



DES FRONTIERES FLOUES

Les prévisions de sécurité de Trend Micro pour 2014 et au delà

NOS PREDICTIONS

- 1 | *La banque mobile sera la cible d'attaques de type MitM. L'authentification en deux étapes connaîtra ses limites.*
- 2 | *Les cybercriminels opteront pour des attaques ciblées, sur les applications open source ou via du spear phishing ultra-personnalisé, et multiplieront les exploits.*
- 3 | *Nous assisterons à une poussée des attaques de clickjacking et de watering hole, de nouveaux exploits et à des attaques ciblant les dispositifs mobiles.*
- 4 | *Un acte majeur de piratage de données chaque mois.*
- 5 | *Intensification des attaques qui utilisent des vulnérabilités sur des logiciels en fin de support comme Java 6 et Windows XP.*
- 6 | *Le Deep Web, réel défi pour les forces de l'ordre, qui, par ailleurs, seront freinées par la dimension internationale des réseaux criminels.*
- 7 | *La méfiance du grand public s'accroîtra alors que les activités de surveillance des états sont dévoilées.*
- 8 | *Les menaces resteront mineures dans le domaine de l'Internet des Objets, mais émergeront dans ceux de la réalité augmentée et de l'Affichage Tête Haute.*

En septembre dernier, Trend Micro en collaboration avec Europol et l'ICSPA (International Cyber Security Protection), publiait le document et la websérie « 2020: The Series », avec pour ambition d'imaginer comment les nouvelles technologies seraient utilisées et évolueraient dans le futur.

En visionnant les différents épisodes de la série, vous découvrirez ce que, en 2020, l'intégration de multiples technologies apportera aux particuliers, aux entreprises et même à l'échelle d'une nation. Ainsi, on imagine que nombre de personnes utiliseront quotidiennement des lunettes ATH (Affichage Tête Haute), voire des lentilles de contact capables de réagir aux gestes des mains. Chaque individu bénéficiera de contenus Internet ultra-personnalisés, qui résultent d'une surveillance et d'une collecte de données en continu, réalisées via des capteurs et implants. Des réseaux intelligents offriront tout un panel de services et favoriseront un mode de vie assisté par les technologies. Par exemple, on peut imaginer que des élections politiques totalement automatisées deviendront une réalité. En contrepartie, de nouvelles menaces liées à la cybercriminalité feront leur apparition. Certaines d'entre elles iront jusqu'à détruire des infrastructures importantes et causer des dommages matériels.

Dans la websérie "2020: The Series", nous avons tenté d'imaginer l'avenir, basé sur plusieurs scénarios que vous ne pouvez pas forcément imaginer aujourd'hui. Par exemple, pourquoi les cybercriminels portent-ils des lentilles de contact ATH pendant que les forces de l'ordre, elles, sont équipées des lunettes ATH. Les lentilles de contact sont alimentées par une réaction biochimique et doivent être renouvelées chaque jour. Ce qui peut être très onéreux ! Comment la police a-t-elle pu obtenir des preuves vidéo dans la chambre d'un des personnages principaux de la série ? Des réponses que vous trouverez en visionnant la websérie "2020: The Series" ... et ses nombreux clins d'œil à "Blade Runner", un de mes films préférés.

De tels scénarios vont-ils se concrétiser ? Leurs prémices sont déjà perceptibles et les conditions sont très favorables à leur développement dans un avenir proche. L'année 2013 a été le théâtre de menaces mobiles qui devraient se poursuivre en 2014, puisque les équipements mobiles deviennent des cibles de choix. Les processus authentification en deux étapes actuels ne seront plus suffisants à l'avenir. Les attaques en ligne deviendront plus ciblées tandis que les assaillants continueront à identifier de nouvelles failles de sécurité. Les forces de l'ordre qui tenteront de faire barrage aux menaces devront affronter de nouveaux défis en territoire inconnu, le Deep Web, ainsi que la méfiance du public face aux révélations sur les opérations de surveillance menées par les états.

L'Internet des Objets reste un buzzword, dans l'attente de la prochaine « killer app », à savoir cette application ou ce dispositif qui changera la donne... et qui deviendra sans doute un nouveau terrain de jeu pour les exactions. Les lunettes Google (Google Glass) et les smartwatches (montres intelligentes) ont fait la une de l'actualité cette année, et nous nous attendons à l'émergence d'autres technologies nomades de ce type. Les compteurs électriques communicants sont déjà d'actualité et bientôt généralisés. Les études sur les attaques contre les systèmes industriels et les technologies de type SIA (Système d'Identification Automatique) montrent que les menaces étendent leur périmètre d'action. Nous devons ainsi nous tenir à l'affût des tendances et technologies émergentes pour être prêts à combattre les menaces qui les accompagneront.

Avant de se pencher sur les menaces futures, concentrons-nous sur les dangers du moment. À titre d'exemple, une de mes adresses électroniques personnelles a fait partie de la méga-fuite de données d'Adobe divulguée récemment. J'ai ainsi commencé à recevoir une multitude d'email de phishing. Heureusement, des années à évoluer dans la sécurité m'ont rendu extrêmement prudent, si ce n'est paranoïaque, jusqu'à examiner avec grande précaution tous mes courriers reçus, même ceux qui me paraissent légitimes. Et nous devrions tous en faire autant. Soyez très vigilants et ainsi protégés en 2014. Une petite dose de paranoïa peut s'avérer utile en matière de sécurité informatique !


Raimund Genes, CTO



La banque mobile sera la cible d'attaques de type MitM. L'authentification en deux étapes connaîtra ses limites.



Les menaces qui ciblent les transactions bancaires ont bondi en 2013. Au troisième trimestre 2013, le chiffre de 200 000 menaces identifiées a été dépassé, instituant ainsi un nouveau record.

Mais ces menaces mobiles ne se sont pas contentées de cibler les ordinateurs et ont proliféré dans l'univers mobile, donnant lieu à des usurpations d'applications bancaires légitimes, ou encore à des applications malveillantes qui imitent les outils d'authentification aux comptes et transactions bancaires.

Cet état des lieux rend obsolète l'authentification en deux étapes : alors que le grand public utilise davantage les équipements mobiles pour leurs opérations bancaires, les cybercriminels savent comment intercepter les codes d'authentification via des malware comme PERKEL et ZITMO.

Aux États-Unis, un utilisateur de smartphone sur 5 a accédé à des applications bancaires mobiles en 2013, et ce chiffre est attendu en très forte hausse dans les années à venir. 2014 sera l'année de la banque mobile, mais nous nous attendons également à une forte recrudescence des attaques de type man-in-the-middle (MitM) pour l'année à venir.

Android™ restera le système d'exploitation prédominant, mais cette position a un coût : nous nous attendons à ce que les applications malveillantes ou à risques ciblant Android franchissent le cap des 3 millions à la fin 2014. Bien que Google ait fait des efforts de sécurité, avec notamment le lancement d'Android KitKat, de nombreux utilisateurs de cette plateforme ne bénéficieront que tardivement des nouvelles fonctionnalités de sécurité, compte tenu d'un processus de mise à jour lent qui résulte de la forte fragmentation de cet OS.

De nouveaux systèmes d'exploitation tels que Tizen, Sailfish et Firefox sont attendus sur le marché mobile, dotés d'une couche de compatibilité avec Android. Cette couche permettra aux applications Android de fonctionner sur ces nouveaux OS, mais les cybercriminels évolueront plus facilement vers des menaces multiplateformes.



Les cybercriminels opteront pour des attaques ciblées, sur les applications open source ou via du spear phishing ultra-personnalisé, et multiplieront les exploits



Les cybercriminels, et notamment ceux qui mènent des attaques ciblées, ont pour objectif de détourner des informations de valeur. Les attaques ciblées sont caractérisées par leur persistance et une furtivité nécessaires à l'exfiltration de données sur le long terme.

Cette année, la [campagne Safe](#) a collecté 12 000 adresses IP uniques sur plus de 100 pays, en n'utilisant que deux infrastructures de serveur C&C. Ainsi, même les attaques mineures et les moins visibles peuvent porter sur des cibles très larges. Le succès des campagnes comme Safe a persuadé les cybercriminels d'adopter des techniques ciblées pour leurs attaques.

Des recherches récentes ont identifié environ 150 échantillons de menaces capables de tirer parti de la récente vulnérabilité zero-day de Microsoft ([CVE-2013-3906](#)), ce qui en fait une cible de choix pour 2014.

En 2014, les cybercriminels utiliseront davantage les attaques ciblées : la recherche de vulnérabilités au sein des solutions open-source et le spear phishing deviendront des standards auprès des cybercriminels.

Ces techniques d'attaques ciblées seront adoptées, pour leur taux de succès élevé, mais aussi parce qu'elles sont simples à exécuter et efficaces pour contourner les outils de sécurité traditionnels. Le spear phishing est plutôt simple, tandis que la création de malware à partir de kit d'exploitation s'effectue en quelques minutes. Enfin, c'est le comportement furtif des attaques ciblées qui rendent leur identification complexe.

Les vulnérabilités, notamment CVE-2012-0158 et CVE-2010-3333, continueront à être privilégiées par les pirates et cybercriminels, parce qu'elles sont simples à être exploitées. La vulnérabilité [CVE-2010-3333](#), par exemple, a été le bug de Microsoft® Word® le plus utilisé, jusqu'à l'apparition de la CVE-2012-0158.

À noter que les cybercriminels ne se contenteront pas de cibler les points faibles dans les logiciels et systèmes. Ils cibleront également l'humain, souvent considéré comme un maillon faible.



Nous assisterons à une poussée des attaques de clickjacking et de watering hole, de nouveaux exploits et à des attaques ciblant les dispositifs mobiles.

En 2013, Facebook a été la cible d'une attaque de type watering hole. Le coupable : un site de développement pour iPhone®. Les assaillants ont infecté une page pour ensuite en cibler les visiteurs. Cet incident témoigne qu'il existe des alternatives aux traditionnels emails avec fichier joint vérolé pour initier une attaque avec succès.

Le watering hole va se développer en 2014. Les assaillants redoubleront d'imagination pour attirer leurs victimes vers des sites infectés, en utilisant des techniques d'ingénierie sociale ou le clickjacking, et ainsi pirater les machines qui consulteront le site malveillant.

La vulnérabilité zero-day récente qui affecte Internet Explorer® (CVE 2013-3918) a déjà été utilisée dans le cadre d'une attaque qui a ciblé des individus intéressés par des « règles de sécurité nationales et internationales », ce qui est quelque peu ironique.

Alors que les vulnérabilités identifiées sur les OS seront moins nombreuses, les assaillants se positionneront davantage sur certaines suites logicielles, et notamment celles qui sont en fin de support chez leur éditeur, pour ainsi identifier de nouvelles vulnérabilités non patchées.

Les cybercriminels ne se contenteront plus de l'email en tant que vecteur d'attaque. Alors que la consommation a le vent en poupe en entreprise, ce sont les dispositifs mobiles personnels qui seront davantage ciblés pour s'immiscer au sein des réseaux corporate. On peut imaginer que même des équipements comme les smartwatches seront ciblés. En réalité, chaque équipement connecté au réseau devient une cible.





Les données restent une cible de choix pour les cybercriminels et les assaillants. Un récent incident de sécurité sur Adobe a entraîné le piratage de 150 millions de comptes selon les estimations. Avec, à la clé, un effet domino : d'autres éditeurs ont incité leurs utilisateurs à modifier leurs identifiants de connexion, si tant est que ces utilisateurs utilisaient les mêmes identifiants pour tous leurs comptes.

2013 a été marqué par de nombreux cas de piratage de données. Evernote a demandé à ses 50 millions d'utilisateurs de modifier leurs identifiants, après découverte que des hackers auraient pu avoir accès à ces informations. Le piratage subi par The Living Social porte sur 50 millions d'utilisateurs, tandis que Yahoo ! Japon a subi une fuite de données portant sur 22 millions d'identifiants.

Voilà typiquement le type d'incident appelé à se poursuivre en 2014. Les serveurs Web comme ceux impliqués dans l'incident d'Adobe, resteront des cibles d'attaques. Aucune organisation ne peut s'estimer à l'abri de tels actes qui, d'ailleurs, seront menés avec de nouveaux outils et en tirant parti de nouvelles vulnérabilités.

Les données détournées sont généralement « nettoyées » (personnalisation, restructuration, ciblage), avant d'être revendues au sein d'une économie souterraine. Par exemple, plutôt que de poster une liste brute sur un site public, les cybercriminels segmenteront cette liste selon des critères pertinents (lieu géographique, sexe, catégorie de revenus, etc.). Nous assisterons donc à de nouvelles méthodes créatives pour monétiser les données détournées, ce qui rendra le marché de la cybercriminalité encore plus concurrentiel et professionnel.



Un acte majeur de piratage de données par mois.



Les cybercriminels et les hackers sont en permanence à l'affût de vulnérabilités et, dans ce contexte, la fin du support pour Java 6 a été une opportunité en or en 2013.

Une vulnérabilité non patchée a ainsi permis une vague d'attaques. Cette menace a été intégrée dans le Neutrino Exploit Kit, connu pour infecter les machines par le biais de ransomware. Ce qui est troublant, c'est que les utilisateurs de Java sont nombreux (environ 50%) à en être resté à la version 6.

Les cybercriminels ont pour habitude d'assurer une retro-ingénierie des patches, pour identifier les vulnérabilités que sont censés pallier ces patches logiciels. Ils ciblent ainsi les versions anciennes et non supportées (donc non patchées) de ces logiciels et c'est sans doute ce qui s'est passé avec Java 6.

Les hackers tirent également parti des vulnérabilités de logiciels spécialisés. Par exemple, les vulnérabilités dans Adobe® ColdFusion®, utilisé pour concevoir des applications et des sites Web, ont été exploitées à de nombreuses reprises pour infiltrer des bases de données. Sur cette seule année, plusieurs actes malveillants ont ciblé des agences et instances liées à l'armée, aux gouvernements et à la recherche spatiale. Ces actes résultent d'accès illégitimes au code source de ColdFusion.

Alors que Microsoft prévoit l'arrêt officiel du support de Windows XP en 2014, on peut s'attendre à ce que le scénario pour Java 6 se reproduise sur XP. Nous pouvons nous attendre à des kits d'exploitation qui intégreront de nouvelles attaques et vulnérabilités Zero-day. Ceci est particulièrement inquiétant, puisque les PC sous XP ont 6 fois plus de chances d'être infectés par rapport aux autres versions de Windows. Ce chiffre ne peut qu'être orienté à la hausse lorsque la fin de support sera actée.

Certaines données laissent penser qu'environ 20% des utilisateurs de PC sont restés sur XP, ce qui représente un nombre important de victimes potentielles. D'autre part, il est estimé que la base installée de Windows XP compte plus de 300 millions de PC au sein des entreprises.

D'autre part, les systèmes embarqués, et notamment les terminaux de point de vente, les équipements de santé et les autres infrastructures critiques peuvent constituer des menaces car ils utilisent des versions anciennes de Windows. Les cybercriminels sauront tirer avantage de cette carence de support et utiliseront les vulnérabilités comme point d'entrée de leurs attaques.

Il faut d'ailleurs s'attendre à ce que les attaques qui ciblent ColdFusion continuent en 2014, compte tenu de leur efficacité.



***Intensification des
attaques qui utilisent des
vulnérabilités sur des
logiciels en fin de support
comme Java 6 et Windows
XP.***





Le Deep Web, réel défi pour les forces de l'ordre, qui, par ailleurs, seront freinées par la dimension internationale des réseaux criminels.



Le Deep Web est régulièrement à la une de l'actualité, avec, par exemple, le démantèlement de la place de marché souterraine Silk Road. Mais cette victoire reste mineure, puisqu'une nouvelle version de ce site a été identifiée un mois plus tard, suivie par d'autres places de marché qui s'enorgueillissent d'apporter « sécurité et anonymat » aux « commerçants » et aux acheteurs.

Contrer la cybercriminalité n'est pas simple, compte tenu d'une nature intrinsèquement différente de celle de la criminalité « classique ». Les forces de l'ordre ne disposent pas forcément de la méthodologie et des compétences adéquates pour neutraliser les cybercriminels, d'autant que certains freins émergent lors d'enquêtes internationales, les législations nationales étant hétérogènes.

En 2014, les cybercriminels utiliseront davantage le Deep Web qui favorise anonymat et non-traçabilité grâce aux réseaux Darknet. Le Darknet le plus populaire est TOR (The Onion Router), qui masque l'origine et la destination d'un transfert de fichier ou d'une navigation. Le Deep Web assure également la furtivité des cybercriminels, en évitant notamment l'indexation des contenus par les moteurs de recherche. Le contenu disponible sur le Deep Web n'est pas toujours accessible via l'Internet Public.

Les forces de l'ordre, qui n'ont pas toujours l'expertise et le savoir-faire pour lutter contre la cybercriminalité, sont souvent démunies lorsqu'il s'agit de poursuivre les cybercriminels dans le Deep Web. Ces économies souterraines inciteront les forces de l'ordre à investir davantage dans la lutte contre la cybercriminalité. Nous assisterons à de nouvelles initiatives de la part d'organisations internationales et de pays développés, qui sont davantage sensibilisés à la situation et prennent des mesures concrètes. Ces pays font appel à des experts pour former leurs forces de l'ordre. Quant aux pays émergents, ils ont environ 4 à 5 ans de retard par rapport à leurs homologues plus développés.



La méfiance du grand public s'accroîtra alors que les activités de surveillance des états sont dévoilées

Les documents confidentiels divulgués par Edward Snowden, ex-collaborateur d'un sous-traitant de la NSA américaine, illustrent que la confidentialité est particulièrement complexe à l'ère du numérique.

Le spyware n'est plus l'apanage de la cybercriminalité, et est utilisé par certains états à des fins d'espionnage politique. Les spyware sont aujourd'hui proposés à la vente, vantés en tant qu'outils pour espionner des conjoints infidèles par exemple. Cette généralisation du spyware, et de l'acte d'espionnage en lui-même, rendent quelque peu flous le distinguo entre ce qui est public et privé.

Les problématiques de confidentialité incitent les utilisateurs à la prudence. Par exemple, nos ados migrent de Facebook vers des applications de messagerie. Avec plus de 1,2 milliard d'utilisateurs de Facebook, certains ados jugent la confidentialité comme inexistante sur ce réseau. Ils s'orientent vers des applications de messagerie : notons par exemple la croissance exponentielle de WeChat, qui affiche un bond de 1 021% de sa base d'utilisateurs âgés de 16 à 19 ans. De son côté, l'appli de partage de photos, Snapchat, affirme assurer l'échange de 350 millions de prises de vues ou d'images par jour. Ce chiffre élevé est sans doute dû à la fonction de suppression automatique des contenus échangés, ce qui protège quelque part la confidentialité de l'utilisateur.

Notons également que les activités de surveillance de la part d'états, aujourd'hui rendues publiques, inciteront nombre de gens et d'entreprises à reconsidérer où ils/elles stockent leurs données. À la clé, une certaine méfiance vis-à-vis des infrastructures basées aux États-Unis. Cette problématique pourrait inciter certains états à reconsidérer leurs règles, notamment en matière d'utilisation d'Internet. Mais en dépit de l'indignation du grand public, nous nous attendons à un renforcement de ce type de surveillance au niveau des états.

Sur le terrain de la confidentialité, les fournisseurs de services cloud devront prouver qu'ils utilisent des contrôles de sécurité et des outils de protection des données confidentielles. Nombre de ces fournisseurs se rapprocheront d'acteurs spécialisés dans la sécurité pour leur déléguer la protection et la confidentialité des données et applications hébergées. Ceci alimentera la tendance du BYOC (bring-your-own-controls), qui rassurera les clients vis-à-vis du fait que leurs données sont segmentées, protégées et inaccessibles par des tiers.

Les utilisateurs voudront mieux contrôler leurs informations et préserver leur confidentialité, notamment sur des sites majeurs tels que Google et FaceBook. Ils opteront pour des outils pour contrôler les contenus personnels partagés en ligne, avec, par exemple, des outils de chiffrement et d'anonymat comme TOR qui garantissent la confidentialité de leurs données.

En 2014 et au-delà, nous assisterons également à des entreprises toujours plus nombreuses à commercialiser leurs données à des fins publicitaires. D'ailleurs les acteurs du traitement analytique du Big Data continueront à prospérer. Du côté des cybercriminels, ces derniers continueront à monétiser leurs données détournées et évolueront dans les arcanes des marchés souterrains.





Les menaces resteront mineures dans le domaine de l'Internet des Objets, mais émergeront dans ceux de la réalité augmentée et de l’Affichage Tête Haute

Alors que les équipements sont toujours plus interconnectés, leur sécurité impliquera de protéger tous les passerelles d'accès, et notamment Internet.

MEILLEURE SÉCURITÉ DES SYSTÈMES SCADA

Des recherches et constats témoignent des carences en sécurité que connaissent les systèmes industriels SCADA. Des efforts sont en cours pour pallier cette carence. Des programmes de correction de bugs ont été déployés, et les éditeurs/constructeurs disposent désormais d'équipes dédiées exclusivement à la sécurité des systèmes SCADA. En dépit de cette sécurité déficiente, le déploiement de systèmes SCADA se poursuit. Par exemple, L'Italie est passée aux compteurs intelligents, une voie qui devrait être suivie par le reste de l'Europe.

Mais les attaques visant les systèmes SCADA devraient se poursuivre, témoignant ainsi de la vulnérabilité de ces systèmes. Les réseaux SCADA se contentent trop souvent d'un cloisonnement physique pour se défendre, et deviennent ainsi des cibles privilégiées pour les cybercriminels.

DE NOUVELLES CIBLES VULNÉRABLES

De leur côté, ce sont les technologies de fréquences radio qui deviendront des cibles de prédilection pour les attaques. Souvent utilisées par les technologies de tracking de type SIA, les fréquences radio constitueront un nouveau point d'entrée des menaces. Les SIA sont souvent utilisés dans le cadre du trafic maritime, pour réguler les navires commerciaux et les paquebots. Ces systèmes pourraient bien devenir une prochaine cible pour des individus malintentionnés.

HARO SUR LES GAMERS

D'autres équipements connectés à Internet deviendront également des cibles. Le lancement de la Steam Machine, et du système d'exploitation SteamOS sous Linux, constituent un changement majeur sur le terrain des menaces pour les jeux. Si cette console devient aussi populaire que ses rivales, nul doute qu'elle sera la cible d'exactions mettant en péril sa sécurité. Le nombre de consoles de jeu est attendu à 165 millions à l'horizon 2017. Les gamers utilisent des ordinateurs très puissants. Cependant, c'est cette puissance de traitement qui est également exploitée et détournée pour le minage de bitcoins. Nous avons déjà assisté dans le passé à des tentatives de détournement de capacités informatiques pour le minage. Ces tentatives devraient se multiplier alors que cette monnaie virtuelle a le vent en poupe.





DANS L'ATTENTE DE LA PROCHAINE « KILLER APP »

Nous assisterons à de nombreuses évolutions techniques mineures, pas mais d'innovation majeure chez les cybercriminels. Ces derniers attendront la prochaine Killer App, à savoir cette innovation technologique qui saura attirer les foules. Alors que certains gadgets ont trouvé leur marché auprès du grand public, aucun d'entre eux n'a attiré l'attention du grand public comme l'a fait l'iPod à son époque.

AU-DELA DE 2014


La réalité augmentée pourrait bien devenir le prochain terrain de jeu des cybercriminels. Le casque à réalité augmentée constitue une technologie réellement disruptive, qui aura un impact majeur sur le terrain du gaming et qui sera également utilisée pour d'autres applications comme les conférences téléphoniques ou le post de contenus sur les réseaux sociaux.

Ces équipements intelligents se généraliseront au fil des années, et donneront lieu aux premières attaques de sécurités dans les deux années qui viennent. Le casque de RA deviendra un moyen pour détourner les informations personnelles. Leur camera intégrée sera utilisée pour pirater des données confidentielles, permettant aux cybercriminels de surveiller furtivement les activités quotidiennes de chaque utilisateur et un moyen d'enregistrer des informations personnelles, comme les code Pin bancaires par exemple.

Les drones seront davantage utilisés en matière de télésurveillance. Ils se généraliseront pour un usage commercial. Malheureusement, les cybercriminels sauront en tirer parti dans le cadre de leurs exactions.

Au-delà de 2014, les technologies de radiofréquence deviendront des cibles majeures d'attaque. Nous nous attendons par exemple à un piratage de station de transmission de SIA d'ici 2020, avec de lourdes conséquences pour le secteur de la navigation maritime.





Quelles conséquences pour le grand public et les entreprises ?

PROTÉGEZ VOTRE RÉSEAU

Les organisations doivent protéger leurs données cruciales et leur patrimoine numérique, car ce sont des cibles privilégiées. Les criminels essaieront de s'introduire dans les réseaux d'entreprise pour détourner ces données.

Hiérarchisez vos données et fichiers selon leur importance (éléments de propriété intellectuelle et base de données par exemple), pour ainsi définir les éléments qui exigent une protection supplémentaire et identifier les étapes pour déployer cette protection.

Les entreprises doivent intégrer l'idée que leur ligne de défense est perméable et qu'un intrus est peut-être déjà au sein des réseaux. Assurez-vous que votre entreprise utilise des règles et outils adéquats afin de protéger votre réseau. D'autre part, une formation appropriée des collaborateurs contribuera à réduire les risques de fuites de données.

Enfin, l'adoption de la consomérisation implique de définir et déployer des règles de sécurité pertinentes et exhaustives, pour tous les équipements. Les cybercriminels ciblent en effet tous les dispositifs susceptibles de servir de passerelle vers le réseau.

PROTÉGEZ VOS ÉQUIPEMENTS

Pour protéger vos données numériques, sécurisez tous les équipements à votre disposition. Le nombre d'applications Android malveillantes ou présentant de risques devrait atteindre 3 millions en 2014, ce qui fait de la sécurité de vos dispositifs Android une priorité. Mais la prolifération des dispositifs nomades ne doit pas pour autant vous amener à négliger la sécurité de vos machines de bureau. Installez et mettez à jour régulièrement les logiciels de sécurité afin de rester à l'abri des attaques, particulièrement celles qui tirent parti des vulnérabilités.

Puisqu'ils utilisent de nombreux dispositifs connectés, les particuliers doivent également penser à sécuriser leurs réseaux résidentiels, une étape essentielle de sécurité, et notamment des équipements qui ne disposent pas de fonctions de sécurité adéquate.

PROTÉGEZ VOTRE VIE PRIVÉE

Il est essentiel de garder à l'esprit que les cybercriminels veulent prendre la main sur les données personnelles et confidentielles, d'où une vigilance accrue lorsque vous accédez à vos comptes en ligne via un de vos dispositifs et lorsque vous devez utiliser des identifiants de connexion. Soyez conscient du volume et du type d'informations que vous partagez en ligne. Réfléchissez deux fois avant de poster quoi que ce soit en ligne. Lisez dans le détail les conditions d'utilisation des services auquel vous souhaitez souscrire, surtout si vous devez divulguer des informations de paiement.



Conditions d'utilisation de ce document

Les informations proposés dans ce document sont d'ordre général et à des fins de sensibilisation. Bien que Trend Micro ait pris soin de vérifier les informations présentes dans ce document, l'entreprise ne peut garantir pas leur parfaite exactitude et n'incite donc pas les lecteur à une prise de décision basés sur ce seul document. Ces informations ne constituent en aucun cas des conseils d'ordre juridiques et ne peuvent entraîner la responsabilité de Trend Micro.

Trend Micro Incorporated, un leader mondial des solutions de sécurité a pour mission de sécuriser les échanges d'informations numériques..
RDV sur www.trendmicro.com pour plus d'informations

©2013, Trend Micro, Incorporated. Tous droits réservés. Trend Micro, le logo t-ball Trend Micro et Trend Micro Smart Protection Network sont des marques commerciales ou des marques déposées de Trend Micro Incorporated. Tous les autres noms de produit ou de société peuvent être des marques commerciales ou déposées de leurs propriétaires respectifs.

Un document conçu par les

TrendLabs

Global Technical Support & R&D Center of **TREND MICRO**