendre de lourds et coûteux travaux avec des spécialistes. Tout le monde peut en principe concevoir une installation domotique soi-même grâce à la nouvelle génération de produits disponibles sur le marché. Au-delà du confort qu'offrent ces nouvelles technologies au quotidien, elles permettent de réaliser de substantielles économies d'énergie, de renforcer la sécurité du foyer, ou encore de se prémunir d'accidents domestiques (incendie, inondation…).

[-]

Confort, sécurité, prévention, économie d'énergie…

Domotique

Les produits ont évolué, mais la promesse de la domotique est toujours la même : centraliser et automatiser grâce à diverses technologies l'ensemble ou une partie des équipements électriques du foyer. Des serrures qui se ferment à distance, des caméras et des détecteurs de mouvements capables de s'animer en votre absence et de vous envoyer des SMS en cas d'intrusion, des thermostats intelligents permettant de gérer la température au degré près dans chaque pièce, des stores électriques qui s'ouvrent et se ferment automatiquement en fonction de la lumière, des détecteurs de fumée (obligatoires dans toute l'Union européenne à partir de mars 2015) qui lancent des alertes en cas de départ d'incendie, des éclairages qui créent différentes ambiances lumineuses selon les heures de la journée… Les possibilités sont quasi-infinies.

Réaliser une installation domotique est maintenant à la portée du plus grand nombre grâce, notamment, à ce qu'on appelle les box domotiques. Ces systèmes prêts à l'emploi que l'on trouve dans tous les magasins de bricolage et d'électronique (Castorama, Leroy Merlin, Electro Dépôt…) et même dans certains hypermarchés permettent de connecter et de contrôler à distance des équipements de la maison via une seule et même interface. Ces packs se composent d'un serveur domotique / multimédia (relié au réseau Wi-Fi du foyer), et d'un éventail plus ou moins important d'équipements de surveillance, d'automatisation, de loisirs, etc.

[-]

Ces dispositifs communiquent entre eux par le biais de différentes technologies sans fil comme le courant porteur (CPL), le Wi-Fi, les radiofréquences, ou des protocoles propriétaires. Pour les contrôler à l'aide d'une tablette ou d'un smartphone depuis le réseau local du foyer ou à distance par Internet, l'utilisateur n'a plus qu'à jouer du bout des doigts avec les icônes représentant les équipements connectés pour planifier des actions immédiates ou différées.

[-]

Créer des scénarios

Dans le jargon de la domotique, un scénario désigne un ensemble d'actions programmées pour différents moments de la journée, de la semaine, du mois, voire de l'année. Les fabricants ont réalisé d'énormes progrès pour faciliter la gestion des produits domotiques et la création de scénarios en développant des applications très intuitives. Exit les lignes de code informatique, ou les menus interminables au vocabulaire incompréhensible, place aux icônes visuelles, aux photomontages représentant les différentes parties du foyer, et à des menus dynamiques inspirés de ceux des smartphones. Quelques clics suffisent pour créer plusieurs scénarios pour la journée, la nuit, le week-end, et les combiner entre eux.

[-]

Point d'orgue des maisons intelligentes, les applications mobiles facilitent la compréhension et l'utilisation des équipements domotiques

On peut imaginer, par exemple du lundi au vendredi, un scénario qui consisterait à déclencher une série d'actions à partir de 7 heures : ouvrir les stores, allumer le ballon d'eau chaude, faire chauffer la cafetière, lancer la radio, déverrouiller les portes, démarrer les caméras de surveillance, etc. Bien entendu, toutes les solutions domotiques n'offrent pas les mêmes possibilités. Les fabricants distillent généralement des packs spécialisés dans un domaine précis (surveillance, automatisation, éclairage, chauffage…) à compléter au fur et à mesure. En parallèle, il existe d'innombrables objets connectés autonomes (stations météo, balances Wi-Fi, réveils intelligents, ampoules connectées…) qui se connectent directement au réseau du foyer, sans passer par un serveur propriétaire.

[-]

Aura, le réveil intelligent de Withings qui analyse votre sommeil pour vous réveiller en douceur

Le problème, c'est que tout ce petit monde ne parle pas le même langage. Les standards universels, que rêvent de concevoir Apple et Google pour que tous les appareils connectés puissent communiquer entre eux via leurs plateformes mobiles respectives, ne sont pas encore d'actualité. À moins de choisir du matériel très haut de gamme comme la box universelle Lifedomus Vision (2 988 euros) compatible avec la plupart des protocoles de communication des solutions domotiques (KNX, EnOcean, MyHome, Zwave, Modbus, Zigbee…), mieux vaut s'équiper chez le même fabricant pour pallier les éventuels problèmes de compatibilité.

[-]

Quels risques pour la sécurité ?

Depuis quelques mois, le sécurité de l'Internet des objets fait couler beaucoup d'encre. Aux quatre coins de la planète, des experts en sécurité prennent le sujet à bras le corps : ils multiplient les démonstrations pour montrer les vulnérabilités de certains produits et la façon dont les cybercriminels pourraient les exploiter pour réaliser des attaques. Les spécialistes n'ont pas tort d'alerter les fabricants, car les risques ne sont plus seulement virtuels. Depuis quelques mois, quelques cas concrets d'attaques basées sur des objets connectés prouvent le bien-fondé de leurs craintes.

[-]

Failles et vulnérabilité des objets connectés

La division de sécurité Fortify on Demand du constructeur HP a récemment publié un rapport alarmant sur la sécurité des objets connectés. Elle a ainsi annoncé avoir découvert plus de 25 vulnérabilités sur 10 objets connectés parmi les plus populaires (Smart TV, thermostats intelligents, webcams, boxs domotiques…). Sans donner plus de précisions sur les marques concernées, elle déclare que la plupart ne crypte pas les données échangées sur le réseau et n'exige pas de mot de passe sécurisé mêlant caractères spéciaux et chiffres pour l'accès à distance. Ces dispositifs autorisent des mots de passe comme « 123456 » particulièrement vulnérables (un fait que nous avons effectivement pu vérifier après quelques recherches sur Shodan). Par ailleurs, la protection de leurs logiciels serait insuffisante, car non chiffrée, et certaines interfaces Web ne sont pas du tout sécurisées.

Toujours selon ce rapport, 90 % des produits évalués collectent des informations personnelles sensibles (adresse email/postale, date de naissance…) susceptibles de circuler en clair sur Internet à cause du manque de protection. Difficile néanmoins de contester un rapport ne précisant pas les modèles et les marques des appareils incriminés. À travers cette étude, la division déclare vouloir sensibiliser les acteurs du marché, mais elle souhaite aussi promouvoir sa solution de sécurité Fortify on Demand auprès des fabricants.

[-]

Ce n'est pas la seule étude de ce type. Le groupe de chercheurs indépendant d'AV-Test avait mis en lumière d'importantes failles de sécurité, notamment sur les systèmes domotiques iComfort de REVRitter, et XAVAX MAX ! d'Hama, permettant de contrôler le chauffage, l'électricité, les prises de courant avec interrupteur, ou encore l'éclairage. Aussi incroyable que cela puisse paraître, leur communication n'était pas sécurisée sur le réseau lors des mises à jour logicielle ou firmware, mais en plus, la solution iComfort ne nécessitait aucune authentification que cela soit pour l'accès local ou via Internet.

Avec un moteur de recherche comme Shodan, n'importe qui aurait pu repérer les dispositifs de la marque sur Internet et en prendre le contrôle à distance… Effrayant. Gageons que les deux fabricants ont pris les mesures qui s'imposent pour sécuriser un tant soit peu leurs systèmes.

Le lapin Karotz sécurisé ? Pas tout à fait.

Dans la sécurité informatique, les experts réalisent des « exploits », c'est-à-dire des tests (appelés Proof-of-concept, preuve de concept) visant à démontrer la présence de vulnérabilités sur des systèmes ou des logiciels pour proposer des patchs. Certains exemples sont particulièrement croustillants. La spécialiste Jennifer Savage avait ainsi montré comment elle avait réussi à exploiter une faille de sécurité du fameux lapin multifonctions Karotz qu'elle avait offert à sa fille. Cela lui avait permis de prendre le contrôle à distance de l'appareil à son insu, à l'aide d'un ordinateur, et d'utiliser sa caméra et son micro pour l'espionner.

[-]

Des ampoules qui éclairent et déverrouillent les réseaux Wi-Fi

Plus récemment, des chercheurs sont parvenus à prendre le contrôle d'ampoules connectées Lifx en exploitant une faille de leur protocole de communication. Ils ont pu démontrer qu'ils pouvaient théoriquement s'introduire dans un rayon de 30 mètres dans le réseau Wi-Fi domestique auquel elles sont connectées et accéder à des données privées stockées sur d'autres appareils du foyer, par exemple. Depuis cette découverte, le fabricant s'est empressé de publier un correctif.

[-]

Des Smart TV qui espionnent les téléspectateurs

Les démonstrations les plus impressionnantes ont souvent lieu lors des conférences Black Hat organisées chaque année à Las Vegas, mais aussi à Amsterdam ou à Tokyo. Elles réunissent aussi bien des chercheurs, des experts en sécurité, que des hackers de haut vol. En 2013, plusieurs conférenciers ont exposé les vulnérabilités des TV connectées. L'un d'entre eux a prouvé notamment qu'il était possible de prendre le contrôle de la caméra et du micro d'une Smart TV et d'espionner leur propriétaire à leur insu. Et cela, même quand l'appareil était éteint.

Le thermostat Nest lub qui joue les « Big Brother »

À l'occasion de la dernière édition qui s'est déroulée au mois d'août 2014 à Las Vegas, des chercheurs d'une université de Floride ont montré comment pirater le thermostat intelligent de Nest (la start-up rachetée par Google). Avec un accès physique à l'appareil (uniquement), ils ont pu prouver qu'il est possible d'insérer un code pour détourner et récupérer les informations récoltées par l'appareil, sans que son propriétaire s'en aperçoive.

[-]

Nouvelle génération de cyberattaques

La sécurité et la protection des données privées ne sont clairement pas la priorité de certains acteurs du marché des objets connectés. Sans vouloir dresser un tableau catastrophique de la situation, les cyberattaques sur les objets connectés présentant des failles de sécurité ont tendance à se multiplier ces derniers mois. Caméras de vidéosurveillance, réfrigérateurs, babyphones, Smart TV, voici quelques exemples connus d'appareils qui ont fait l'objet d'attaques diverses et variées.

Des caméras au service des voyeurs

Impossible de ne pas citer la faille de sécurité qui avait permis à des hackers de diffuser sur Internet le flux vidéo de milliers de webcams et caméras de vidéosurveillance Trendnet, installées chez des particuliers. Malgré la publication rapide d'un correctif par le fabricant après sa découverte, de nombreux utilisateurs continuaient un an plus tard à être espionnés à leur insu, car ils n'avaient toujours pas fait la mise à jour.

[-]

Un hack jusque dans… le berceau d'un nourrisson !

Début 2014, la société spécialisée en sécurité PodPoint a révélé pour la première fois une cyberattaque réalisée à partir de toutes sortes de dispositifs connectés dont des Smart TV, des NAS, des consoles de jeux vidéo, un réfrigérateur, etc. Les pirates auraient exploité leur vulnérabilité pour installer un serveur de spams (botnet) et envoyer plus de 750 000 emails frauduleux. Dans l'Etat de l'Ohio aux Etats-Unis au mois d'avril dernier, un hacker n'a rien trouvé de mieux que de pirater un babyphone pour terroriser un bébé et ses parents. En prenant le contrôle de l'appareil équipé d'une caméra, d'un micro et d'un haut-parleur, il s'est mis à hurler des insanités sur le nourrisson.

[-]

Analyse et collecte de données en règle

En Grande-Bretagne, le bloqueur spécialisé en développement informatique connu sous le nom de DoctorBeet's a fait une étonnante découverte. Suite à l'acquisition d'une Smart TV de la marque LG, il a remarqué l'apparition de publicités ciblées comme on peut en voir sur des services Web tels que Gmail. Il en a donc déduit que la TV devait forcément analyser ses habitudes, les programmes qu'il regarde, les sites qu'il visite, etc. En cherchant à en savoir plus, il constate en effet que son téléviseur dispose d'une fonction activée par défaut de collecte d'informations de visionnage.

Même après avoir désactivé cette fonction, le téléviseur continuait de transmettre des informations à son insu à LG. Le constructeur ne se contentait pas de scruter ses habitudes de consommation, mais il récupérait également des données personnelles telles que des vidéos de famille qu'il avait projetées sur son écran depuis son ordinateur. Un scandale dont se serait bien passé LG qui aurait, depuis, décidé de permettre à ses clients de « vraiment » désactiver l'option de collecte de données. Outre le manque de sécurité constaté sur de nombreux objets connectés, il faudra donc aussi dorénavant se méfier des pratiques intrusives de certains fabricants !

[-]

Source DoctorBeet's Blog

Sous l'œil de Shodan

En faisant un tour d'horizon des objets connectés pour la maison, susceptibles de présenter des risques, on se rend compte qu'ils sont tous potentiellement vulnérables. Certains ne sont pas sécurisés ou pas suffisamment, tandis que d'autres présentent des failles de sécurité plus ou moins importantes pouvant être exploitées pour mener des attaques externes ou à courte distance. Mais la principale faille qu'exploitent les hackers est encore trop souvent l'absence de vigilance des utilisateurs. Beaucoup n'ont pas conscience des risques et n'utilisent pas de mots de passe pour protéger l'accès à distance de leurs équipements, ou se contentent de laisser les identifiants par défaut fournis par les fabricants. Un vrai problème, d'autant qu'avec un moteur de recherche comme Shodan, tous les appareils connectés ayant une adresse IP visible sont désormais répertoriés sur le Web.

D'une efficacité redoutable, ce service permet d'effectuer des recherches globales, ou par pays, en saisissant une simple requête pour identifier, localiser, voire prendre le contrôle des appareils connectés non protégés par un mot de passe. Il suffit de saisir le nom d'une marque de produits connectés connue (DLink, Netgear, Samsung…) ou de cliquer sur les mots recherchés les plus populaires (Webcam, Camera, Netcam…) pour voir apparaître leurs adresses IP et s'y connecter. Le service indique de surcroît de nombreux détails sur les dispositifs, comme leur système d'exploitation, s'ils sont connectés, protégés ou non par des identifiants, etc.

[-] [-]

Comme cela avait été démontré dans une enquête baptisée Null CTRL, réalisée par deux journalistes norvégiens pour le site Dagbladet en 2013, d'innombrables équipements connectés référencés par Shodan ne possèdent aucune protection. Quelques clics suffisent pour les repérer et visionner, par exemple, le flux vidéo de caméras de surveillance chez des particuliers, jouer avec le tableau électrique ou le thermostat d'un immeuble, s'introduire dans des bases de données, etc. Gageons qu'à terme, cette surexposition des objets connectés permette de sensibiliser les utilisateurs sur l'importance de sécuriser leur accès.

[-]

Qu'en pensent les experts ?

Au-delà des rapports alarmants, des exploits des chercheurs et des affaires relatées dans les médias, nous avons souhaité donner la parole à un expert en sécurité ainsi qu'à un fabricant de solutions domotiques. Tous deux apportent une vision concrète sur les risques que représentent les objets connectés à l'heure actuelle, et donnent quelques conseils aux utilisateurs pour mieux se protéger.

[-]

Cybermenaces sur les maisons intelligentes

Pour en savoir un peu plus sur les menaces qui planent sur les maisons intelligentes et leurs installations domotiques, nous avons rencontré un expert en sécurité qui travaille depuis plus de dix ans pour Kaspersky Lab Angleterre. Il dresse un portrait plus nuancé que celui des cabinets d'experts en sécurité que nous avons évoqué précédemment.

[-]

David Emm

Clubic : Que pouvez-vous nous dire sur la sécurité des objets connectés pour la maison ?

David Emm : Les gens utilisent Internet pour faire des achats, gérer leurs comptes en banque, aller sur les réseaux sociaux mais aussi pour chercher des informations liées à tous les aspects de leur vie quotidienne. Et cela va encore plus loin maintenant que nous utilisons les technologies informatiques pour réaliser des actions qui étaient, par le passé, purement mécaniques, voire manuelles. Malheureusement, lorsque de nouvelles technologies voient le jour, ou lorsque la technologie génère de nouveaux usages, la sécurité n'est souvent pas l'une des priorités. Ce n'est pas un phénomène nouveau et si l'on regarde en arrière, on remarque que les évolutions sont portées par une volonté de simplicité, de réduction des coûts ou d'autres bénéfices, alors que la sécurité n'est envisagée qu'après l'émergence d'un problème. Les risques sont multiples, allant du vol à la manipulation des données. Il est facile d'imaginer par exemple qu'un compteur intelligent soit manipulé pour falsifier la consommation électrique. Pour l'instant, cela reste de l'ordre du possible plus que de celui du réel car à ma connaissance il n'y a eu aucune attaque réelle visant des compteurs électriques.

Clubic : Selon vous, quels sont les types d'appareils domotiques les plus vulnérables ?

David Emm : Lorsqu'ils entendent parler de l'Internet des objets ou de maisons intelligentes, la plupart des gens imaginent leurs appareils traditionnels disposant de nouvelles fonctionnalités (réfrigérateur, contrôle des portes, chauffage central, etc.). Pourtant, ces appareils ne sont pas encore massivement connectés et pour l'instant, leur vulnérabilité a été démontrée le plus souvent au travers d'exploits d'experts dans le cadre de tests. Bien sûr, lorsque ces appareils seront plus courants dans nos vies, je pense qu'ils deviendront régulièrement la cible d'attaques. Mais il faut surtout s'inquiéter de la vulnérabilité d'appareils qui sont aujourd'hui des incontournables, comme par exemples les modems Internet, les tablettes, les smart TV, etc.

Clubic : À quel type d'attaques les maisons intelligentes (Smart Home) sont-elles exposées ?

David Emm : Je dirais qu'il y a trois principales catégories :
1 – Obtenir l'accès à un appareil et l'utiliser pour prendre le contrôle d'autres systèmes connectés dans la maison
2 – Avoir accès à des informations privées ou sensibles, y compris des mots de passe
3 – Falsifier des informations reçues / envoyées par un appareil à l'insu des personnes du foyer

Clubic : Quelles sont les vulnérabilités que vous avez pu constater ?

David Emm : L'un de mes collègues David Jacoby a publié un rapport pour alerter sur les dangers de l'exécution de code à distance et des mots de passe faibles sur les appareils de stockage NAS, mais aussi la possibilité d'orchestrer une attaque de type « man-in-the-middle » (NDRL : l'attaque de « l'homme du milieu » consiste à s'infiltrer sans être vu dans un réseau et y intercepter des informations) via une Smart TV. Il a également découvert des fonctionnalités d'analyses non référencées intégrées dans les routeurs par les constructeurs (sans doute pour des raisons légitimes), mais qui pourraient être exploitées par un attaquant. Un appareil sans fil est repérable et potentiellement vulnérable aux attaques lorsque ses communications ne sont pas cryptées, et que le mot de passe d'accès utilisé est celui par défaut ou faible.

Clubic : Est-ce que Kaspersky envisage de proposer des solutions de sécurité pour les objets connectés ?

David Emm : Ce n'est pas parce qu'il est possible d'installer une solution de sécurité sur les terminaux traditionnels (PC, tablettes, smartphones…), que cela sera possible sur tous les appareils du quotidien qui sont connectés à Internet. Ces appareils pourraient recevoir et envoyer des données sans pour autant autoriser l'installation de code ou disposer de suffisamment d'espace pour le faire. Ils pourraient être verrouillés (par exemple si une Smart TV tourne sous un OS standard, il est possible que le code ne puisse être modifié que par le constructeur). En plus, le vendeur n'est pas toujours le constructeur des composants informatiques intégrés. Cela signifie qu'il pourrait être impossible de patcher ces appareils, même en cas de mise à jour de sécurité disponible via le constructeur des composants. On comprend mieux pourquoi il est primordial que les constructeurs d'appareils et les entreprises qui les exploitent prennent en compte la sécurité dès le début de la fabrication d'un produit. Il est essentiel de pouvoir établir un dialogue entre experts en sécurité et développeurs d'appareils informatiques pour maisons connectées.

Clubic : Que peuvent faire les utilisateurs pour protéger au mieux leurs systèmes domotiques ?

David Emm : La première chose est de lister tous les objets connectés de la maison et de savoir comment et à quoi ils sont connectés (à Internet, ou à d'autres objets de la maison). Ensuite, il est impératif de mettre des obstacles sur la route du hacker. Pour ce faire, il faut tout d'abord installer régulièrement les mises à jour de sécurité et les mises à jour logicielles, pour limiter le nombre de vulnérabilités connues qui pourraient être exploitées. Après, il faut changer le nom et le mot de passe par défaut de chaque objet connecté, car c'est la première chose qu'un hacker tentera d'attaquer pour en prendre le contrôle. Pour finir, il faut limiter l'accès d'un objet connecté aux autres objets connectés dans la maison. Par exemple, si vous avez une Smart TV, vous devrez restreindre l'accès à cette TV et autoriser seulement son accès à des ressources particulières du réseau (il n'est pas vraiment nécessaire que votre imprimante soit connectée à votre TV, par exemple…).

Clubic : Selon vous, quel serait LE scénario catastrophe pour une maison intelligente ?

David Emm : C'est une question difficile, car LE scénario catastrophe impliquant un seul individu n'aura pas forcément le même impact au niveau d'une communauté. Pour les individus, le risque qui importe c'est le #vol de données personnelles – par exemple, les noms d'utilisateurs, les mots de passe, etc. Ou encore, le fait que l'on puisse vous espionner vous ou votre famille (comme le hack du babyphone survenu dans l'Etat de Ohio). Il y aussi le risque qu'une application contrôlant la sécurité de votre porte d'entrée puisse être hackée, vous laissant enfermé dehors. Du point de vue de la communauté, l'impact peut être plus important. Si un hacker arrive par exemple à intercepter des données d'un compteur intelligent (Smart Meter), cela peut affecter les relevés : il peut remettre les compteurs à zéro, voire créer une panne générale d'électricité.

[-]

Le point de vue d'un spécialiste de la domotique

Pour compléter ce dossier, nous avons voulu donner également la parole à un fabricant de solutions domotiques. Somfy, l'un des leaders du marché de la domotique, a bien voulu répondre à nos questions sur la sécurité des maisons intelligentes.

[-]

Clubic : Comment la box Somfy et les appareils qu'elle permet de piloter à distance sont-ils protégés ?

Somfy : En tant que spécialiste de solutions domotiques, notre box prend en compte les problématiques de sécurité. L'ensemble des actions effectuées avec nos solutions Tahoma et Somfy Box transite sur un serveur sécurisé et est chiffré sur 128 bits. Le protocole RTS propriétaire de Somfy (10 millions de systèmes installés dans le monde) qui est utilisé pour la commande radio est sécurisé grâce à un code tournant de 16 millions de combinaisons.

Clubic : En tant que fabricant, que pensez-vous du remous médiatique autour de la vulnérabilité supposée ou avérée de certains objets connectés pour la maison ?

Somfy : Nous sommes aujourd'hui en plein boom des objets connectés, avec de nombreux nouveaux acteurs qui lancent parfois des solutions un peu trop vite et pas suffisamment abouties. Il faut veiller à bien se renseigner sur le fabricant et sa légitimité sur le secteur. Somfy possède une expertise en matière de radio et d'IP qui nous rend légitimes sur ce secteur. Depuis que nous avons lancé notre box il y a quatre ans, aucun piratage ne nous a été signalé.

Clubic : Quels sont selon vous les points faibles d'une installation, ou quels pourraient-ils être ?

Somfy : Les points faibles de l'installation seraient de ne pas avoir de système de protection, d'avoir positionné les détecteurs de mouvements aux mauvais endroits ou de ne pas couvrir tous les accès de la maison.

Clubic : Selon vous, quel serait LE scénario catastrophe pour une maison intelligente ?

Somfy : Le scénario catastrophe, s'il y en a un, serait de se faire voler son téléphone sans code pour le déverrouiller en laissant ainsi libre accès à l'application qui commande la maison intelligente. Il faut donc prendre les précautions nécessaires.

Conclusion

En moins de deux ans, la domotique est passée d'un marché de niche à un nouvel eldorado convoité par la plupart des géants de l'industrie high-tech. Apple, Google, Microsoft ou encore Samsung, pour ne citer qu'eux, se sont lancés tour à tour sur ce marché promis à une très forte croissance en multipliant les partenariats et les rachats de start-up spécialisées. Début 2014, Google n'a pas hésité par exemple à faire la troisième acquisition la plus importante de son histoire, en rachetant Nest Labs pour la bagatelle de 3,2 milliards de dollars et, plus récemment, le spécialiste de caméras IP Dropcam pour 555 millions de dollars.

Courant 2014, Samsung s'est offert la start-up spécialisée SmartThings (montant de l'achat non divulgué), Microsoft a noué un partenariat avec Insteon, un des leaders de la domotique aux USA, et Apple a dévoilé à l'occasion de la WWDC la plateforme HomeKit pour iOS8 qui permettra de contrôler les objets connectés de nombreux fabricants via Siri (l'assistant vocal d'Apple). En attendant les solutions des poids lourds des nouvelles technologies, le marché est déjà bien occupé par les acteurs historiques – Somfy, Philips, Haier, Legrand, etc. –, une foule de nouveaux fabricants de tous horizons, des fournisseurs d'électricité ou encore des opérateurs comme Orange et SFR, qui commercialisent en France des kits de domotique pour accompagner leurs box. Si tout ce monde frappe à la porte de nos foyers, c'est que le potentiel est énorme.

[-]

Il ne fait aucun doute que les produits du quotidien vont être de plus en plus connectés (comme nous avons pu le voir au CES cette année), mais pas toujours bien sécurisés. Les acteurs comme Google, Apple et Microsoft, qui ambitionnent qu'un maximum d'objets connectés puissent fonctionner à l'avenir avec leurs plateformes mobiles respectives, vont sans doute imposer aux fabricants un cahier des charges drastique en matière de sécurité s'ils veulent obtenir une certification. Cela pourrait peut-être permettre d'augmenter le niveau de protection des objets connectés, même si comme nous l'avons vu, il n'est pas toujours possible de patcher des produits comprenant des composants provenant de différents fabricants.

Le nombre croissant d'objets connectés risque d'intéresser de plus en plus les cybercriminels pour entreprendre des diffusions de spams ou de logiciels malveillants à grande échelle, par exemple. Mais le plus effrayant serait qu'ils puissent prendre le contrôle total des maisons intelligentes, espionner leurs habitants à l'aide des caméras de surveillance, s'introduire ni vu ni connu dans le foyer en déverrouillant la porte à l'aide d'un smartphone, couper l'électricité ou le chauffage en plein hiver, ou encore, déclencher l'alarme au beau milieu de la nuit…

Pour que les maisons intelligentes tiennent vraiment toutes leurs promesses, il est indispensable qu'à l'avenir leur sécurité soit garantie. En attendant, côté utilisateur, il faudra être de plus en plus vigilant, se renseigner sur le système de protection des produits, faire systématiquement les mises à jour, ou encore instaurer un mot de passe fort pour l'accès à distance de tous les appareils connectés. Le prix à payer pour que le rêve de posséder une maison intelligente ne tourne pas au cauchemar.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : #http://www.clubic.com/antivirus-securite-informatique/article-723729-1-objets-connectes-representent-risque.html
Par Jérôme Cartegini