LA PROTECTION RAPPROCHÉE DES DONNÉES

Les règles de **sécurité informatique** pour les PME/PMI

AVIS D'EXPERT

Jonathan Azria
Malware Specialist
ATHENA Global Services

www.athena-gs.com

SOMMAIRE

PRD – Protection rapprochée des données :

La paranoïa comme seule solution de défense ?

Jonathan Azria, Consultant Sécurité chez Athena Global Services, Malware Specialist pour ESET France

Les données informatiques, objets de discordes et de convoitises binaires, font aujourd'hui vivre la majeure partie des entreprises. En effet, les sociétés de toutes tailles voient les différents éléments les constituant reposer sur l'informatique. Parmi ces éléments : la comptabilité, la gestion des ventes, la représentation de ces entreprises via des sites vitrines, ainsi que la commercialisation de leurs produits à travers des sites marchands et bien plus encore. Certaines entreprises n'existent même que sur l'Internet.

Les nouvelles tendances technologiques et plus particulièrement la simplification de mise en œuvre matériels et logiciels de ces solutions, telles que les services de « Cloud » et les « CMS » (Système de gestion de contenu) permettent aujourd'hui à la plus petite entreprise d'être présente sur la toile sans la moindre difficulté et presque sans connaissance informatique. La « Vulnérabilité » suit-elle la même tendance en devenant plus accessible ? Peut-on désormais s'inviter sur l'Internet sans en connaître les codes et sans recourir à un investissement conséquent pour protéger ses données ? Quels sont les risques auxquels nous nous exposons en ne prêtant pas attention aux règles élémentaires de sécurité ?

Répondre à ces questions pourrait sembler inutile, pour peu que l'on suive l'actualité. Personne, en effet, ne peut prétendre être à l'abri de voir ses données diffusées sur la toile ou d'avoir ses ordinateurs infectés par des « malwares ». Les attaques ciblent pour la plupart des victimes de façon aléatoire, il est donc inutile d'essayer de se voiler la face ou de ne pas se sentir concerné. Néanmoins certaines règles de bonnes conduites et politiques de sécurité permettent de réduire considérablement les risques. Or, si tout le monde admet pouvoir être potentiellement la victime d'un vol de données, d'une infection par un virus ou d'une diffusion non autorisée de données, il est important également de prévoir le risque de la simple perte de données provoquée par une erreur humaine ou matérielle. En outre, l'accroissement naturel de données produites par une entreprise justifie de penser systématiquement à effectuer des sauvegardes régulières et de prévoir des mécanismes de restauration ultra rapides pour réduire au minimum les périodes d'indisponibilité du système d'information. La seule attitude raisonnable à adopter est d'appliquer le principe de précaution en élaborant un « Plan de Reprise d'Activité ».

Compte tenu de toutes ces remarques, le fait d'accorder sa confiance en permettant à certains employés d'accéder à des données confidentielles, en exposant l'entreprise sur l'Internet et plus simplement d'utiliser les outils informatiques, peut mettre en péril ces entreprises si des précautions ne sont pas prises. Faut-il alors sombrer dans une paranoïa intensive pour éviter tout risque ? Heureusement, la réponse est Non.

La démarche rationnelle consiste plutôt à évaluer les risques : connaître les vecteurs d'attaques majeurs, analyser les causes, prévoir les conséquences et adopter les solutions adéquates. Si les risques augmentent à la même vitesse que les innovations progressent, les solutions de sécurité évoluent aussi et offrent une panoplie d'outils dédiés à la sécurité de l'entreprise et de ses données.

Les principaux vecteurs d'attaques sont au nombre de quatre : l'infection des ordinateurs par des « malwares », la perte de données causée par des pannes matériels et/ou des erreurs humaines, la fuite de données et enfin les attaques sur le Web à travers des failles de sites internet qui favorisent le vol d'informations critiques stockées dans les bases de données.

Ainsi, pour chaque vecteur d'attaque correspond une solution : les Antivirus, les systèmes de sauvegarde et de restauration rapides, les audits de sécurités Web et les outils de DLP (Data Leak Prevention).

Antivirus, une protection indispensable

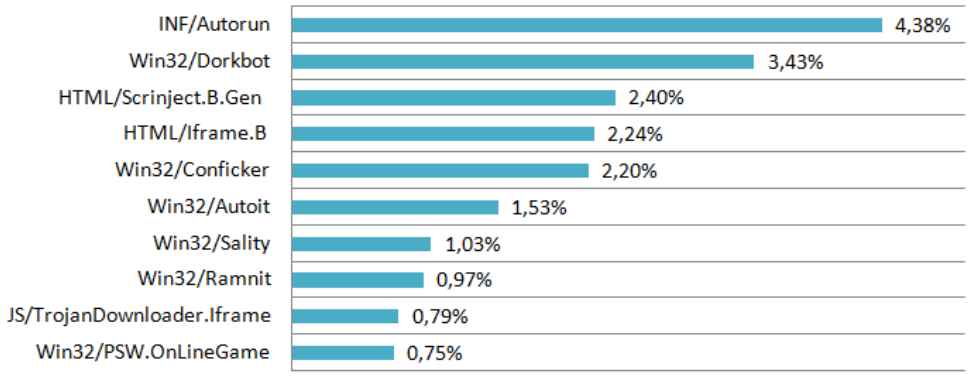
→ *Tous égaux face à la menace*

Aujourd'hui encore, certaines entreprises ne se préoccupent pas réellement de leur sécurité informatique et pensent pouvoir passer entre les mailles du filet, en considérant leurs domaines d'activités comme éloignés de l'informatique, en raison de la faible quantité de machines utilisées ou simplement parce qu'elles ne visualisent pas le risque qui se présente à leur porte. Cette méconnaissance de la capacité de nuisance des cybercriminels est contraire à la réalité des faits. Lorsqu'il s'agit d'infecter des ordinateurs et de propager les vers, ces pirates attaquent sans distinction. En effet, rares sont les « malwares » ciblant une victime spécifique, les objectifs principaux étant la diffusion massive pour créer des réseaux de « botnets » ou dérober des informations bancaires destinées à la revente sur le marché noir. Dans le cas d'entreprises, tout fichier peut être utile à voler, que ce soit des bases clients, des documents confidentiels, des propriétés intellectuelles ou des carnets d'adresses. La seule limite est l'imagination.

D'autres encore font preuve de laxisme en considérant que leurs machines n'étant pas reliées à Internet ou étant sécurisées en amont, ne requièrent pas l'usage d'un Antivirus. Ce raisonnement va à l'encontre de nos chiffres : nous avons constaté sur l'année 2011 (tout pays confondus) que l'infection par « Autorun » (NB : exécution automatique à partir d'un CD, clé USB ou autres contenant un fichier malveillant introduit via le fichier autorun.inf) se plaçait en première position de notre TOP 10 depuis le mois de février 2011 (en seconde position pour le mois de Janvier) et n'a plus quitté cette place depuis, malgré les nombreux rappels effectués régulièrement par les éditeurs d'antivirus, tels que ESET.

Doit-on rappeler que « Stuxnet », l'un des « malwares » le plus évolué et premier à cibler les systèmes « SCADA » se propageait via des clés USB infectées…

Global Threats According to ESET Live Grid® Statistics (November 2011)



(source: ESET)

Même constat du côté des systèmes d'exploitation. L'époque où seul Windows était le terrain de jeu des pirates est révolue. Comme nous avons pu le constater, le système d'exploitation d'Apple Mac OS X n'est plus épargné, même si les chiffres ne sont pas encore inquiétants, nous avons pu observer de nouvelles variantes de malwares connus tels que « OSX/TrojanDownloader.Jahlav », de nouveaux venus avec «OSX/TrojanDownloader.FakeAlert » mais aussi des portages comme cela a été le cas avec « OSX/Tsunami » backdoor, créée à l'origine pour les systèmes « Linux » et qui a été découvert par les chercheurs d'ESET.

→ *Quelques types de menaces, leurs causes, leurs conséquences*

La diversité des menaces, communément appelées « Malwares », est composée de toutes sortes de vecteurs ayant chacun un rôle et une façon de travailler bien définie. Parmi eux nous retrouvons les virus, les vers, les spyware, les Trojans, les rootkit, les rogues et la liste est encore longue.

Les virus sont de petit programmes capables de s'auto-reproduire en recopiant leurs codes dans un fichier sain présent sur le système, le réseau LAN (Local Area Network) ou sur d'autres formes de médias. Ils se classifient ensuite en virus de fichier, virus de boot et macro virus qui infectent respectivement les fichiers, les secteurs de démarrage du disque dur et les documents bureautiques fonctionnant avec des macros.

Les vers mettent la barre un peu plus haute car ils ont la capacité de se reproduire de façon indépendante et de se diffuser à travers le réseau LAN mais aussi via Internet. De plus les vers peuvent rapatrier des logiciels malveillants, tels que des « Backdoor » sur les machines infectées. Ainsi, un ver peut être diffusé dans le monde entier en quelques heures.

Quant aux Spywares, ils ont notamment pour objectif de cibler vos habitudes, vos attentes, et de repérer les sites que vous visitez. Ces programmes servent à récolter toutes les informations vous concernant et à les transmettre via Internet. Ces données seront ensuite vendues à des annonceurs ou autres, pour des campagnes d'e-mailing.

Les troyens (Trojan ou Chevaux de Troie) ont principalement la faculté de prendre la main à distance de la machine, de supprimer des fichiers et d'enregistrer tout ce qui est saisi.

o *Mon antivirus m'indique continuellement que je suis infecté !*

Les Rogues ou Scarewares sont de faux logiciels de sécurités se présentant comme des antivirus ou des anti-spyware. Installés la plupart du temps par l'utilisateur, en cliquant sur un lien malveillant, en installant un crack ou simplement en installant de faux codecs vidéos, ils ont pour but de faire peur à l'utilisateur en lui indiquant que son ordinateur est totalement infecté. La solution proposée est alors d'acheter la version payante de l'outil pour tout désinfecter. Or, dans la majorité des cas l'ordinateur n'est pas réellement infecté et même si c'est le cas, le Rogue ne désinfectera rien, sauf dans quelques rares circonstances où le Rogue va jusqu'à réaliser une légère correction et optimisation de la base de registre afin de démontrer une quelconque utilité.

Les sociétés éditrices de ces logiciels ne négligent aucun détail pour crédibiliser leurs escroqueries en donnant un look professionnel à leurs outils ainsi qu'à leurs sites Internet. Ils savent très bien employer le style et le design des sites des vrais éditeurs pour piéger plus facilement les personnes non averties.

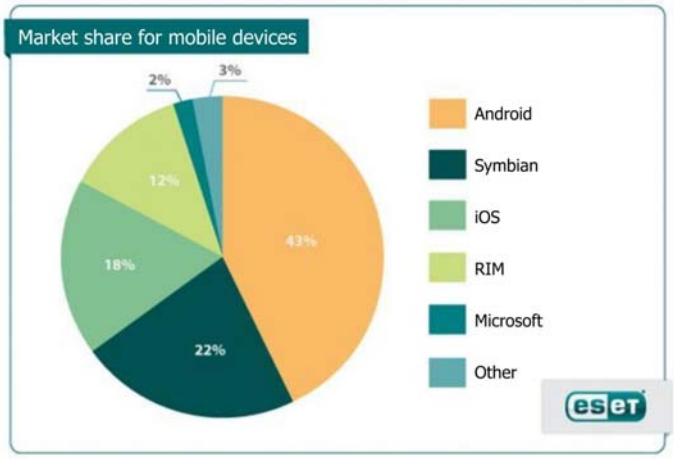
Les rogues sont aussi présents sur Mac !

(Mac Guard - http://kb.eset.com/esetkb/index?page=content&id=SOLN2746)

o *Les Smartphones en ligne de mire*

D'après les données publiées récemment par « Gartner », les ventes de Smartphones dans le monde ont atteint 115,185 millions d'unités sur le troisième trimestre de 2011, un chiffre supérieur de 42% par rapport à la même période en 2010. Parmi eux, Android représente près de 61 millions d'appareils, Symbian 19,500 millions et iOS 17,295 millions. Comme d'habitude, lorsqu'un système peut permettre aux pirates d'atteindre une large cible, ils n'hésitent pas une seconde à travailler plus spécialement sur des malwares destinés à ces systèmes.

D'après ESET, le système d'exploitation Android représente 43% de part du marché :



(ESET – Malware Goes Mobile)

Les Smartphones actuels permettent à peu de chose près de réaliser les mêmes actions que sur un ordinateur : les utilisateurs consultent leurs emails, leurs calendriers, font des achats en lignes et consultent leurs comptes bancaires. C'est pourquoi nous voyons apparaître de plus en plus de malware à destination des Smartphones.

Sur « Symbian » par exemple, nous trouvons des malwares se présentant comme des « Updater » d'applications, mais qui en réalité vont, dès l'installation, envoyer des SMS à des numéros surtaxés. Du côté d'Android, hormis l'application de surveillance « Carrier IQ » installée par les fabricants, il existe de vrais « Malwares ».

Certains « Malwares » conçus pour Android travaillent de façon astucieuse, puisqu'à l'origine lors du téléchargement sur le « Market », ils sont totalement inoffensifs. Puis, dès l'exécution, ils indiquent qu'une mise à jour est disponible. Cette mise à jour implémente en réalité du code malveillant mais demande aussi à disposer de plus de privilèges. En effet, si lors d'une première installation, l'utilisateur ne se soucie pas de vérifier les privilèges requis par l'application, il se préoccupera encore moins de les vérifier lors de la mise à jour d'une application à laquelle il a déjà accordé sa confiance une première fois. Une attention particulière doit être prêtée à l'apparition de la menace « SpyEye » sur Android qui permet de voler des informations bancaires et qui est bien connue sous Windows.

iOS, quant à lui, est aussi concerné mais de manière différente. La politique de sécurité d'installation et de mise en ligne des applications sur le « Market » étant assez restrictive (à l'inverse d'Android), l'utilisateur bénéficie d'un système relativement sain, sauf bien sûr si il a subi un « Jailbreak », auquel cas un grand nombre d'applications « crackées » contiennent des menaces.

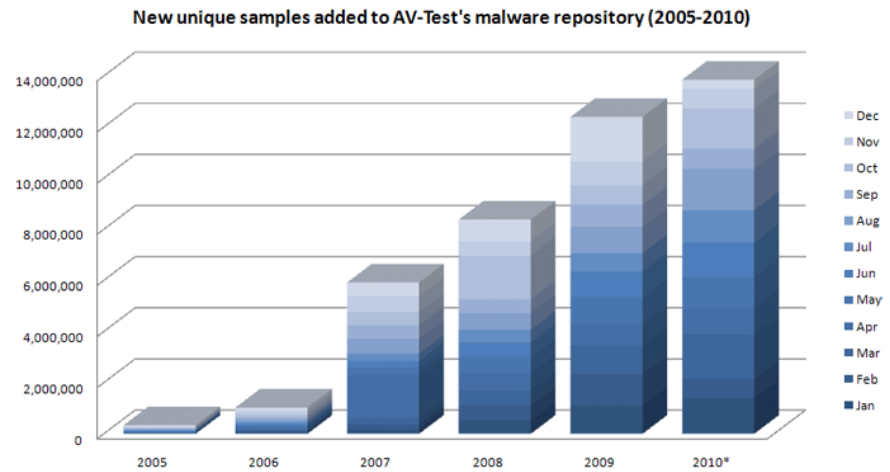
→ Devons-nous accepter la fatalité ?

En réalité, il n'y a pas de fatalité dans ce domaine. Bien que le danger soit bien réel et permanent, nous disposons néanmoins de solutions. Il est important de comprendre qu'une infection peut être réalisée par différentes voies : le SPAM, l'ingénierie sociale, le SEO Poisoning, les réseaux sociaux jusqu'aux vulnérabilités « Zero-Day » même si ces dernières sont plus rares.

Le paradoxe est qu'une grande partie des vulnérabilités exploitées par les malwares actuels ont été corrigées depuis plusieurs semaines, plusieurs mois, voire plusieurs années dans certains cas. Selon « Gartner », « 90% des attaques exploitent des failles de sécurité pour lesquelles des correctifs existent ». Une simple mise à jour régulière du système d'exploitation aurait ainsi pu permettre de les éviter. Il est aussi primordial d'équiper chaque poste d'une solution de sécurité disposant des dernières technologies de détections proactive et de protection, telles que la vérification de la mise à jour du système, la détection heuristique, la détection de rootkit et la vérification de la réputation d'un fichier sur le Cloud.

Pour répondre à ces problématiques des solutions existent et ont déjà largement fait leurs preuves, telles qu' « ESET NOD32 » ou « ESET Smart Security » qui disposent de l'ensemble de ces critères, notamment avec « ESET Live Grid ». De la même façon, ESET propose des solutions de sécurité destinées à Linux, MAC OS X et autres OS de Smartphones.

Enfin, il faut garder à l'esprit que quelque soit le secteur, la source d'erreurs ou de négligences qui possède le plus grand potentiel de risques se situe entre la chaise et le clavier… Il est donc impératif d'éduquer les utilisateurs.



(source : AV-Test.org)

Ne soyez plus dépendant de votre matériel

→ *Quand la simple sauvegarde ne suffit plus*

Difficile aujourd'hui de nier le fait que les entreprises sont de plus en plus dépendantes de leur Système d'Information et par conséquent, de plus en plus menacées en cas de défaillance. Que ce soit dans le domaine de la sécurité liée aux attaques malveillantes ou plus simplement, lors de la perte de données ou de la panne d'un serveur, le risque est plus ou moins bien estimé, mais paradoxalement assez mal appréhendé. Le constat est simple : la mise en œuvre d'un plan de secours pour assurer la continuité de services, notamment dans les PME, est jugée trop complexe et coûteuse. Autre constat alarmant, la plupart des entreprises qui possèdent un PRA (Plan de Reprise d'Activité), ne testent pas le processus de restauration, comme si la mise en place du système de secours ne pouvait pas subir lui même de défaillance et que le système d'information n'évoluait jamais.

Le type d'évènement pouvant amener à la perte de donnée, voire du système d'informations complet se résume à cinq cas de figure :

- Un fichier sensible corrompu (virus, vers, etc.) ou supprimé accidentellement
- Une application inopérante ou corrompue suite à une mise à jour
- Une panne matérielle du poste de travail ou du système d'exploitation
- Une erreur humaine, un vol ou autres actes malveillants
- Une catastrophe naturelle : incendie, inondation, tremblement de terre etc.

À l'évidence, la simple sauvegarde des données ne répond que très partiellement au problème posé, car le mécanisme de la restauration se heurte, dans de nombreux cas, à des contraintes techniques. Si la sauvegarde de fichiers sur un autre support d'enregistrement est suffisante lors de la perte d'un ou plusieurs fichiers, la restauration complète d'un système (OS, pilotes associés au matériel, applications, configurations spécifiques…) suite à une défaillance plus large, suppose l'emploi de technologies de création d'images disques permettant de répondre à ces problèmes. Qu'il s'agisse de la restauration d'un ou plusieurs fichiers, d'un serveur entier ou d'un système d'information complet, nous entrons alors dans une logique de Plan de Reprise d'Activité réduisant l'indisponibilité des ressources de l'entreprise.

Autre point important qui touche aussi bien les PME que les grandes entreprises, l'absence de cohérence entre la vision des informaticiens et celles des métiers au sujet de la criticité des applications et des données. Pour les premiers, la réponse est d'ordre technologique alors que pour les seconds, elle se réfère à des processus de gestion de l'information. Les responsabilités partagées des acteurs métiers et de ceux du SI ne sont pas toujours clairement définies. Or, le fait de pouvoir sauvegarder et restaurer rapidement ne permet pas de s'affranchir d'une recherche des causes de la défaillance, telles que l'introduction d'un virus, un acte malveillant, une erreur de manipulation, et plus généralement, le non respect de règles de sécurité qui va de pair avec un PRA efficient.

→ *Cinq raisons pour convaincre*

o *Sauvegarde à chaud*

La notion de sauvegarde « à chaud » se réfère à l'idée de pouvoir créer une image de sauvegarde intégrale d'un système sans pour autant bloquer son usage pendant l'opération. En s'appuyant sur la technologie Snapshot de Windows, certains logiciels permettent de créer des sauvegardes systèmes à chaud sans aucun temps d'indisponibilité pour les utilisateurs. Ainsi les images de sauvegarde créées à chaud comprennent le système d'exploitation, les données critiques, les paramètres de configuration, applications et les bases de données en cours d'utilisation (exemple : MS Exchange, MS SQL, etc.)

o *Restauration d'un système complet*

Lorsqu'un incident se produit, l'entreprise doit pouvoir restaurer les volumes de ses serveurs, postes de travail et PC portables, aussi rapidement que possible afin de minimiser les interruptions de service aux utilisateurs. Réinstaller manuellement les systèmes d'exploitation et reconstruire les environnements utilisateurs, est non seulement fastidieux, mais prend en moyenne au moins trois heures. Grâce à la technologie de création d'image disque, il est possible de restaurer un système complet en quelques minutes à la condition d'effectuer l'opération sur la même machine. L'utilisateur retrouve alors le même environnement, comme précédemment.

o *Restauration complète sur un matériel différent*

En raison d'une défaillance matérielle ou d'autres circonstances qui rendent inutilisables la machine, il est nécessaire de restaurer un volume système sur un matériel partiellement ou complètement différent, ou encore dans un environnement virtuel. Il existe des solutions logicielles peu coûteuses intégrant une technologie de mise à jour des pilotes matériels pour restaurer un système sur un matériel différent ou dans un environnement virtuel prenant en charge tous les types de restauration système (P2P, P2V, V2P et V2V).

o *Disposer d'un serveur virtuel miroir de secours*

Disposer d'un serveur miroir complet est une solution relativement onéreuse. Aussi, l'idée de créer une machine virtuelle de secours, susceptible de prendre le relais dans le cas où le serveur principal deviendrait défaillant, s'avère pertinente sur bien des aspects. À ce titre, on trouve sur le marché des solutions logicielles, telles que ShadowProtect, qui permettent maintenant de générer des disques durs pour machine virtuelle qui sont mis à jour en parallèle des sauvegardes incrémentales. Si le serveur de production s'arrête de fonctionner pour une raison quelconque, il suffit de démarrer la machine virtuelle qui, en quelques minutes, restitue le système dans son intégralité. Cette solution constitue véritablement les bases d'un Plan de Reprise d'Activité, voir de continuité de service.

o *Messagerie*

Dans le cas où la fonction serveur de messagerie est assurée en interne, à l'aide de Microsoft Exchange par exemple, il est également important de prévoir des mécanismes de sauvegarde et de restauration des boîtes aux lettres individuelles, courriels et pièces jointes. Cette solution doit pouvoir s'intégrer dans un processus global de plan de reprise d'activité afin de minimiser le temps d'indisponibilité de la messagerie suite à un incident survenant sur le serveur Exchange ou sur les postes.

→ *Les bonnes pratiques*

Le SI évolue sans cesse à travers les applications, les mises à jour des OS, les nouvelles menaces, la croissance de telle ou telle activité...Ces évolutions conduisent nécessairement à des changements de configurations matérielles notamment. Par voie de conséquence, le PRA peut rapidement devenir obsolète. Il est donc indispensable de tester régulièrement le processus de restauration pour vérifier que tout le monde retrouve bien ses données et son environnement. Cette opération, ne peut pas être uniquement dévolue au responsable du SI. Seul l'utilisateur peut réellement déterminer la conformité avec son contexte habituel et surtout juger de la criticité des données auxquelles il a accès. À l'image des exercices d'alertes incendies pratiquées dans les entreprises, il est toujours "préférable" de découvrir les points faibles lors de ces tests, que d'attendre la catastrophe.

En somme la mise en œuvre d'un PRA efficient suppose de définir un plan de sensibilisation de tous les acteurs de l'entreprise afin de garantir son efficacité à long terme. Quant aux diverses technologies entrevues plus haut, la solution haut de gamme qui consiste à employer des serveurs virtuels de secours s'avère à la fois performante et très économique, et suffisante dans bien des cas.

Avant d'engager n'importe quelle initiative en la matière, il est bon de rappeler quatre évidences : l'image de l'entreprise est dépendante de la fiabilité et de la sécurité du SI ; le coût de la réparation d'un incident est souvent sans commune mesure avec la mise en place d'un PRA ; la prévention ne se limite pas à des solutions technologiques, elle dépend également des campagnes de sensibilisation et d'éducation auprès des utilisateurs ; l'analyse des risques (outre ceux qui dépendent de l'infrastructure, bien entendu) n'est pas du seul ressort des informaticiens.

→ *Les technologies de pointes au secours de la technologie*

Des solutions telles que ShadowProtect comprennent plusieurs options de sauvegarde des données : soit la sauvegarde se limite à une partition complète d'un disque, soit c'est l'intégralité de la machine qui est sauvegardée à travers une copie image. La sauvegarde s'effectue vers un autre PC, un disque réseau (NAS), un disque externe USB ou encore vers une machine virtuelle.

En cas d'incident, ce type de solution offre la possibilité de choisir entre une restauration intégrale vers un PC, même de configuration différente, ou de redémarrer quasi instantanément sur la machine virtuelle en attendant la restauration sur un autre PC. Cela permet d'effectuer une copie exacte des données, même si celles-ci sont en cours de traitement par le système. Ainsi l'indisponibilité du poste de travail est réduite à son minimum lorsqu'un incident survient.

Grâce à la fonction HIR (Hardware Independent Recovery) de ShadowProtect, la restauration ou la migration de systèmes est facilitée même lorsque la configuration matérielle de la machine cible est différente de la machine d'origine. Les nouveaux pilotes sont automatiquement détectés et intégrés lors de la restauration ou de la migration. La reprise sur incident est également facilitée dans un environnement virtuel grâce à la technologie VirtualBoot qui offre à l'administrateur la capacité de booter toute image de sauvegarde à l'aide de Sun VirtualBox, même la version gratuite.

Grâce à la technologie VirtualBoot permettant d'effectuer une restauration image d'un téraoctet de données, en moins de 2 min sur une machine virtuelle dotée de Sun VirtualBox, ShadowProtect assure une reprise de l'activité quasi immédiate afin de pouvoir préparer tranquillement un autre serveur local ou distant destiné à prendre le relais. En outre, il inclut une nouvelle fonctionnalité unique appelée HeadStart Restore (HSR) qui permet d'effectuer la restauration du serveur en même temps que les sauvegardes afin d'obtenir presque instantanément un serveur restauré en quelques minutes.

Y0u h4v3 b33n h4ck3d…

→ *PME-PMI le danger frappe à votre porte !*

Avec l'ampleur du développement de l'e-commerce et des réseaux sociaux, les entreprises sont fortement incitées à disposer d'un site web attractif qui associe des critères de convivialité, de fluidité et de dynamique. Le site devient également un lieu naturel de saisie d'informations par les utilisateurs (coordonnées personnelles et bancaires notamment) ce qui ouvre la voie à des tentatives malveillantes de toutes sortes. La vulnérabilité du site représente en conséquence, un risque que l'on ne peut pas ignorer.

L'enquête exclusive menée en France par Athena Global Services confirme les données du rapport « Winter 2011 » publié par White Hat (Jeremiah Grossman). Sur 100 sites français audités (institutionnels et marchands), seulement 8 % d'entre eux sont exempts de faille. À titre d'exemples, un extranet comportait 440 failles dont 323 critiques ; un site e-Commerce comptait 742 failles dont 254 critiques et le site d'une Web Agency présentait 10 failles dont 2 critiques. Cette enquête a permis à ces sites d'analyser quelles étaient les failles critiques, les dégâts qu'elles pouvaient engendrer et les risques potentiels.

Six mois plus tard le constat corrobore cette étude. Les experts ont réalisé une cinquantaine d'audits de vulnérabilité, principalement sur des sites de commerce en ligne. Par rapport aux types de menaces constatées lors de l'étude, les méthodes employées ont peu évolué. Toujours en tête les injections SQL et le « Cross Site Scripting » (XSS). Sur quelques sites de grandes sociétés, qui ont souhaité effectuer l'audit par acquis de conscience, pensant qu'elles étaient bien protégées par des pare-feux applicatifs, il a été majoritairement trouvé ce même type de failles ainsi que des erreurs de paramétrage des serveurs web entrainant de la divulgation d'informations. En réalité ces pare-feux ont tendance à dissuader les pirates amateurs, mais pas les professionnels, une telle solution n'est qu'une barrière de dissuasion mais ne comble en aucun cas une faille existante.

Sur l'un de ces sites, 343 failles critiques avec des possibilités d'exécution de codes ont été recensées. Il existait différentes possibilités de manipulations critiques, par exemple, exécuter des commandes systèmes sur le serveur à travers des données non sécurisées par la Web Application. Des vulnérabilités de type XSS furent aussi découvertes essentiellement au niveau des moteurs de recherche, des formulaires de création de compte et d'inscription sur des listes de newsletter. Plus surprenant, un grand nombre de fichiers de « backup » étaient conservés sur l'ensemble de ces sites internet et Web Applications permettant alors en toute tranquillité d'analyser le code source à la recherche de failles potentielles. Enfin nous avons pu déterminer, pour la plupart de ces sites, que les identifiants et mots de passe des utilisateurs étaient inscrits en « clair » dans les bases de données ou n'étaient simplement que stockés sous leur représentation « MD5 » (hachage cryptographique), sans même l'utilisation d'un « salt » rendant donc possible leur déchiffrement en quelques secondes à l'aide de « Rainbow Table ».

Les PME-PMI sont naturellement les cibles de cyber-attaques car elles ne prennent souvent pas garde à des failles critiques qui fragilisent leur informatique. En effet, elles n'ont généralement pas une structure suffisante pour disposer au sein de leurs équipes d'un développeur Web ayant de solides connaissances dans la sécurisation de son code. Grâce aux différents systèmes de gestion de contenu (CMS) accessibles aujourd'hui, ainsi qu'aux différents codes sources présents sur la toile et tutoriels de développement, presque tout le monde peut s'improviser développeur/webmaster.

Les dirigeants de ces entreprises sont alors tentés d'exploiter ces solutions et confient la réalisation de leurs sites Web et de leurs applications associées, à des personnes non qualifiées ou dont ce n'est pas le métier. Pourtant, les conséquences de ces vulnérabilités sont graves : détournement/effacement du site, prise de contrôle du serveur, vol de données confidentielles, altération des données… Ainsi, de nombreuses personnes malintentionnées savent parfaitement exploiter les failles.

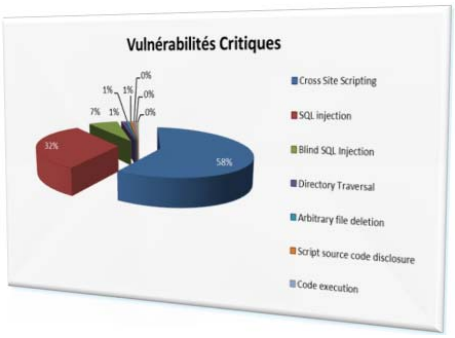
Il est même possible pour un amateur dans le domaine du « hacking » de réaliser ces opérations sans aucune connaissance, tout simplement en utilisant des outils d'analyses et d'exploitation automatiques des vulnérabilités que l'on retrouve assez facilement sur internet.

D'après les statistiques du « Web Application Security Consortium », 13% des sites peuvent être endommagés de façon automatique, et parmi eux, 49% sont vulnérables à travers des failles dites « critiques ». De plus, l'usage de techniques d'audits manuels révèle un pourcentage de vulnérabilité inquiétant qui se situe entre 80 et 96% des sites.

→ *Les quatre vulnérabilités les plus marquantes*

La vulnérabilité « SQL Injection » plus connue du grand public depuis sa forte médiatisation suite à son exploitation chez Sony Picture et au prestigieux MIT ILP (Massachusetts Institute of Technology – Industrial Liason Program), est très fréquente car la majorité des sites d'aujourd'hui repose en partie sur une base de données. Dès lors, une faille de ce type permettra à un pirate d'explorer cette base de données à la recherche d'informations confidentielles, telles que des identifiants, des numéros de cartes bancaires, etc. Dans certains cas, le pirate se servira de cette faille pour rapatrier un « malware » sur le poste du visiteur via l'injection de code JavaScript réalisée au préalable.

La vulnérabilité « Cross Site Scripting » ou « XSS » souvent sous-estimée, est la plus présente sur les sites internet. Elle a pour principale vocation la manipulation côté « client » des données et/ou des actions du visiteur. Son impact peut aller du vol des sessions utilisateurs, vol de données sensibles, injection de code dans la page Web, redirection vers un site d'hameçonnage, jusqu'au téléchargement invisible de malwares sur le poste du visiteur. Généralement cette vulnérabilité de par sa grande présence sur le web, ne se retrouve médiatisée que lorsqu'elle touche des sites tels que Twitter, Facebook ou Google.



La vulnérabilité « Broken Authentification and Session Management » qui prend de plus en plus d'ampleur, consiste à récupérer les identifiants d'un utilisateur qui circuleraient en clair sur le réseau car les requêtes HTTP ne seraient pas en SSL. Elle vise encore à récupérer les identifiants de sessions d'un utilisateur afin d'usurper son identité et donc de disposer de l'accès complet à son compte. Ces identifiants de sessions sont la plupart du temps récupérés via une faille « Cross Site Scripting » et de plus en plus de sites intègrent ces identifiants de sessions directement dans l'url.

La vulnérabilité « Cross Site Request Forgery » est presque aussi répandue que le « Cross Site Scripting » car elle repose sur le même principe, à savoir injecter du code. Le but étant de faire générer une requête vers un site malveillant, directement par le navigateur de la victime, ou bien d'exploiter à son insu ses droits sur le site où il est connecté afin de lui faire réaliser des actions. Dans ce dernier cas, ce sont essentiellement les utilisateurs ayant des accès privilégiés qui sont ciblés.

Toutefois nous avons récemment observé l'exploitation de cette méthode sur un des services proposés par Google sur lequel si la victime cliquait sur un lien spécialement forgé par le pirate, elle se retrouvait redirigée vers le site choisi par ce dernier tout en se rendant « de base » sur le site originale de Google. Le pirate a donc exploité une vulnérabilité dans le service de Google tout en utilisant une URL valide pour piéger ses victimes.

→ *Les causes les plus courantes*

La cause principale des failles est tout simplement le manque de filtrage des données et la trop grande confiance accordée aux utilisateurs par le développeur. Une autre cause se situe dans l'utilisation des données par défaut, que ce soit dans un CMS, un serveur Web, un serveur de base de données ou autre. Par manque de temps, les administrateurs systèmes et les développeurs occultent très souvent ces paramètres. On retrouve donc des serveurs de base de données exécutés avec des paramètres « root » accordant au pirate, en cas d'injection SQL, une totale liberté d'action. Ainsi on retrouve aussi des serveurs Web dont l'affichage des bannières est activé, où le « Directory Listing » est activé, les sessions non protégées. Dans le cas du « PHP », on remarque également des options critiques activées, tels que l'inclusion de fichier distant, l'exécution de commande système, l'affichage de la version installée, l'affichage des messages d'erreurs, etc. Dans certains cas, nous observons même des « Web applications » dont les identifiants administrateur sont « root / password ».

Nous rencontrons aussi de nombreux sites dont les messages d'erreurs sont affichés en clair. A priori, pour la plupart des développeurs, cela ne constitue simplement qu'un « design » perturbé, mais pour les « hackers » en revanche, cela représente bien plus. En effet, dans le cas d'une « SQL Injection » si les erreurs SQL sont affichées, le pirate connaîtra alors la structure de la requête, le type et le nom des données attendues et économisera 80% de temps de recherche pour exploiter la faille.

De plus, l'un des gros points noirs des outils « CMS » est qu'ils sont pour la plupart « Open Source ». Si d'un côté cela permet aux développeurs et testeur de trouver plus rapidement les bugs et vulnérabilités à corriger, d'un autre côté ces découvertes impliquent la vulnérabilité immédiate des utilisateurs ne mettant pas à jour leur version. A cela se rajoute le fait qu'un pirate peut facilement analyser le code source à la recherche de failles pendant des journées entières qu'il exploitera ensuite sur un site utilisant le même « CMS ».

→ *Quelques règles simples*

Il faut garder à l'esprit que les vrais hackers trouvent chaque jour de nouvelles failles. Il est donc très difficile, voire impossible de disposer d'un site inviolable. Néanmoins, certaines bonnes pratiques permettent d'avoir un bon niveau de sécurité qui nécessitera bien plus de travail pour les hackers.

Plusieurs règles doivent être respectées :

- Filtrer chaque donnée en entrée et en sortie
- Utiliser les fonctions d'échappement/assainissement avant d'effectuer une requête SQL et si possible travailler avec des « procédures stockées ».
- Travailler avec un système de « White List » et non de « Black List »
- Ne jamais rien exécuter avec les droits « root »
- Limiter les droits des applications et leurs accès uniquement à leurs propres répertoires

- Ne jamais laisser des fichiers de Backup accessibles
- Désactiver le Directory Listing
- Utiliser des noms de fichier/dossiers non courants
- Chiffrer toutes données sensibles (mot de passe, numéro de carte bancaire)
- Désactiver toutes les fonctions qui ne sont pas nécessaires au bon fonctionnement du site/application
- Lire la documentation complète de la configuration des serveurs Web, base de données utilisée afin de connaître les paramètres de sécurité
- Ne jamais afficher les messages d'erreurs
- Mettre à jour le plus souvent possible les outils utilisés (CMS, Serveur, OS, Langage)
- Ne jamais faire confiance aux utilisateurs
- Travailler autant que possible en connexion sécurisée
- Intégrer un système de « Jeton » pour chaque action
- Régénérer une nouvelle variable de session à chaque chargement de page

Certains outils permettent, non pas de détecter les vulnérabilités, mais plutôt de repérer les tentatives d'exploitation/d'intrusion. Ces outils connus sous les noms d'IDS pour « Intrusion Detection System » et d'IPS, pour « Intrusion Prevention System », permettent d'obtenir une évaluation du niveau de risque d'une requête effectuée par un utilisateur afin d'autoriser ou non la requête selon ses propres règles. Attention, même si ces outils améliorent la sécurité, il est fortement déconseillé de se reposer uniquement sur eux car de toute manière, les vulnérabilités doivent être corrigées. La mesure la plus efficace consiste à effectuer régulièrement des audits de chaque site et de chaque serveur. Pour cela, il existe de nombreux outils d'analyses automatisées, tel qu' « Acunetix Web Vulnerability Scanner », des solutions SAAS telles que « WebSure », ou encore des audits réalisés par des experts.

Malgré tout, réaliser un audit peut coûter relativement cher. Volià pourquoi, le service d'audit WebSure proposé par ATHENA Global Services, s'adresse plus particulièrement aux PME. Il utilise le moteur de détection Acunetix, intégré dans un processus automatisé en ligne, pour effectuer un contrôle complet du site à auditer. Une fois le scan effectué, un ingénieur analyse les résultats de manière à établir une étude circonstanciée et remettre deux rapports d'audit : l'un de synthèse destiné à la direction de l'entreprise, l'autre détaillé et technique à l'usage du webmaster et/ou du développeur. Ainsi, les entreprises de toutes tailles peuvent obtenir un audit professionnel pour un coût très modique, sans passer par des solutions d'audit réservées jusqu'alors à de très grandes organisations.

Maitrisez la fuite de vos données

→ *Des données qui valent de l'or*

Depuis l'ordonnance du 24 août 2011, les articles 38 et 39 associés à l'article 34 de la loi « Informatique et Libertés », imposent aux entreprises une obligation de notification en cas de violations de données personnelles. L'absence de notification engendre une peine pouvant aller jusqu'à 5 ans de prison et 300.000 euros d'amende. La France fait donc un pas en avant concernant la sécurité des données personnelles.

Selon la 14ème étude annuelle sur la sécurité informatique menée par « PWC », 6 entreprises sur 10 déclarent avoir subi au moins 1 incident au cours des 12 derniers mois contre 4 entreprises sur 10 l'année précédente. Dans le même temps, le nombre d'incidents liés à des entités externes a triplé ces trois dernières années en France. D'après l'étude menée par l' « Institut Ponemon » en 2010 sur les fuites de données en France, les pertes financières moyennes subies par les entreprises sont estimées à 2,2 millions d'euros soit une augmentation de 16% par rapport à l'année précédente. Les records des coûts de perte pour les sociétés étudiées furent pour le plus élevé de 8,6 millions d'euros et de 282 000 euros pour le coût le plus bas. Des chiffres pouvant s'expliquer par la quantité colossale de données transitant au sein des réseaux d'entreprises chaque jour qui croit de façon exponentielle. Parmi ces données, des messages contenant des informations confidentielles, des identifiants de connexion, la comptabilité, la propriété intellectuelle ainsi que des bases clients.

Au delà de la perte d'informations elle-même, il faut prendre en compte le temps passé à effectuer les corrections techniques des faiblesses ayant permis ces fuites. Dans la majorité des cas ces « causes » ne pourront être mises en lumière par l'entreprise seule qui devra alors faire appel à une équipe de consultants spécialisés. En outre, il est indispensable de prendre en compte un autre aspect des conséquences de la perte d'informations : la dégradation de la confiance accordée par le client susceptible de générer un manque à gagner conséquent. En effet, il n'est pas rare que les clients qui constatent que leurs données personnelles ont fait l'objet de fuites, se dirige vers une rupture de contrat avec l'entreprise concernée.

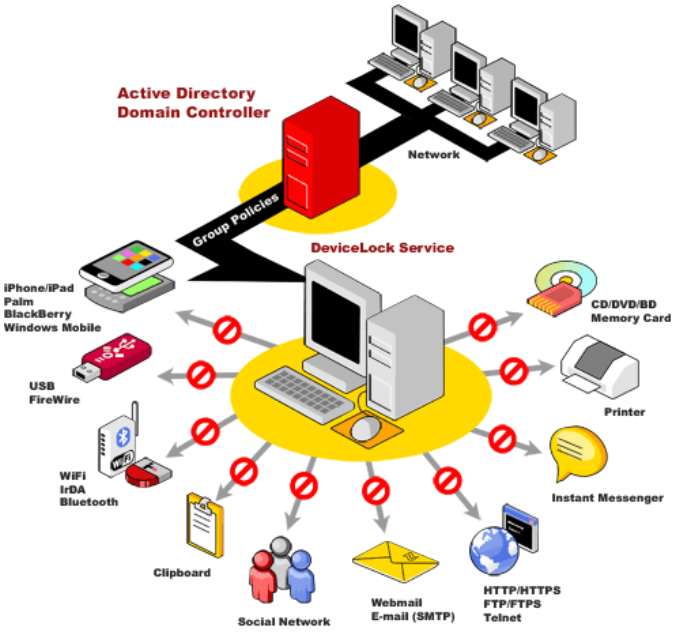
→ *Les vecteurs de fuites*

A l'heure des sociétés 2.0, les vecteurs de fuites se multiplient et le risque de retrouver ces informations sur la toile prend une ampleur considérable. Avec les emails consultables sur les smartphones, les dispositifs de stockage USB de grosse capacité capables de recopier une quantité de documents impressionnante, les graveurs de CD, les lecteurs de cartes, …une multitude d'outils présentait déjà des sources de données accessibles. Or, de nouveaux vecteurs sont venus enrichir la longue liste des risques de fuites : les réseaux sociaux et les outils de « presse-papiers » online.

En effet, diffuser massivement une information de façon volontaire ou involontaire est à portée de clic de tout un chacun avec Facebook, Twitter, Google+, Pastebin , blogs et wiki en tout genre. Et, comme nous avons pu le voir récemment à plusieurs reprises avec Pastebin et plus encore avec l'affaire WikiLeaks, une fois l'information en ligne, il est déjà trop tard. D'après une étude réalisée par « Lexi », 15% des salariés sont responsables de fuites d'informations confidentielles sur les réseaux sociaux et le plus inquiétant c'est que dans bon nombre de cas, ils postent ces informations sans s'en rendre compte. Toutefois, de plus en plus d'entreprises se doivent d'interagir avec les réseaux sociaux afin de construire une image de marque, communiquer avec les clients ou tout simplement être dans la tendance. L'avènement du « Cloud » renforce la difficulté de la tâche en hébergeant les données sur des architectures distribuées pour lesquelles les entreprises n'ont aucun contrôle.

S’ajoute à cela, le phénomène « Bring You Own Device » ou « apportez votre propre appareil », issu de l’engouement du public pour les Smartphones et tablettes qui ont la faculté de répondre également à des besoins professionnels. IDC indique que 78 % des collaborateurs d’une entreprise qui emploient un Smartphone l’utilisent pour consulter leur messagerie professionnelle et 68 % l’agenda de l’entreprise.

Plus grave encore, le risque s’amplifie avec ces appareils qui ont la possibilité de contourner le réseau d’entreprise en employant le WIFI externe ou le réseau 3G. De plus, n’étant pas connecté au réseau de l’entreprise, un agent devrait être placé directement sur l’appareil. Or, il est pour le moment impossible de réaliser une telle action sur des appareils Android ou iOS de façon « claire ».



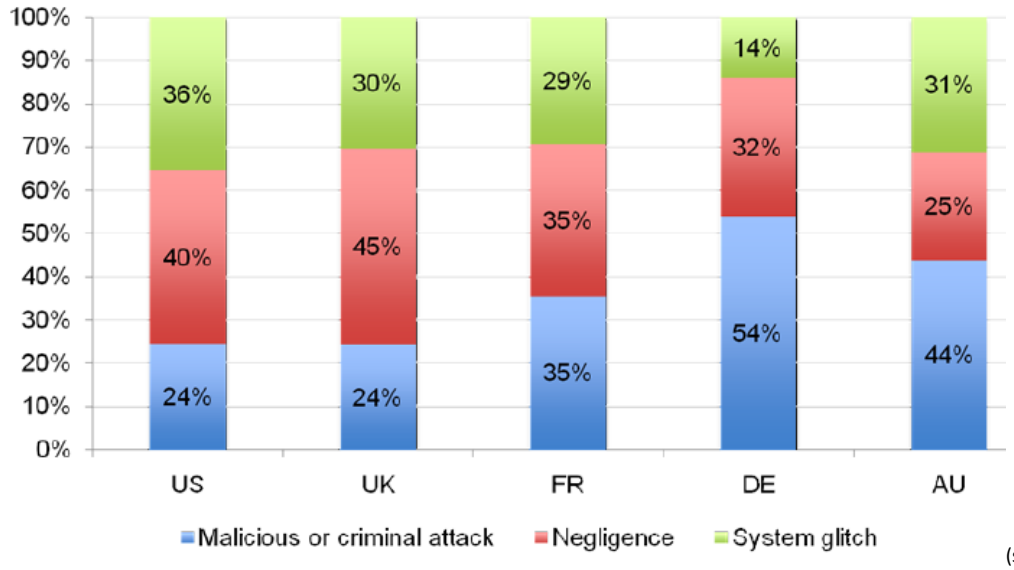
(source : devicelock.com)

Selon l’étude de l’ « Institut Ponemon », on observe que 43 % des pertes de données sont dues à des erreurs de tiers, telles que des partenaires, fournisseurs, clients ou sous traitants. À noter également que 38 % des pertes sont le fruit d’actes malveillants. Les dispositifs mobiles par leurs pertes ou leurs vols impliquent quant à eux 38 % des pertes d’informations sensibles. Il est toutefois utile de signaler que les fuites causées par de la négligence sont de moins en moins fréquentes. L’étude fait le constat d’une baisse de 6 % par rapport à l’année précédente, en passant de 29 % à 23 %. Toutefois 80 % des violations de l’information viennent de l’intérieur (stagiaires, prestataires, collaborateurs). La crise a aussi engendré cette dispersion d’information car toujours d’après l’ « Institut Ponemon », 59 % des employés licenciés se sont livrés à des vols de données sensibles et confidentielles lors de leur départ, sans que les entreprises ne s’en rendent compte.

Les méthodes préférées restent l’impression des documents, la copie sur clé USB et l’envoi sur la boîte de messagerie personnelle. N’oublions pas non plus les envois d’emails contenant des informations confidentielles, adressés à de mauvais destinataires suite à une erreur de saisie.

→ *Soyez le « Garde fou »*

Si nous sommes conscient des risques liés au facteur humain, doit on pour autant agir de façon répressive en interdisant toute communication avec l'extérieur ou en « scannant » chaque individu à l'entrée de l'entreprise pour s'assurer qu'il ne transporte pas de clé USB ? La prévention contre la fuite de données ne peut être combattue de cette façon. Au contraire, elle risque de cette manière de s'accentuer. La formation et la sensibilisation des utilisateurs aux risques et aux conséquences provoqués par la fuite de données, qu'elle soit volontaire ou non, aura un impact bien plus fort et permettra d'obtenir de meilleurs résultats.



(source : Ponemon Institute – 2010 Global CODB)

La mise en place d'un outil de « DLP » (Data Loss Prevention) n'est pas la seule réponse à ce problème. Il apporte néanmoins, une solution permettant de réduire au minimum le risque de fuite. Un projet de « DLP », qui se compose d'un ensemble de mesures organisationnelles et techniques visant à identifier, surveiller et protéger les informations, doit s'appuyer à la fois sur l'outil lui même, sur la formation des utilisateurs, mais aussi sur la connaissance de l'existant à savoir :

- Quelles sont les données à protéger ?

- Où sont stockées ces informations ?

- Qui peut y accéder ?

- Quels sont les risques en cas de fuite ?

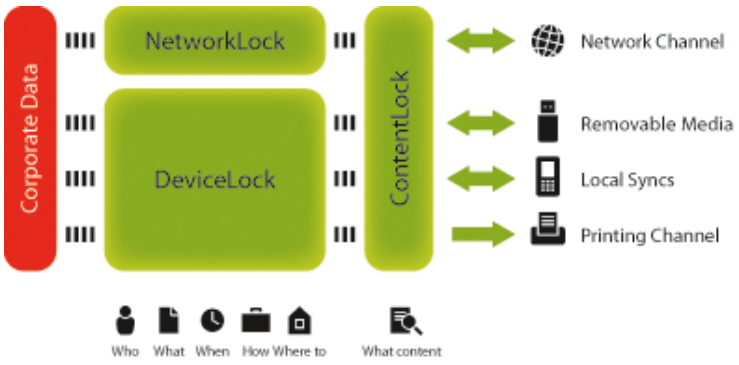
De plus, un projet de « DLP » ne peut assurer à lui seul l'entière sécurité de l'entreprise. Il est un composant sécuritaire parmi d'autres tels que l'antivirus, le firewall, le système de sauvegarde etc., mais doit avant tout reposer sur une « infrastructure sécurisée ».

→ *Assister le collaborateur*

D'après une étude menée par « Forrester Research » en 2010, seulement 15% des entreprises avaient mis en œuvre une solution de protection contre la fuite de données. Un chiffre s'expliquant par la complexité de mise en place d'un tel projet. Afin d'aider les entreprises à lutter contre des fautes d'inadvertances, des curiosités exacerbées ou de la diffusion délibérée de la part des utilisateurs, des outils existent. Ils sont capables d'autoriser de façon transparente les actions selon les privilèges accordés et peuvent, en cas de tentative volontaire ou accidentelle, empêcher l'opération de s'exécuter.

Ces solutions de prévention ont pour principe le « moindre privilège », pour toutes opérations de transfert et de stockage de données sur le poste de travail. L'une des particularités de ces solutions, telle que « DeviceLock » réside dans sa capacité à analyser le contenu de chaque transaction à la recherche de format de données spécifiés à l'aide d'expressions régulières, d'empreintes de fichiers ou en se basant sur des mots clés permettant alors à l'entreprise de se prémunir contre tous types de fuite, peu importe que l'information soit spécifique ou générale. De plus, en enregistrant chaque tentative et chaque déclenchement d'une règle, ces outils permettent d'identifier immédiatement la cause et le responsable de la tentative de fuite. Dès lors, cela a pour effet de rassurer les collaborateurs étourdis contre une éventuelle fuite que l'on pourrait leur amputer et cela freine ceux qui avaient des intentions malveillantes.

La solution « Endpoint DLP Suite » de DeviceLock permet d'assurer un contrôle total sur les flux réseaux ainsi que les données transitant par email, messagerie instantanée, réseaux sociaux, sessions telnet, réseaux sans fils et bien plus encore en sachant qui, quoi, quand, comment, où.



(source : devicelock.com)

Des solutions complémentaires

→ *Single Sign-On*

Extranet, Intranet, Email, CRM, Logiciel comptable, FTP un grand nombre de mots de passe différents sont saisies chaque jour. Récemment, un sondage mené par « LeJournalDuNet » auquel ont participé 301 internautes, a révélé que 34,2% d'entre eux utilisent pas plus de cinq mots de passe pour travailler, 31,2% entre deux et trois, 21,6% entre quatre et cinq et 13% n'en utilisent qu'un seul.

Si aujourd'hui l'utilisation de mots de passe "forts" commence doucement à s'imposer dans les esprits, elle s'accompagne de deux nouveaux problèmes pour les RSSI :

- Comment faire pour que chacun puisse retenir l'ensemble de ces mots de passe complexes ?
- Comment faire pour changer régulièrement ces mots de passe afin d'assurer une meilleure sécurité ?

Une réponse logicielle a donc commencé à se répandre : le SSO (Single Sign-On ou Authentification Unique). Cette solution offre la possibilité à un utilisateur de ne procéder qu'à une seule authentification lui permettant alors d'être reconnu sur l'ensemble des applications et sites internet sans avoir à se préoccuper de ses mots de passe.

Du côté du service informatique, l'ensemble des mots de passe réels peuvent alors avoir un cycle de vie très court et du côté utilisateur l'apprentissage du mot de passe « général » est bien plus aisé et il ne sera donc plus tenté de commettre les erreurs si courantes, telles qu'écrire ses différents identifiants sur un post-it ou utiliser le même mot de passe partout.
De plus en plus souvent les solutions de SSO sont assistées par des méthodes d'authentification forte, telles que la carte à puce et la biométrie.

→ *Authentification renforcée*

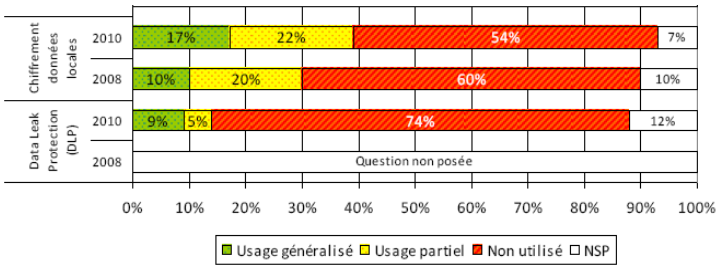
L'autre problématique à prendre en compte concerne les utilisateurs qui perdent leurs mots de passe, les oublient simplement ou qui ont été volés . Par conséquent, beaucoup de sites sont obligés de mettre en place des procédures de type « Mot de passe oublié ? » pour rappeler par un envoi d'e-mail le bon mot de passe. Or, cette solution est dangereuse, notamment dans le cas où un piratage d'adresses mails aurait pu s'effectuer auparavant. Certains sites proposent également de répondre à des questions personnelles, comme : « Quel est le prénom de votre mère ou l'année de naissance d'un parent ? », pour vérifier l'identité du demandeur. Cela suppose que des données personnelles aient été saisies lors de la procédure d'enregistrement. Toutes ces procédures sont fastidieuses pour l'utilisateur, lourdes à gérer par le site et ne permettent pas d'obtenir une véritable authentification.

Pour les entreprises qui souhaitent garantir un niveau d'authentification plus élevé et plus simple à mettre en œuvre, il existe une solution qui combinent deux facteurs : le premier qui reprend le mode classique de la saisie de l'identifiant et du mot de passe et un second qui va authentifier la personne par l'envoi par SMS d'un code ponctuel qu'il faudra enregistrer pour valider la connexion finale. De cette manière, l'entreprise qui souhaite contrôler l'accès de ses employés au système d'information par VPN, par exemple, peut ainsi à travers son annuaire (Active Directory, LDAP, etc.) autoriser ou non la connexion par l'envoi automatique d'un code via SMS sur le téléphone mobile ou Smartphone personnel de l'utilisateur. À chaque nouvelle tentative de connexion, un code différent est envoyé par SMS à l'utilisateur. C'est une approche simple et moderne qui peut facilement être déployée dans une configuration de cloud privé.

La solution SMS PASSCODE emploie cette méthode qui possède de nombreux avantages comme celui de ne pas avoir à installer la moindre application, ni sur l'ordinateur qui tente de se connecter, ni sur le téléphone mobile ou Smartphone. L'administrateur doit simplement veiller à maintenir à jour dans son annuaire, les numéros de téléphones mobiles des employés susceptibles de se connecter.

→ *Chiffrement des données*

Malgré les différents composants de sécurité mis en place par des entreprises considérées comme sérieuses ou prudentes, grâce à l'usage de solutions antivirus, de sauvegarde, de DLP , de SSO et d'audits, il n'est hélas pas possible de garantir à 100 % qu'une donnée confidentielle ne se retrouvera pas à l'extérieur de l'entreprise, notamment en cas de vol/perte d'ordinateur portable. C'est pourquoi il est également utile de se prémunir contre ce risque par l'usage du chiffrement des données sous toutes leurs formes.



Les chiffres inquiétants du CLUSIF présentés dans leurs rapports « Menaces informatiques et pratiques de sécurité en France - Édition 2010 » démontrent toutefois qu'encore trop peu d'entreprise applique cet aspect sécuritaire incontournable. En effet, leur étude démontre que seule 17 % d'entreprises de plus de 200 salariés font usage du chiffrement des données locales, 22 % un usage partiel et 54 % n'en font pas usage.

A propos de l'auteur

Jonathan Azria est spécialiste en logiciels malveillants et en vulnérabilité des sites web chez Athena Global Services. Auparavant, il a obtenu plusieurs diplômes relatifs aux NTIC, tels que le MEINF - European Masters in Information Technology ; le DEESINF - European Diploma Higher Education for IT ainsi que le BTS IRIS - Informatique et Réseaux pour l'Industrie et les Services.

Il collabore actuellement aux travaux menés par le laboratoire de recherche en malwares d'ESET à Montréal et fait partie de l'équipe d'auditeur WebSure.

A propos d'Athena Global Services

Créée en 1997, ATHENA Global Services est une entreprise indépendante spécialisée dans la distribution de logiciels de sécurité informatique.

A travers un vaste réseau de distribution - constitué de VARs, revendeurs locaux professionnels et des plus importantes enseignes spécialisées dans la distribution de logiciels - Athena Global Services propose des logiciels et des équipements de sécurité novateurs destinés aux particuliers et aux entreprises pour protéger et gérer leur environnement informatique :

- Antivirus, Pare-feu
- Cryptage
- Politique de sécurité
- Authentification
- Sauvegarde
- Migration des données
- Contrôle du trafic Internet

Outre cette spécialisation dans les solutions de sécurité, ATHENA Global Services propose également une gamme de logiciels utilitaires dédiés à la protection et l'optimisation des parcs informatiques.
Grâce à son savoir-faire, ATHENA Global Services entretient des relations privilégiées avec des éditeurs mondiaux et même français pour lesquels, elle localise et distribue leurs logiciels.

ESET Smart Security est une suite complète de sécurité comprenant l'antivirus le plus primé du marché, un anti-spyware, un pare-feu ainsi qu'un anti-spam.

StorageCraft ShadowProtect est une solution de sauvegarde et de restauration rapide permettant une reprise d'activité après sinistre rapide et fiable tout en assurant la protection des données et la migration des systèmes.

WebSure est une solution d'audit personnalisé pour vérifier l'intégrité de votre site et vous prémunir contre les risques d'attaques.

DeviceLock est une solution permettant la protection contre la fuite de données et l'intrusion de menaces.

Références

http://go.eset.com/us/threat-center/
http://www.eset.com/us/home/whyeset/livegrid/
http://kb.eset.com/esetkb/index?page=content&id=SOLN2746
http://www.gartner.com/it/page.jsp?id=1848514
http://go.eset.com/us/resources/white-papers/malware-goes-mobile.pdf
http://www.av-test.org
https://www.whitehatsec.com/resource/stats.html
http://www.zataz.com/news/21678/redirection_-url-injection_-google-maps.html
http://www.webappsec.org/
http://www.gartner.com/id=1764920
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460
http://www.pwc.com/gx/en/information-security-survey
http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2010%20Global%20CODB.pdf
http://www.indexel.net/actualites/reseaux-sociaux-prevenir-fuites-d-information-et-entree-de-malwares-3313.html
http://www.forrester.com
http://www.devicelock.com
http://www.journaldunet.com/solutions/questionnaire/fiche/16132/d/f/1/
http://www.clusif.asso.fr/fr/production/sinistralite/docs/CLUSIF-rapport-2010.pdf