ÉTUDE TECHNIQUE

Assurer la sécurité des entreprises mobiles

Stratégies pour réduire les vulnérabilités et les risques en matière de sécurité

Les enjeux de sécurité pour les ordinateurs, les utilisateurs, les applications et les données ont grandement évolué au cours des dernières années. À l'ère de l'informatique mobile, de l'approche « apportez votre propre appareil », des services d'informatique en nuage et des applications pour téléphones intelligents, il est non seulement essentiel d'apporter des solutions ciblées, mais surtout de proposer une stratégie globale de « défense en profondeur » pour protéger tous les services de l'entreprise.

Ces réalités ont toujours caractérisé la sécurité des TI en entreprise, mais aujourd'hui, les enjeux sont plus importants que jamais puisque les utilisateurs peuvent accéder à l'information en tout temps, n'importe où, sur n'importe quel appareil et sur tous les types de réseaux.

Ce document fait le point sur les vulnérabilités et les risques découlant des écosystèmes informatiques mobiles et présente les meilleures pratiques en vue de minimiser les pertes de données précieuses en cas d'attaque.

Table des matières

VUE D'ENSEMBLE 3

L'ÉCOSYSTÈME MOBILE 3

VULNÉRABILITÉS ET RISQUES 4

- Manquements à la sécurité causés par les utilisateurs 5
- Attaques d'authentification 5
- Stockage de données locales 6
- Détournement de sessions 7
- Faible niveau de sécurité lors de la transmission des données 7
- Faible niveau de sécurité du serveur 7

STRATÉGIES DE SÉCURITÉ 8

- Formation 9
- Protection des terminaux 10
- Cryptographie ROBUSTE 10
- Authentification multifactorielle 10
- Sécurisation des centres de traitement des données 12
- Pratiques optimales de codage 12
- Outils de gestion des postes mobiles 13

RÉPERCUSSIONS ET COMPROMIS 13

MENACES ÉVENTUELLES 14

CONCLUSION 14

Vue d'ensemble

À l'ère de la mobilité, la sécurité informatique d'entreprise n'est plus ce qu'elle était. Les différences observées de nos jours résultent essentiellement de l'évolution des ordinateurs en appareils personnels, comme le iPhone, le iPad et les produits Android, que les utilisateurs achètent par eux-mêmes (ou qui sont fournis par l'employeur) et utilisent au bureau à titre d'équipement auxiliaire ou de plateforme de travail principale. La rapidité du développement de logiciels et de matériel a grandement augmenté au cours de la dernière décennie et les utilisateurs ne veulent plus attendre que les services informatiques d'entreprise achètent les plus récents gadgets avant d'être en mesure de les utiliser. Aujourd'hui, les utilisateurs veulent se procurer ces appareils eux-mêmes, dans les jours ou les heures suivant leur lancement, et les apporter aussitôt au travail.

Ce scénario comporte beaucoup de risques. D'abord, les utilisateurs perçoivent l'appareil comme leur propriété plutôt que comme de l'équipement professionnel utilisé pour accéder à des systèmes et des données sensibles d'entreprise. Ainsi, ils ont tendance à prendre plus de risques en matière de sécurité que s'ils utilisaient de l'équipement strictement dédié au travail. Puis, il est probable que l'utilisateur installe plusieurs applications et jeux sur l'appareil, en plus de visiter des sites Web douteux pouvant en compromettre la sécurité. Enfin, puisque l'utilisateur apporte l'appareil partout, les risques de perte ou de vol sont plus élevés.

Il est essentiel de comprendre la portée du problème avant d'établir des stratégies pour y remédier. Dans la première section de ce document, nous explorerons l'ensemble de l'écosystème mobile d'entreprise. Nous découvrirons ensuite certaines vulnérabilités de cet écosystème ainsi que les risques qu'elles représentent. Dans la dernière section, nous observerons certaines stratégies de défense et d'atténuation afin de corriger ces vulnérabilités et de réduire les répercussions des risques qui en découlent.

En raison de la complexité de l'écosystème mobile d'entreprise, il s'avère essentiel de bien maîtriser cet environnement avant d'établir une approche complète en matière de sécurité.

L'écosystème mobile

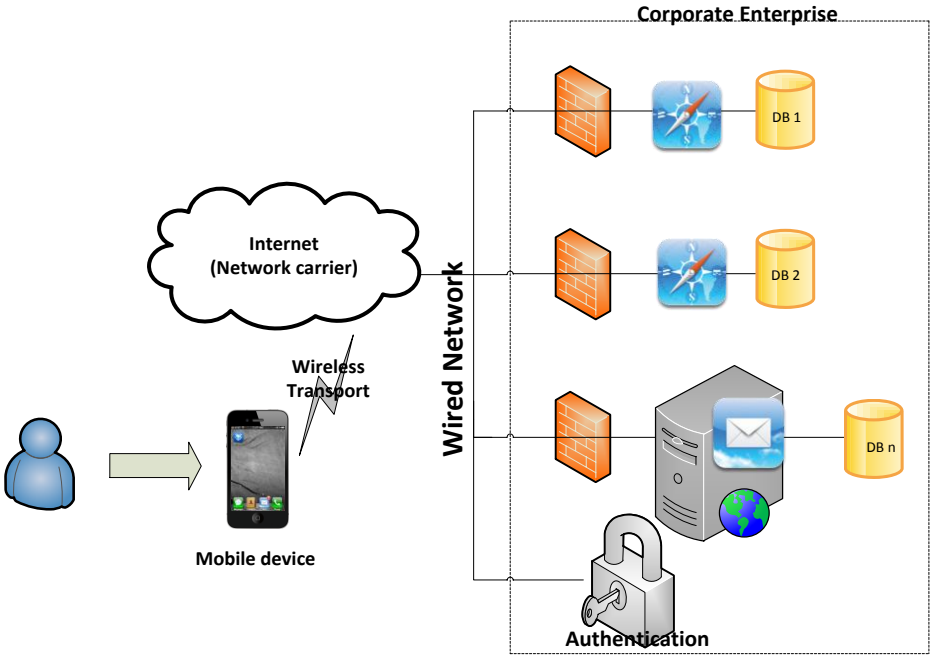
En raison de la complexité de l'écosystème mobile d'entreprise, il s'avère essentiel de bien maîtriser cet environnement avant d'établir une approche complète en matière de sécurité.

L'écosystème comprend quatre sous-systèmes principaux :

- **l'utilisateur final**;
- **l'appareil mobile** (matériel, système d'exploitation et applications);
- **l'entreprise** (serveurs, applications et services, sources de données);
- **le chemin d'accès réseau** (relie l'appareil mobile à l'entreprise : connexion WiFi locale ou communications cellulaires, opérateurs de réseaux, Internet, routeurs, etc.).

Pour assurer la sécurité de l'ensemble de l'écosystème mobile, il est essentiel de sécuriser ces quatre sous-systèmes. Chaque sous-système présente un ensemble distinct de vulnérabilités et requiert donc une solution de sécurité répondant à ses besoins.

Figure 1 – L'écosystème mobile d'entreprise



Vulnérabilités et risques

Le tableau ci-dessous dresse la liste des vulnérabilités les plus courantes et de l'emplacement où elles surviennent dans l'écosystème mobile.

Tableau 1 – Vulnérabilités dans l'écosystème mobile

	Utilisateur final	Appareil mobile	Chemin d'accès réseau	Entreprise
Manquements à la sécurité causés par les utilisateurs	•			
Attaques d'authentification	•	•	•	•
Stockage de données locales		•		
Détournement de sessions		•		•
Faible niveau de sécurité lors de la transmission de données			•	•
Faible niveau de sécurité du serveur				•

Observons brièvement chacune de ces vulnérabilités et les risques qui y sont associés. Certaines d'entre elles peuvent différer d'une plateforme mobile à une plateforme fixe, comme les ordinateurs portables et de bureau. Le cas échéant, nous présenterons les différences au besoin.

MANQUEMENTS À LA SÉCURITÉ CAUSÉS PAR LES UTILISATEURS

Lorsque les utilisateurs posent des gestes qui compromettent la sécurité, les résultats peuvent être désastreux. Il peut s'agir du partage de mots de passe à l'installation de logiciels non approuvés, comme de la sauvegarde de données sensibles non cryptées sur des appareils pouvant être perdus ou volés. Certains actes sont souvent non intentionnels ou résultent d'une ignorance des politiques d'entreprise, alors que d'autres sont délibérés et sont commis par une personne malveillante (p. ex. : attaques d'hameçonnage).

Les manquements à la sécurité causés par les utilisateurs compromettent souvent la sécurité d'un système et entraînent une perte de données ou un accès non autorisé à un système où sont stockées des données sensibles. Dans le pire des cas, la perte de données résulte d'une attaque au moyen d'un cheval de Troie ou d'un logiciel espion permettant à la personne malveillante d'accéder en permanence au réseau de l'entreprise. Ces attaques peuvent non seulement compromettre une partie des précieuses données, mais peuvent également permettre une visibilité à long terme de leur évolution et de leur emplacement. Cette visibilité à long terme peut également mener l'assaillant vers d'autres données sensibles stockées sur le réseau.

La perte ou le vol d'appareils mobiles constituent un autre type majeur de manquement à la sécurité par les utilisateurs. Lors d'un tel événement, les données stockées sur l'appareil sont à risque. Dans le meilleur des cas, ces données se limitent à l'historique des courriels, mais peuvent également comprendre des coordonnées professionnelles, des documents de travail (surtout sur les tablettes) et des données locales mises en cache extraites des serveurs de l'entreprise (consultez la section « stockage de données locales » ci-dessous).

Les manquements à la sécurité causés par les utilisateurs peuvent survenir sur n'importe quel type de plateforme. On peut soutenir qu'ils surviennent plus souvent – et entraînent des conséquences plus importantes – sur des systèmes traditionnels comme des ordinateurs portables et de bureau. D'une part, ces environnements sont plus susceptibles de contenir des composantes logicielles connues pour leur vulnérabilité, comme Flash ou Acrobat d'Adobe, Java, etc.[1] De plus, les courriels d'hameçonnage qui mènent à des attaques exploitent les vulnérabilités de ces composantes. Par conséquent, les plateformes qui ne supportent pas l'utilisation de telles composantes sont moins vulnérables à ce type d'atteintes à la sécurité.

ATTAQUES D'AUTHENTIFICATION

Les attaques d'authentification surviennent lorsqu'un assaillant tente de compromettre le système de sécurité en s'appropriant les données d'authentification d'un utilisateur. L'identification monofactorielle (identifiant et mot de passe) constitue une vulnérabilité depuis des décennies. Les vecteurs d'attaque

Les manquements à la sécurité causés par les utilisateurs peuvent survenir sur n'importe quel type de plateforme. On peut soutenir qu'ils surviennent plus souvent – et entraînent des conséquences plus importantes – sur des systèmes traditionnels comme des ordinateurs portables et de bureau.

[1] *Kaspersky Labs IT Threat Evolution Q3 2012*: http://www.securelist.com/en/analysis/204792250/IT_Threat_Evolution_Q3_2012 (en anglais)

comprennent notamment les attaques exhaustives, les essais-erreurs ciblés, le piratage psychologique ainsi que l'utilisation d'outils complexes comme des enregistreurs de frappe et autres.

Lors des attaques exhaustives, les assaillants volent les mots de passe cryptés des systèmes vulnérables. De récentes innovations technologiques ont contribué à simplifier et à accélérer les méthodes d'extraction de mots de passe en texte clair. Des tables arc-en-ciel permettent d'extraire une grande partie des mots de passe sans formule mathématique et les processeurs graphiques de certaines cartes vidéo pour jeux sont en mesure de traiter des dizaines, voire des centaines de milliards de possibilités de mots de passe à la seconde.[2] Cette technologie permet de trouver un mot de passe de huit lettres en quelques heures, et même en quelques minutes, sur un ordinateur personnel de moins de 2 000 $.[3] Ces capacités informatiques peuvent même être « louées » à l'heure par l'entremise de fournisseurs de services en nuage comme Amazon. Toute personne possédant une carte de crédit peut payer un tarif horaire pour utiliser des centaines ou des milliers de processeurs, tarif qui s'avère très bas aux heures creuses. L'informatique en nuage de cette nature permet aux pirates informatiques de disposer de superordinateurs virtuels à peu de frais et de risques.

Une attaque d'authentification réussie comporte le risque évident que l'assaillant consulte des données dont l'accès est limité à l'utilisateur. Lorsque les utilisateurs de confiance disposent d'un accès privilégié, l'exposition des données peut avoir des conséquences catastrophiques. Les attaques d'authentification peuvent survenir sur n'importe quel type de plateforme.

STOCKAGE DE DONNÉES LOCALES

Sur les appareils mobiles, les utilisateurs ne savent pas toujours quelles données sont stockées localement par les applications qu'ils utilisent. La plupart des applications stockent les données de la configuration de base, mais certaines effectuent une mise en cache locale des données téléchargées pour réduire l'utilisation du réseau ou le temps d'attente. Dans les systèmes d'exploitation mobiles, les données sont généralement dirigées vers un bac à sable afin que seule l'application utilisée pour les stocker puisse y accéder. Toutefois, si le système d'exploitation de l'appareil est compromis, il est possible d'accéder au contenu des bacs à sable, offrant ainsi un accès complet à toutes les données des applications stockées sur l'appareil. Même s'il ne s'agit que de données de configuration, la violation peut s'avérer importante. Imaginez les conséquences si l'application stockait localement les noms d'utilisateurs et les mots de passe!

Si une application mobile met en cache les données téléchargées et qu'un assaillant s'infiltre dans le bac à sable, ce dernier aura accès aux données d'entreprise téléchargées dans l'application. Bien que cette vulnérabilité ne soit pas

[2] http://blog.cryptohaze.com/2012/07/154-billion-ntlmsec-on-10-hashes.html (en anglais)
[3] http://hashcat.net/oclhashcat-lite/ (en anglais)

aussi grave que le vol des identifiants d'authentification, elle peut entraîner d'importantes fuites de données.

Les vulnérabilités associées au stockage de données locales sont beaucoup plus importantes sur les plateformes fixes que sur les plateformes mobiles, puisque l'architecture de type « bac à sable » a été implantée de façon générale sur les plateformes mobiles depuis leur entrée sur le marché (une pratique moins répandue sur les plateformes fixes). À la base, certains navigateurs Web (notamment Google Chrome) ont été conçus au moyen d'une architecture de type bac à sable, qui ne protège que des atteintes effectuées à partir du navigateur. L'infiltration des bacs à sable requiert généralement l'emploi de logiciels malveillants (maliciels) de routage sophistiqués, ce qui réduit le nombre d'assaillants détenant les compétences techniques requises pour s'en prendre à la plateforme.

DÉTOURNEMENT DE SESSIONS

Le détournement de sessions survient lorsque les identifiants de session sont employés dans une application Web une fois que l'utilisateur est identifié et que l'assaillant a accès à ces identifiants. Ces attaques surviennent généralement lorsque l'application Web utilise une adresse URL qui contient les identifiants de session après l'authentification. Les utilisateurs ont ensuite accès à l'identifiant de session et peuvent partager (de façon intentionnelle ou non) ces données en copiant et collant l'URL dans un courriel ou un message texte. L'assaillant peut également lire l'URL sur un appareil compromis en accédant à l'historique du navigateur. Le détournement de sessions est observé aussi bien dans les environnements fixes que les environnements mobiles.

FAIBLE NIVEAU DE SÉCURITÉ LORS DE LA TRANSMISSION DES DONNÉES

Les interfaces de programmation d'applications (API) Web devraient toutes employer un protocole TLS (protocole de sécurité de la couche transport), anciennement appelé protocole SSL (couche de sockets sécurisés). Cette technologie grandement répandue encode les communications entre le client et le serveur. Bien que le niveau de sécurité qu'offre cette technologie soit présentement remis en question, son application constitue une précaution de base qui pourrait s'avérer suffisante. À tout le moins, l'utilisation d'un protocole TLS/SSL augmente le niveau de difficulté pour les assaillants en compliquant l'accès aux données des réseaux par le repérage d'erreurs et d'autres attaques du chemin d'accès.

FAIBLE NIVEAU DE SÉCURITÉ DU SERVEUR

L'aspect serveur d'une application client-serveur doit essentiellement être sécurisé pour atteindre un niveau de sécurité d'ensemble adéquat. Cette démarche requiert l'apport de tous les correctifs nécessaires au système d'exploitation et à l'application, le renforcement des serveurs accessibles de l'extérieur, la configuration de pare-feu et de systèmes de détection d'intrusion, etc. Il faut également accorder de l'importance à la conception du système pour que l'accès aux données s'effectue au moyen d'interfaces bien définies sur des appareils

L'aspect serveur d'une application client-serveur doit essentiellement être sécurisé pour atteindre un niveau de sécurité d'ensemble adéquat… Si cette condition n'est pas respectée, les assaillants disposent d'un accès pratiquement illimité au réseau de l'entreprise et aux données qui y sont stockées.

renforcés pour éviter les violations de grande envergure exposant des bases de données entières.

Si l'aspect serveur de l'application n'est pas correctement sécurisé, les assaillants disposent d'un accès pratiquement illimité au réseau de l'entreprise et aux données qui y sont stockées. Toute démarche en matière de sécurité d'ensemble de l'architecture devrait débuter par la sécurisation des serveurs.

Stratégies de sécurité

L'unique stratégie valable consiste à remédier directement à l'ensemble des vulnérabilités. Une telle stratégie devra combiner technologie, formation et processus dans un effort concerté visant à sécuriser les systèmes vulnérables, à réduire la surface exposée à des attaques potentielles et à limiter les dommages causés en cas d'attaque réussie.

Par le passé, il a été démontré qu'aucun système informatique connecté à un réseau n'est sécuritaire à 100 %. C'est pourquoi un bon paradigme de sécurité doit débuter par la prise de conscience qu'une attaque réussie est possible et par l'intégration de mécanismes de défense en mesure de déterminer qu'une telle attaque est survenue (ou mieux encore, de la détecter lorsqu'elle est en cours) pour ensuite la contrer, isoler les systèmes compromis et freiner la perte de données engendrée.

Le maintien de l'intégrité du système est également essentiel à des fins d'enquête. L'intégrité aide à identifier le vecteur d'attaque et à prendre les mesures nécessaires pour remédier aux vulnérabilités en cas d'attaques ultérieures.

Le tableau 2, ci-dessous, dresse la liste des stratégies à adopter pour atténuer chacune des vulnérabilités exposées dans la section précédente. Certaines stratégies s'appliquent à plus d'une vulnérabilité, comme l'indique la présence du signe « • » dans la case d'intersection.

Comment [WU1]: There is a mistake in the English version, it should read Table 2 (currently Table 1).

Tableau 2 – Stratégies d'atténuation

	Formation	Protection des terminaux	Cryptographie accrue	Authentification multifactorielle	Sécurisation des centres de traitement des données	Pratiques optimales de codage	Outils de gestion des postes mobiles
Manquements à la sécurité causés par les utilisateurs	•	•					•
Attaques d'authentification			•	•		•	
Stockage de données locales		•	•			•	•
Détournement de sessions	•		•	•		•	
Faible niveau de sécurité lors de la transmission de données	•		•				
Faible niveau de sécurité du serveur					•	•	

Abordons maintenant chacune des stratégies d'atténuation des vulnérabilités pour comprendre comment elles contribuent à réduire la surface d'attaque ou les répercussions d'une attaque fructueuse.

FORMATION

Il s'agit certainement de la plus importante stratégie pour accroître la sécurité d'une entreprise. Même le système le mieux sécurisé est vulnérable tant que ses utilisateurs écrivent leurs mots de passe, partagent leurs comptes, accèdent à des réseaux suspects, transfèrent leurs données d'un appareil à un autre au moyen de dispositifs USB infectés, installent des maliciels ou exposent leurs ordinateurs à des attaques d'hameçonnage. Les informaticiens n'échappent pas non plus à cette vulnérabilité s'ils ne se méfient pas des attaques de piratage psychologique.

La seule façon de réduire la surface d'attaque consiste à former les utilisateurs afin de les aider à adopter de meilleures pratiques en matière de sécurité pour cerner (et éviter) les attaques potentielles. La plupart des organisations ont mis en place des politiques pour empêcher les utilisateurs de poser des gestes, en apparence anodins, mais qui s'avèrent peu judicieux, à l'endroit des actifs de TI d'entreprise. Cependant, de nombreux programmes de formation omettent d'expliquer pourquoi ces gestes comportent des risques et les utilisateurs ont tendance à ignorer les politiques qu'ils jugent indûment restrictives. Pour que les employés prennent les politiques au sérieux, ils doivent d'abord comprendre la nature des vulnérabilités causées par leurs gestes. De plus, dans un contexte où les menaces de sécurité évoluent rapidement, la formation en matière de sécurité doit être renouvelée fréquemment et les utilisateurs doivent se tenir au fait des menaces actuelles et antérieures.

Finalement, les professionnels de la sécurité TI doivent communiquer de façon régulière avec les utilisateurs, surtout lorsque de dangereuses menaces apparaissent à l'improviste. Plusieurs menaces émergentes peuvent être évitées en présentant la nature de ces menaces aux utilisateurs et en leur demandant de rester à l'affût jusqu'à ce qu'un correctif soit déployé.

PROTECTION DES TERMINAUX

La protection des terminaux regroupe un éventail de technologies visant à sécuriser l'appareil de l'utilisateur. Depuis leur apparition, ces technologies ne sont offertes que pour les ordinateurs portables et de bureau, mais on s'attend à ce qu'elles conquièrent le marché des appareils mobiles sous peu. La protection des terminaux comprend des fonctionnalités antivirus et antimalicielles et contribue également à éviter la perte de données, à renforcer les politiques, à filtrer le contenu et à optimiser le pare-feu.

Il n'est cependant pas raisonnable de s'attendre à ce que toutes ces fonctionnalités soient mises en marché à court terme pour les appareils mobiles. Les systèmes d'exploitation de ces appareils ne comportent pas le seuil d'accès requis pour effectuer certaines tâches (p. ex. : l'inspection des paquets des réseaux, le balayage de fichiers, etc.) et les appareils eux-mêmes ne sont pas assez puissants pour exécuter certaines tâches sans s'imposer une charge trop lourde. Nous recommandons toutefois aux entreprises d'installer sur leurs appareils certains outils antivirus et antimaliciels de base déjà sur le marché. Il y a peu de chances que nous soyons en mesure de déployer de tels logiciels sur nos appareils personnels.

CRYPTOGRAPHIE ROBUSTE

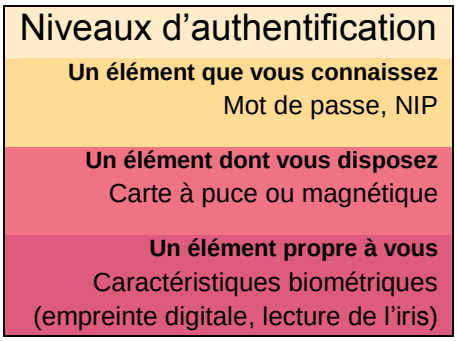
Appliquée régulièrement, une cryptographie robuste peut contribuer à atténuer la plupart des menaces énoncées dans ce document. Une solution cryptographique conçue adéquatement permet de protéger les données en transfert ou inactives, réduisant ainsi la surface d'attaque des données stockées localement ou de la couche réseau. Une cryptographie accrue est également essentielle à la prévention des attaques d'autorisation (en évitant de transmettre en clair des identifiants d'authentification) et joue un rôle de premier plan dans la prévention des détournements de sessions (en exigeant des communications de données adéquatement cryptées pour toutes les sessions). Les solutions cryptographiques peuvent également être employées pour lier les données aux applications, aux sessions et à une authentification rigoureuse des utilisateurs et des appareils, renforçant ainsi le bac à sable pour assurer que seules les applications autorisées puissent accéder aux données.

AUTHENTIFICATION MULTIFACTORIELLE

Un contrôle accru de l'accès aux ressources constitue la base d'une sécurité adéquate. Cette approche requiert un certain niveau de confiance en l'identité des utilisateurs qui accèdent au système. À cet effet, l'authentification monofactorielle (nom d'utilisateur et mot de passe) est inadéquate pour se protéger des menaces constantes et complexes de l'environnement actuel. Deux, voire trois facteurs

Un contrôle accru de l'accès aux ressources constitue la base d'un niveau de sécurité adéquat. Cette approche requiert un certain niveau de confiance en l'identité des utilisateurs qui accèdent au système. À cet effet, l'authentification monofactorielle (nom d'utilisateur et mot de passe) est inadéquate pour se protéger des menaces complexes constantes de l'environnement actuel.

d'authentification sont requis pour empêcher les assaillants d'accéder aux systèmes en s'appropriant ou en détournant les identifiants d'authentification.



Les systèmes bifactoriels consistent non seulement à identifier l'utilisateur au moyen d'un renseignement secret, d'où la méthode « un élément que vous connaissez », mais appliquent également la formule « un élément dont vous disposez » ou « un élément propre à vous », forçant ainsi l'assaillant à s'identifier au moyen d'un élément concret. À titre d'exemple, un utilisateur doit disposer à la fois de la bande magnétique et du NIP à quatre ou cinq chiffres d'une carte de guichet pour l'utiliser. La clé cryptographique (RSA, SafeNet, Entrust, etc.) constitue un autre bon exemple de cette approche. Cet outil oblige l'utilisateur à inscrire un nombre à plusieurs chiffres affiché sur un petit dispositif électronique qu'il a en sa possession. Dans cet exemple, les chiffres du dispositif constituent « l'élément dont vous disposez », alors que le mot de passe ou le NIP de l'utilisateur constitue « l'élément que vous connaissez ».

De nos jours, des systèmes trifactoriels sont offerts dans le domaine de la sécurité physique. Ils misent sur les approches « un élément que vous connaissez » et « un élément dont vous disposez » décrites ci-dessus, mais emploient également un « élément propre à vous » supplémentaire, qui prend généralement la forme d'une empreinte digitale ou d'une lecture de l'iris. Bien que leur utilisation soit complexe pour l'utilisateur, ces systèmes ont été implantés dans l'univers électronique, notamment au sein du gouvernement américain, dans le cadre du programme CAC (carte d'accès commune) du département de la Défense. Ce programme requiert l'insertion d'une carte dans un lecteur annexé aux ordinateurs des utilisateurs, parfois combiné à un lecteur d'empreintes digitales pour intégrer les trois facteurs de contrôle d'accès.

Cette approche pour le moins rigoureuse en matière de sécurité trifactorielle n'est pas nécessairement réaliste pour les entreprises souhaitant authentifier des utilisateurs mobiles. Par contre, de nouvelles technologies d'authentification trifactorielle ne requérant pas l'utilisation de matériel supplémentaire par l'utilisateur

sont en train de voir le jour. La solution QuadroVoice™ de CGI fait partie de ces technologies.

SÉCURISATION DES CENTRES DE TRAITEMENT DES DONNÉES

Nous pourrions facilement rédiger des articles complets sur la sécurisation des centres de traitement des données. C'est pourquoi nous n'aborderons que brièvement la question dans ce document. Il suffit de rappeler que l'intrusion dans des serveurs qui stockent et acheminent les données sensibles d'entreprise marque la fin de la partie et la victoire des assaillants. À l'image de cambrioleurs qui dévalisent une banque, les pirates s'en prennent aux serveurs d'entreprise parce que c'est à cet endroit que les données les plus précieuses sont stockées.

Par ailleurs, la configuration des serveurs et des centres de données (y compris l'emplacement physique, les adresses IP, les pratiques de sécurité, etc.) ne change que très lentement, ce qui permet aux assaillants d'identifier leur cible, d'établir une stratégie d'attaque et de poursuivre les attaques jusqu'à ce que leur objectif soit atteint. Les appareils mobiles, quant à eux, changent souvent d'emplacement et d'adresse IP, généralement jusqu'à plusieurs fois par heure pour un appareil utilisé par quelqu'un qui se déplace sur une autoroute. Pour cette raison, il est difficile pour les assaillants d'attaquer les appareils mobiles à l'aide des mêmes outils utilisés pour attaquer les centres de données.

Un centre de traitement des données adéquatement sécurisé comprend, entre autres, des pare-feu, des systèmes de détection d'intrusion et des systèmes de surveillance des réseaux. Une telle installation requiert également d'excellentes pratiques en matière de configuration, des logiciels dotés des plus récents correctifs de sécurité, une exposition minimale des ports et des services ainsi qu'une stratification optimale des serveurs et des API. Toute entreprise souhaitant diffuser des données sensibles par l'entremise d'Internet doit embaucher des professionnels de la sécurité pour superviser la sécurisation de ses centres de traitement des données afin de s'assurer que ces systèmes sont adéquatement protégés.

PRATIQUES OPTIMALES DE CODAGE

Les développeurs de logiciels tiennent rarement compte de la sécurité à moins qu'ils n'y soient obligés. Les entreprises qui développent des solutions internes doivent donc offrir de la formation visant à établir les meilleures pratiques en matière de sécurité et à évaluer le niveau de sécurité des solutions avant leur mise en œuvre. Une pratique de codage adéquate s'avère essentielle pour éviter les attaques massives par injection SQL et par débordement de la mémoire tampon, les infiltrations des caches locales, les attaques d'authentification, le détournement de sessions, etc.

Le traitement complet du présent sujet dépasse la portée de cet article. Par contre, d'excellents ouvrages sur la question sont offerts et plusieurs firmes accréditées offrent de la formation technique à cet effet.

Si votre entreprise effectue le développement interne d'applications destinées à des systèmes reliés à Internet (client ou serveur), vous devez assurer la formation de vos développeurs et veiller à ce qu'ils se conforment aux politiques. Si vous

Les développeurs de logiciels tiennent rarement compte de la sécurité à moins qu'ils n'y soient obligés. Les entreprises qui développent des solutions internes doivent donc offrir de la formation visant à établir les meilleures pratiques en matière de sécurité et à évaluer le niveau de sécurité des solutions avant leur mise en œuvre

externalisez le développement, il s'avère tout aussi important d'examiner les stratégies et politiques de sécurité de votre fournisseur.

OUTILS DE GESTION DES POSTES MOBILES

Les outils de gestion des postes mobiles permettent aux entreprises de surveiller l'état des appareils, c'est-à-dire de vérifier quelles applications y sont installées, quelles mesures de sécurité y sont appliquées, quels sites Web y sont autorisés, etc. L'une des plus importantes fonctionnalités offertes par de tels outils s'avère probablement la capacité d'effacer à distance le contenu d'un appareil perdu ou volé. Il n'est peut-être pas facile de convaincre les utilisateurs de laisser leur employeur installer ces logiciels sur leurs appareils personnels, mais l'élaboration de politiques sensées par l'entreprise peut contribuer à apaiser leurs craintes. Les entreprises qui fournissent des appareils mobiles à leurs employés devraient envisager la mise en œuvre d'une solution de gestion des postes mobiles par un fournisseur reconnu comme Good, ManageEngine, Airwatch ou IBM.

En plus des solutions de gestion des postes mobiles, une nouvelle technologie prometteuse a vu le jour en 2012. AT&T offre désormais une application de commutation d'environnement appelée Toggle. Cet outil permet à l'utilisateur de diviser l'appareil mobile en deux partitions distinctes : une pour le travail et une pour l'utilisation personnelle. Les applications et les données installées sur une partition ne sont pas visibles sur l'autre et vice-versa. Les utilisateurs peuvent ainsi installer Angry Birds, Facebook et autres applications de ce genre sur la partition personnelle et stocker les données et les applications de travail sur l'autre partition. Puisque les deux partitions sont complètement séparées, une application indésirable installée sur la partition personnelle ne pourrait accéder aux données ou à la configuration de la partition professionnelle. Cette dernière peut aussi être gérée par le service TI de l'entreprise afin que son accès soit restreint – une procédure qu'un utilisateur n'accepterait pas que l'on applique, en temps normal, à son appareil personnel.

Il est fortement conseillé aux entreprises qui adoptent l'approche « apportez votre propre appareil » de déployer Toggle ou l'un de ses futurs concurrents sur les appareils des employés. Cette technologie contribue à réduire davantage les répercussions des activités malicieuses sur les appareils mobiles de l'entreprise.

Répercussions et compromis

Le processus visant à sécuriser complètement les plateformes mobiles requiert la création d'une image sécurisée du système d'exploitation, comme Android SE (« Security Enhanced »). Cette stratégie devrait être employée conjointement avec d'autres outils spéciaux tels que Toggle, une solution antimalicielle pour appareils mobiles. Le défi pour le personnel de soutien d'entreprise réside dans le fait que les utilisateurs veulent le logiciel le plus récent et le plus performant, tandis que les images de systèmes d'exploitation spécialisées ont de la difficulté à suivre le rythme de renouvellement des images prêtes à l'emploi et peuvent accuser un retard de 12 mois ou plus. En outre, les tâches de base d'un logiciel antivirus peuvent compromettre les capacités d'un appareil à faible puissance comme un téléphone

mobile. Lorsque réunies, ces approches ne sont généralement pas approuvées par les utilisateurs, surtout s'ils sont propriétaires de l'appareil.

Les services TI d'entreprise doivent plutôt miser sur une combinaison de techniques afin de remédier au plus grand nombre de vulnérabilités possible sans empêcher les utilisateurs d'employer leurs appareils. Cette approche requiert de la formation, de la conteneurisation, les meilleures pratiques en matière de conception, le codage de toutes les composantes d'une solution d'entreprise, etc. Lorsque respectée, cette approche contribue à réduire la surface de menace et à minimiser les répercussions d'une attaque sans perturber le travail de l'utilisateur.

Menaces éventuelles

Les menaces ne cessent d'évoluer. Même si nous nous protégeons contre les menaces et vulnérabilités actuelles, nous devons demeurer à l'affût des technologies émergentes et des vulnérabilités potentielles qui y sont associées. Par exemple, il semble évident que la communication en champ proche (NFC) deviendra plus répandue sur les appareils mobiles au cours des prochaines années. Même si cette technologie a surtout été conçue pour les solutions de paiement, elle signifie tout de même qu'un autre émetteur sera ajouté aux appareils mobiles et que cet émetteur assurera la transmission et la réception de données. En plus des vulnérabilités associées à ces transmissions, il faut s'attendre à ce que les assaillants s'en prennent à la plateforme mobile en espérant mettre la main sur des données leur permettant d'accéder directement aux comptes bancaires de l'utilisateur. Bien que cette menace ne compromette pas nécessairement l'environnement informatique d'une entreprise, elle poussera assurément les développeurs de maliciels à cibler davantage les plateformes mobiles.

Le personnel TI des entreprises devra absolument tenir compte de la surface de menace des plateformes mobiles et aider les utilisateurs à protéger leurs appareils. Les mesures de protection des appareils mobiles doivent évoluer au même rythme que celles des ordinateurs portables et de bureau des entreprises.

Conclusion

L'effectif moderne s'attend à pouvoir travailler n'importe où et en tout temps, en plus d'accéder aux ressources et aux données d'entreprise sur n'importe quelle plateforme. De nos jours, la plupart des grandes entreprises comprennent la valeur de ce modèle, mais sont préoccupées par la perte ou le vol de données d'entreprise.

Pour réduire la menace à un niveau tolérable, les services informatiques d'entreprises devraient adopter une stratégie globale de « défense en profondeur » visant à remédier à l'ensemble de la chaîne de vulnérabilités. Ces dernières touchent l'utilisateur, l'appareil, le réseau, le serveur du centre de traitement des données et les piles d'applications qui l'utilisent.

Chacun des maillons de la chaîne présente un ensemble distinct de vulnérabilités qui requièrent des stratégies précises pour réduire la surface de menace. Ces stratégies comprennent la formation des utilisateurs, la protection des terminaux,

À PROPOS DE CGI

Grâce à ses 69 000 membres présents dans 400 bureaux établis dans 40 pays, CGI met en place des équipes locales, responsables du succès des clients, tout en mettant à leur portée un réseau mondial de prestation de services.

Fondée en 1976, CGI applique une approche rigoureuse afin d'afficher un bilan inégalé de projets réalisés selon les échéances et budgets prévus.

Nos services-conseils en management ainsi que nos services d'intégration de systèmes et d'impartition de grande qualité aident nos clients à tirer profit de leurs investissements tout en adoptant de nouvelles technologies et stratégies d'affaires.

Grâce à cette approche, au cours des 10 dernières années, la note moyenne de satisfaction de nos clients a constamment dépassé 9 sur 10.

Pour plus d'information à propos de CGI, visitez **www.cgi.com** ou écrivez-nous à **info@cgi.com**.

une cryptographie accrue, une authentification multifactorielle, la sécurisation des centres de traitement des données, des pratiques optimales de codage et des solutions de gestion des postes mobiles.

En résumé – Établir un niveau de sécurité approprié tout en soutenant le travailleur mobile exige la prise en compte des vulnérabilités propres à tout le contexte des télécommunications mobiles et l'adoption en entier ou en partie de toutes les stratégies énoncées dans ce document.