



EDITORIAL p 1

AGENDA p 1

ACTUALITES p 2

L'ESSENTIEL p 3

UN PATCH POUR RENFORCER LE NOYAU GNU/LINUX : GRSECURITY

Comment améliorer la sécurité d'un serveur Linux ? L'un des avantages de l'open source est qu'il procure l'accès au code source du système d'exploitation, ce qui permet de le modifier. L'intégration de Gsecurity au noyau offre une boîte à outils pour renforcer considérablement la sécurité du noyau Linux.

ZOOM p 6

LA SECURISATION DES TERMINAUX MOBILES [2/2]

La gestion des risques qui pèsent sur une flotte de smartphones / PDA doit avant tout être définie par une politique de sécurité la plus complète possible. Celle-ci peut s'appuyer sur une solution de gestion de flotte mobile qui permettra de s'assurer du respect des règles de sécurité lors du déploiement des terminaux.

EDITORIAL

**« Les empires ont leurs crises
comme les montagnes ont leur hiver.
Une parole dite trop haut
y produit une avalanche. »**

Victor Hugo « Littérature et philosophie mêlées (1834) »

La crise financière américaine aura finalement réussi à se propager au monde entier pour devenir une crise économique de très forte ampleur qui va marquer l'année 2009. Cette crise soumet l'économie à rude épreuve et constitue un risque pour les activités de nos entreprises.

Les situations de crise forcent les entreprises à recentrer leurs activités sur leur cœur de métier et à mettre en œuvre les moyens pour s'assurer de leur pérennité et de leur fiabilité afin de tenir bon pendant toute la durée de ces turbulences. Les informations liées à ces activités et les systèmes qui les traitent, constituent une part importante du patrimoine et l'outil de travail des entreprises. Leur sécurité est de plus en plus impérieuse afin que soient évités les risques qui feraient s'échouer l'entreprise sur les écueils de l'économie.

Le management des risques de sécurité de l'information a permis aux entreprises d'anticiper, avant la crise, les risques de sécurité pouvant survenir dans leurs systèmes d'information en mettant en place les mesures et les organisations nécessaires à s'en prémunir. Il ne leur reste plus qu'à s'assurer que rien n'a été oublié (par exemple, la sécurité des serveurs Linux ou celle des terminaux mobile évoqués dans cette newsletter) et que le vent glacial de l'hiver ne pourra pas trouver d'ouverture pour s'infiltrer.

Il ne faut pas oublier que l'hiver est également le signe d'un renouveau ; la nature fait une pause pour mieux reprendre sa croissance. L'an nouveau nous le dit aussi : tous les vœux que nous nous échangeons nous rappellent à l'espérance de jours plus beaux qui, comme l'été, reviendront de manière inéluctable.

**Aussi, toute l'équipe de l'ESEC
vous adresse
ses meilleurs vœux
pour l'année 2009.**

AGENDA

« La lutte informatique offensive » séminaire ESEC - Paris, 3 février 2009

Pour sa deuxième édition, l'équipe R&D de l'ESEC présentera les résultats de ses recherches sur la thématique de la lutte informatique. Le concept de « Lutte informatique Offensive (LIO) » porte sur les moyens d'attaquer les SI dans le but d'en prendre le contrôle, d'en extraire des informations confidentielles ou encore de les mettre hors d'état de fonctionner.

➤ Plus d'infos : <http://esec.fr.sogeti.com/seminaire/index.html>

Black Hat - Washington DC, 16-19 février 2009

Les briefings et trainings de Black Hat se tiendront à Washington sur les thèmes des dispositifs embarqués, du *reverse engineering*, de la sécurité des applications et de la protection des réseaux.

➤ Plus d'infos : <http://www.blackhat.com>

Secure IT 2009 Conference - Los Angeles, 4-6 mars 2009

Cette 7^{ème} édition de la conférence s'enrichit de sessions sur le management de la sécurité, sur les technologies et pratiques opérationnelles pour la sécurité de l'information et sur le développement de la recherche.

➤ Plus d'infos : <http://secureitconf.com/index.asp>

ACTUALITÉS

Un patch en urgence pour Internet Explorer

Une vulnérabilité du navigateur Internet Explorer de Microsoft, permettant l'exécution de code à distance, a conduit à une procédure exceptionnelle pour livrer rapidement un patch.

Effectivement, les premières attaques utilisant cette vulnérabilité ont commencé le 9 décembre : plus de 10 000 sites Web et des millions d'ordinateurs ont été

infectés avant la mise à disposition du patch.

Des chercheurs chinois auraient diffusé par erreur le code permettant d'exploiter cette vulnérabilité. Ce code se serait revendu jusqu'à 15 000\$.

La contamination a été tellement forte que certains spécialistes en ont appelé à utiliser d'autres navigateurs concurrents

d'Internet Explorer tels que Firefox, Opera, Chrome...

Microsoft n'a pas attendu le rendez-vous habituel du deuxième mardi du mois pour livrer ce patch et l'a diffusé dès le 17 décembre.

Pour en savoir plus :

http://www.microsoft.com/protect/computer/updates/bulletins/200812_oob.msp



Rapport de sécurité annuel - Cisco 2008

Cisco a publié son rapport annuel sur la sécurité dans lequel il met en exergue les menaces et les enjeux de sécurité, parmi lesquels il souligne les points suivants :

- Le spam représente 200 milliards de messages par jour, ce qui représente 90% des emails envoyés dans le monde.
- Le nombre de vulnérabilités détectées a augmenté de 11,5% par rapport à 2007.

Le nombre de vulnérabilités liées aux produits de virtualisation a triplé par rapport à 2007.

Les menaces initiées depuis des domaines légitimes ont augmenté de 90% par rapport à 2007.

Heureusement, les réponses à ces menaces s'améliorent grâce principalement à la meilleure collaboration entre les industriels et les chercheurs en sécurité

pour identifier, étudier et combattre les vulnérabilités.

Pour en savoir plus :

http://www.cisco.com/en/US/prod/vpndev/c/annual_security_report.html



Des fuites, toujours des fuites

Après les fichiers perdus en Angleterre, c'est au tour de l'Allemagne de défrayer la chronique.

Un trafic de CD-Rom contenant les noms, adresses, numéros de compte et domiciliation bancaire de 21 millions de particuliers allemands a été dévoilé par la

presse. Ce trafic s'élèverait à plus de 12 millions d'euros.

Ces informations auraient été obtenues par le biais d'employés peu scrupuleux de « calls centers » qui ont subtilisé ces informations, à l'aide de clés USB, avant de les revendre au plus offrant.

Pour en savoir plus :

http://www.silicon.fr/fr/news/2008/12/08/donnees_personnelles_nouveau_scandale_en_allemande



Faux avis de sécurité Microsoft

Le portail de la sécurité informatique du gouvernement met en garde contre les faux avis de sécurité Microsoft.

Un faux avis de sécurité Microsoft a été diffusé par messagerie avec le titre « Avis de sécurité Microsoft (951306) », qui invite les destinataires à exécuter la pièce jointe.

Cette pièce jointe est un cheval de Troie qui enregistre les données sensibles (mots de passe) et les envoie aux pirates à l'origine de l'attaque.

La DCSSI rappelle que « Microsoft ne diffuse jamais de correctifs par messagerie. Ils sont disponibles par la fonction de mise à jour de votre

ordinateur, soit à la demande, soit par mise à jour automatique. »

Pour en savoir plus :

<http://www.securite-informatique.gouv.fr/>



Guerre de l'information et lutte informatique : état des lieux et enjeux

L'Institut des Hautes Études de la Défense Nationale (IHEDN) a organisé en fin d'année 2008, à l'École Militaire une table ronde intitulée « Guerre de l'information et lutte informatique : état des lieux et enjeux ».

Après un rappel sur la genèse du concept de guerre de l'information et de son actualité, la table ronde a été animée par divers intervenants civils et militaires, sur le thème des menaces informatiques et celui de la prévention et de la protection contre les attaques informatiques.

Les interventions ont permis d'aborder ces questions sous les aspects techniques mais aussi juridiques, sociologiques et géopolitiques.

Pour en savoir plus :

<http://esec.fr.sogeti.com/blog>

L'ESSENTIEL

Un patch pour renforcer le noyau GNU/Linux : Grsecurity

Grsecurity est un patch de sécurité pour les versions 2.4 et 2.6 du noyau Linux. Ce patch, développé par Bradley Spengler, est une boîte à outils qui permet d'améliorer la sécurité. Dans sa dernière version publiée le 21 avril 2008, il contient de nombreuses fonctionnalités de sécurité parmi lesquelles : des restrictions sur le système de chroot, la protection de la mémoire exécutable avec l'inclusion d'un projet nommé PaX, un système de contrôle des rôles des utilisateurs nommé RBAC (Role-Based Access Control), des protections des connexions réseaux et enfin, des possibilités étendues de log et d'audit. Ce patch se présente comme l'un des projets importants pour renforcer le noyau Linux et il est très bien adapté à la protection des serveurs. Bien entendu ce patch ne peut par lui-même assurer toute la protection d'une machine, c'est pourquoi il doit être inclus dans un ensemble de sécurité plus vaste qui comprend entre autres les firewalls et le cloisonnement des réseaux.

✉ Pourquoi appliquer Grsecurity ?

La configuration du patch nécessite un travail non négligeable pour être adapté à chaque serveur. Ainsi, plutôt que de s'orienter vers un déploiement de masse, il est préférable d'opter pour un déploiement ciblé sur certains serveurs critiques. Deux types de serveurs sont particulièrement concernés par l'application de ce patch :

- un serveur directement exposé à Internet comme un serveur web, un pare-feu,
- un serveur sur lequel de nombreux utilisateurs se connectent à distance, (donc qui offre un grand nombre de shells).

Dans le premier cas, pour protéger le service web contre une prise de contrôle éventuelle, on activera principalement les options PaX de protection de la mémoire, les protections du chroot et de TCP/IP.

Dans le deuxième cas, la problématique est de contrôler finement les droits des utilisateurs. Ainsi, en plus d'activer toutes les options précédentes, le système de contrôle des utilisateurs basé sur les rôles, RBAC, est une fonctionnalité très intéressante.

Grsecurity (références [1] et [2]) est constitué de différentes options activables ou non dans le noyau Linux. Cet article va présenter dans un premier temps les options de protection de l'espace mémoire. Puis seront abordées les options de protection du système de fichiers, le système de gestion des droits des utilisateurs basé sur RBAC, les protections réseaux, pour enfin se pencher sur les possibilités étendues de log et d'audit.

✉ Protection de la mémoire avec PaX

PaX (cf. références [3] et [4]) développé par « PaX team », est un patch pour le noyau Linux, intégré au projet Grsecurity. Son objectif est de protéger les pages mémoire lors de l'exécution des programmes. En effet ce projet part du principe que de nouveaux bugs seront toujours trouvés dans les logiciels. PaX va donc rendre beaucoup plus difficile l'exploitation de ces bugs en mémoire, en s'assurant que le programme n'exécute seulement ce qui lui est nécessaire.

Après un aperçu des vulnérabilités auxquelles PaX répond, deux

fonctionnalités principales, les pages non exécutables et la « randomisation » de l'espace mémoire seront étudiées.

Vulnérabilités logicielles auxquelles PaX répond

PaX répond aux bugs qui permettent à un attaquant d'obtenir un accès non autorisé en lecture ou écriture à l'espace mémoire. Cette classe de bugs contient notamment les *buffer overflow* (débordement de tampon), qu'ils soient basés sur le tas ou sur la pile, et les problèmes de format string.

PaX prévient également contre les attaques qui vont exécuter le code dans un ordre différent de celui prévu par le programme. Ces attaques sont connues sous le nom de « return-to-libc ».

Pages non exécutables

La fonctionnalité des pages non exécutables repose sur l'utilisation du bit NX. Le bit NX est une fonctionnalité matérielle des CPU utilisée pour marquer certaines zones mémoires comme « exécutables » et d'autres comme « données non exécutables ». NX signifie « Non eXecutable » et fait référence au bit numéro 63 d'une table des pages à 64 bits.

- Si ce bit est à 0, la zone mémoire peut être exécutée,
- si le bit est à 1, la zone mémoire est considérée comme contenant des données non exécutables.

La force de PaX est d'utiliser le bit NX du processeur et même si le processeur n'offre pas de bit NX, PaX va *émuler* cette fonctionnalité ! Pour cela deux méthodes sont utilisées : PAGEEXEC et SEGMEEXEC.

PAGEEXEC est la première implémentation permettant d'utiliser ou d'émuler le NX Bit pour i386. Elle repose sur un système de cache nommé TLB (*translation lookaside buffer*) qui donne la correspondance entre adresse virtuelle et adresse physique. Ce TLB fait la distinction entre zones exécutables et zones de données ce qui permet de détecter si une exécution de code est réalisée dans une zone inappropriée. PAGEEXEC fonctionne aussi pour une architecture non x86.

SEGMEEXEC émule le bit NX pour les processeurs x86 uniquement. Il agit en segmentant la mémoire virtuelle, allouée à un processus, en deux parties. Une partie va contenir les données et le code exécutable, tandis que l'autre partie contiendra une copie du code exécutable.

Lorsqu'un processus exécute une instruction, celle-ci est d'abord transférée dans la zone qui contient la copie du code exécutable. Si l'adresse correspond, le code est exécuté. Si l'adresse transférée est erronée, le code est considéré comme *malicieux* et le processus est tué. L'espace mémoire virtuel alloué aux applications est alors de 1,5 Go au lieu des 3 Go habituels, mais cette réduction n'a qu'un impact négligeable sur les performances.

La fonction RESTRICTED MPROTECT() est une protection supplémentaire qui permet de s'assurer qu'aucune page mémoire n'est à la fois « writable » et « executable ». Il s'agit donc de vérifier qu'aucune page mémoire n'a les options PROT_WRITE et PROT_EXEC activées à la fois. Cela permet de se prémunir contre des attaques simples d'injection de code.

Address Space Layout Randomization (ASLR)

ASLR signifie allocation aléatoire de l'espace adressé.

L'ASLR est une technique pour se prémunir contre les attaques par injection de shellcode, et contre l'exécution de code dans un ordre différent de celui prévu par le programme.

En effet, beaucoup de techniques d'exploit reposent sur la connaissance d'adresses mémoire du programme attaqué. ASLR va rendre le processus d'allocation aléatoire pour chaque demande de mémoire. Cette « randomisation » a un effet négligeable sur la performance.

PAXCTL

PAXCTL est un utilitaire situé en espace utilisateur qui permet de contrôler les options PaX pour chaque binaire du système. Ces options de PaX sont présentes dans les entêtes ELF des fichiers. Il est ainsi possible d'activer ou de désactiver les principales options PaX, comme MPROTECT ou PAGEEXEC, pour chaque binaire. Cela permet d'affiner la configuration de PaX avec une granularité par fichier.

Autres options de protection de la mémoire

D'autres options de protection de la mémoire sont disponibles. On peut citer l'option PAX_MEMORY_SANITIZE qui efface les pages mémoires aussitôt qu'elles sont libérées par un *free()* ce qui limite la possibilité de fuite d'information pour certains processus.

Également, l'option de GRSECURITY GRKERNSEC_BRUTE empêche les attaques de type « bruteforce » contre les services qui « forkent » comme apache ou sshd : en cas de crash d'un processus « child » dû à PaX ou à une violation d'adresse mémoire, le processus « parent » doit attendre 30 secondes avant de forker de nouveau.

Protection du système de fichiers

Grsecurity contient de nombreuses options pour protéger le système de fichiers.

Une option notable est GRKERNSEC_PROC_USER. Cette option permet de montrer aux utilisateurs non-root uniquement les processus qui leur appartiennent. Elle limite également l'accès aux informations réseau et aux symboles du kernel.

Une autre option intéressante est GRKERNSEC_LINK. Elle empêche les utilisateurs de suivre des liens symboliques établis par d'autres utilisateurs dans un répertoire autorisé en écriture pour tous et avec un « sticky bit +t » comme le répertoire /tmp par exemple. Cela permet de prévenir les « /tmp race exploit ».

Il existe également d'autres d'options pour renforcer le système de chroot.

Renforcement du chroot

Un chroot permet d'exécuter un processus dans une arborescence de répertoires restreints. Il peut être déployé directement dans un démon, ou via l'utilitaire chroot. Chroot est généralement utilisé pour faire tourner des services comme Apache ou sshd. Ainsi en cas de prise de contrôle du service par un attaquant, il n'aura pas accès à la totalité du système de fichiers. Néanmoins, il existe des techniques de contournement connues, comme par exemple :

- Des exploits qui montent un deuxième chroot à partir du premier chroot ;
- Des exploits basés sur le montage du système de fichiers avec la commande mount ;
- Des exploits qui permettent de modifier un processus en dehors du chroot avec la commande ptrace.

Le patch Grsecurity prend en compte tous ces points, avec en particulier les options suivantes :

- GRKERNSEC_CHROOT_MOUNT : empêche les processus à l'intérieur d'un chroot de monter un système de fichier ;
- GRKERNSEC_CHROOT_DOUBLE : évite qu'un processus enfermé dans un chroot ne crée un deuxième chroot et prévient donc une cause de cassage du chroot largement répandue ;
- GRKERNSEC_CHROOT_FINDTASK : contrôle qu'un processus enfermé dans un chroot n'ait pas accès à un processus exécuté en dehors du

chroot : il ne peut ni le voir, ni lui envoyer des signaux ni le tuer via les appels systèmes *fcntl*, *ptrace*, *capget*, *getpgid*, ou *getsid*.

Toutes les options disponibles dans le patch ne sont pas présentées ici. Il faut retenir qu'avec toutes les options activées le système de chroot est largement renforcé et se rapproche du niveau de sécurité du système jail de FreeBSD, qui constitue une référence.

Le système RBAC (Role Based Access Control)

Sous Linux, la politique d'autorisation d'accès aux fichiers est habituellement le modèle DAC (*Discretionary Access Control*) : chaque utilisateur définit lui-même les droits d'accès à ses fichiers.

Il existe un autre modèle appelé MAC : *Mandatory Access Control*. Dans ce modèle l'administrateur force tous les utilisateurs à se conformer à sa politique d'accès aux fichiers. RBAC est une application de cette politique pour Linux.

La philosophie RBAC

Dans un système RBAC on parle de rôles, de sujets et d'objets.

On appelle **sujets** les différents processus, et **objets** les fichiers auxquels le système accède. Les **rôles** constituent les définitions de sécurité.

Un rôle peut par exemple être un administrateur DNS, des utilisateurs locaux qui consultent leurs emails ou des utilisateurs distants ayant accès à un système de code source comme CVS. L'administrateur peut définir pour chacun de ces rôles la vue qu'il aura du système de fichiers et des processus du système.

Ainsi, un rôle est un utilisateur ou un groupe qui effectue une tâche. Un compte d'utilisateur peut avoir plusieurs rôles en fonction des tâches qu'il doit effectuer.

Avec cette notion de rôle, le compte root devient un utilisateur comme un autre, limité par les rôles qui lui sont attribués. Il n'y a plus de super-utilisateur !

Utilisation de gradm

Gradm est l'utilitaire situé en espace utilisateur servant à la création d'un mot de passe pour l'administrateur RBAC et à l'activation/désactivation de la politique RBAC.

Par défaut les politiques RBAC ne sont pas activées. Il faut tout d'abord configurer la politique voulue dans */etc/grsec/policy*, puis l'activer avec gradm.

Définition des ACL

Les ACL (*Access Control List*) sont les contraintes de sécurité pour les différents rôles. Regroupées ces ACL forment la politique de sécurité située dans */etc/grsec/policy*.

Sur chacun des sujets (processus) on peut définir différents modes comme :

- cacher de tous les processus ;

- autoriser la vue des processus cachés ;
- autoriser de tuer les processus protégés.

Sur chacun des objets (fichiers) on peut définir différents modes comme :

- autoriser en lecture ;
- autoriser en écriture ;
- autoriser en exécution.

Pour les rôles on peut définir également des modes :

- user role ;
- group role ;
- special role.

Ces modes ne sont que des exemples parmi de multiples possibilités.

Génération automatique de politique

Une grande force de Grsecurity est qu'il possède un système d'apprentissage intelligent de la politique de sécurité appelé « learning mode ». Il suffit de lancer le mode d'apprentissage et d'utiliser le système normalement pendant quelques jours. La seule contrainte est de ne pas lancer des tâches d'administration comme l'arrêt ou le redémarrage de services, la création d'utilisateurs ou l'installation de logiciels. Grsecurity va journaliser toute l'activité du système. Puis au moyen d'un programme dédié, il va analyser les logs et générer automatiquement une politique de sécurité.

Protections TCP/IP

Grsecurity contient quelques options pour renforcer l'utilisation du réseau :

- GRKERNSEC_RANDNET augmente l'entropie utilisée par différentes fonctions de Linux.
- GRKERNSEC_SOCKET permet de créer un groupe d'utilisateur, et de restreindre l'accès des sockets à ce groupe : la restriction peut être faite sur tous les sockets, ou bien sur les sockets clients uniquement, ou bien sur les sockets serveurs uniquement.

Possibilités de logs et d'audit

Les possibilités de logs et d'audit sont étendues avec Grsecurity. Les options suivantes sont à noter :

- Possibilité de journaliser toutes les exécutions au sein d'un chroot ;
- Possibilité de journaliser certains signaux comme SIGSEGV qui peuvent indiquer une tentative d'exploit sur un programme ;
- Possibilité de journaliser les échecs de fork() ;
- Possibilité de restreindre les logs à un groupe d'utilisateurs.

Ces options liées à d'audit du noyau rendent plus facile la détection de tentatives d'attaque sur le système, comme les exploits basés sur les débordements de tampons ou les tentatives de déni de service (DOS) basées sur les « fork() bombes ».

Installation de Grsecurity

Pour installer Grsecurity sur un serveur il faut télécharger le noyau Linux, appliquer le patch, puis recompiler le noyau avec les options voulues. Cela nécessite un redémarrage du serveur et donc une indisponibilité de quelques minutes au minimum.

L'idéal est de faire une copie du serveur et de réaliser ces opérations en environnement de test « isoprod » avant l'installation sur le serveur en production.

De plus, comme avant toute opération qui modifie le système d'exploitation, il est recommandé de faire une sauvegarde du système et des données.

L'installation de Grsecurity se fait de préférence sur un noyau « vanilla », c'est-à-dire un noyau non patché téléchargé depuis kernel.org. En effet, les noyaux prépatchés par différentes distributions ne sont pas forcément compatibles avec le patch Grsecurity.

Afin de réaliser les tests, une option dans le patch Grsecurity s'avère pratique. Elle active le support `sysctl`. Ainsi il est simple de régler toutes les options du patch sans avoir à recompiler le noyau après chaque changement. Attention cependant, car l'activation de cette option désactive toutes les autres options de sécurité, ce qui permet à l'administrateur d'activer les

options voulues après le démarrage de la machine.

Les versions de noyau actuellement supportées sont les 2.6.24.5 et 2.4.36.2. Les versions du patch sont donc en très léger décalage avec le support des noyaux récents puisque les versions actuelles du noyau sont 2.6.27.9 et 2.4.37.

Des alternatives à Grsecurity

Protection de la mémoire

Pour assurer la protection de la mémoire, il existe un concurrent plus léger mais moins performant : Exec shield, qui a déjà été intégré pour partie au noyau Linux, notamment dans le 2.6.25. Exec shield est un projet qui émule le bit NX sur architecture x86.

Un autre concurrent de PaX dans le monde open source est le système W^X de OpenBSD [5]. W^X se prononce « *W xor X* » et signifie qu'une zone mémoire ne peut être à la fois accessible en écriture et en exécution. Cela permet de se prémunir, comme avec Grsecurity, contre beaucoup d'attaques par *buffer overflow*. Par ailleurs, OpenBSD supporte également l'ASLR.

Contrôle d'accès RBAC

En ce qui concerne RBAC, il existe plusieurs autres systèmes de gestion des droits basés sur les rôles.

Le système le plus connu est SELinux [6] le projet de la NSA, directement intégré au noyau Linux. SELinux est un Linux Security Module (LSM) c'est-à-dire un module du noyau qui fournit un système MAC. Par contre, il ne gère pas de protection de la mémoire. Il est intéressant de remarquer que certains développeurs et notamment Bradley Spengler apprécient peu les LSM. L'un de leurs arguments est que ces modules exportent énormément de symboles ce qui facilite l'insertion de *rootkits*.

On trouve également le système RBAC sous OpenSolaris et Solaris [7].

Il existe un autre patch RBAC pour le noyau Linux appelé RSBAC [8] (*Rule Set Based Access Control*). RSBAC peut être combiné à PaX pour concurrencer de Grsecurity.



Grsecurity est une brique supplémentaire pour la protection d'un système Linux, au niveau noyau. Bien entendu, cette brique ne suffit pas à elle seule, pour se prémunir contre les attaques. Elle doit s'ajouter à des éléments déjà existants comme : la désactivation des services inutiles, une gestion raisonnable des utilisateurs et de leurs mots de passe, la mise en place d'un firewall, la protection des services par chroot, la mise à jour du noyau et des logiciels installés. Dans ce cadre Grsecurity va ajouter un niveau de sécurité important :

- La protection de la mémoire pour se prémunir contre les exploits « 0-day » (vulnérabilités non divulguées au public et pour lesquelles aucun correctif de sécurité n'est disponible) ;
- La protection du chroot pour améliorer la sécurité des services en place ;
- La définition de politiques RBAC pour définir des droits d'accès avec une forte granularité pour les utilisateurs ;
- La possibilité de logs étendus pour détecter plus facilement les tentatives de prise de contrôle du serveur.

Après avoir réalisé ce tour d'horizon des fonctionnalités, on peut se rendre compte que Grsecurity va permettre de se protéger de classes entières de vulnérabilités. En vue du déploiement il ne reste plus qu'à déterminer sur quels serveurs l'installer et quelles sont les options de configuration les plus adaptées.

Références :

- [1] <http://www.grsecurity.com/>
- [2] <http://en.wikipedia.org/wiki/Grsecurity>
- [3] <http://pax.grsecurity.net/>
- [4] <http://en.wikipedia.org/wiki/PaX>

- [5] <http://www.openbsd.org/>
- [6] <http://www.nsa.gov/selinux/>
- [7] <http://www.sun.com/software/solaris/>
- [8] <http://www.rsbac.org>



FORMATION ESEC

<http://esec.fr.sogeti.com/FR/poles/formations.php>

20 février 2009 : Introduction à l'ISO 27002 et ISO 27001

2-4 février 2009 : Réaliser une analyse de risque ISO 27005

23-27 février 2009 : Responsable d'audit 27001 (Formation Certifiante)

ZOOM

La sécurisation des terminaux mobiles [2/2]

La première partie de cet article [1] traitait de la sécurisation des terminaux mobiles (smartphones/PDA), sujet large et complexe, étant donné les nombreux risques qui pèsent sur ces appareils. Restait alors une question : comment l'entreprise doit-elle aborder et gérer ces risques ? Cet article traite des principales problématiques liées au déploiement des terminaux mobiles en entreprise : la définition d'une politique de sécurité et les solutions de gestion de flotte.

De l'importance de la politique de sécurité de l'entreprise

Un contexte marqué par de nombreux risques potentiels

Le NIST (*National Institute of Standards and Technology*) est une agence du département du Commerce des États-Unis, chargée de promouvoir des normes technologiques. Celle-ci a publié en 2008 un guide sur la sécurité des smartphones et des PDA [2]. Ce guide commence par rappeler les principaux éléments à prendre en compte pour leur sécurité :

- la petite taille et l'usage nomade des terminaux facilite leur perte et leur vol. Ainsi, près de 8 millions de téléphones mobiles ont été perdus dans le monde en 2007 ;
- les fonctionnalités d'authentification fournies dans les systèmes d'exploitation sont considérées comme insuffisantes ;
- les backdoors installées par les constructeurs dans un but de débogage font courir un risque supplémentaire pour la sécurité du système ;
- les nombreux moyens de communication (réseau, synchronisation avec un PC, Bluetooth, Wifi, etc.) augmentent le risque d'infection par un malware. Les risques sont alors réels : virus, déni de service, fraude, prise de contrôle, etc. ;
- le spam cause non seulement des désagréments mais génère également des surcoûts liés à la facturation des connexions data ;
- les réseaux sans fil (GSM, 3G, Wifi) sont susceptibles d'être surveillés. Les données en transit sur ces réseaux peuvent être interceptées. Des moyens simples comme les malwares permettent l'espionnage [1] ;
- les technologies de géolocalisation (par GSM ou GPS) peuvent engendrer des atteintes à la vie privée ;
- les données stockées sur les serveurs des opérateurs mobiles (SMS, logs, contacts, etc) peuvent être accessibles à des employés malintentionnés.

La mise en place d'une politique de sécurité

Étant donné les éléments décrits précédemment, l'entreprise doit définir une politique de sécurité spécifique aux terminaux mobiles. Cette politique doit intégrer :

- la définition des risques qui pèsent sur les terminaux et les solutions techniques et organisationnelles qui sont prises pour y faire face ;

- la manière dont les terminaux doivent être gérés tout au long de leur cycle de vie, ainsi que les procédures à suivre dans des situations comme la perte d'un terminal ou la mise à jour d'une application ;
- le plan de déploiement, quelle que soit la taille de la flotte mobile ;
- le plan de formation et de sensibilisation des collaborateurs à propos de l'usage sécurisé des terminaux.

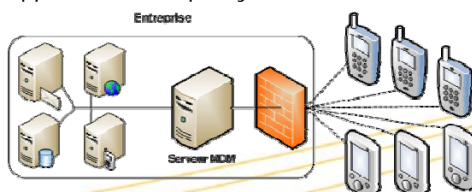
La rédaction de la politique doit également prendre en compte les évolutions qui sont susceptibles d'affecter le marché de la sécurité mobile. Ainsi selon le NIST, la menace représentée par les malwares va se développer à moyen terme, car les terminaux vont devenir de plus en plus performants et de plus en plus connectés. Parallèlement, les plateformes mobiles comme Windows Mobile ou Symbian ne sont pas suffisamment mises à jour par les constructeurs.

Les solutions MDM (Mobile Device Management)

Présentation

Les solutions MDM ont pour but d'aider l'entreprise à gérer sa flotte de terminaux mobiles.

Comme le montre le schéma ci-dessous, ces solutions de type logiciel constituent un point d'accès unique au système d'information de l'entreprise pour tout appareil mobile qui s'y connecte.



Architecture d'une solution MDM

Fonctionnalités

Ces solutions comportent de nombreuses fonctionnalités :

- ▶ **Gestion des actifs**
 - inventaire des ressources matérielles ;
 - gestion des licences ;
 - contrôle de l'usage des terminaux (contrôle des programmes installés) ;
 - contrôle de l'accès au système d'information (authentification forte) ;
 - paramétrage à distance ;
 - support des différentes plateformes (Windows Mobile, Symbian, Blackberry, iPhone) ;
 - backup automatisé des données ;

▶ Télédistribution

- déploiement aisé des programmes (en quelques clics ils peuvent être installés sur toute la flotte des terminaux) ;
- distribution rapide des mises à jour ;

▶ Sécurité

- blocage ou effacement à distance (quand le terminal est perdu ou volé, l'administrateur peut rapidement le bloquer ou effacer les données à distance) ;
- chiffrement des données stockées sur le terminal ;
- chiffrement des communications entre le terminal et le serveur MDM ;

▶ Fonctionnalités mobiles avancées

- optimisation des communications (gestion des déconnexions, compression des flux, transferts intelligents, etc.) ;
- prise en main du terminal à distance ;
- intégration facile avec le système d'information.

Les solutions de sécurité décrites dans la première partie de cet article [1] présentent l'inconvénient de ne pas être facilement administrables de manière centralisée. En effet, le fichier de configuration des applications doit être déployé vers tous les terminaux, en passant par Active Directory, les GPO (Group Policy Object) et une synchronisation ActiveSync. Ces tâches d'administration sont particulièrement lourdes à mettre en place, surtout si on ne dispose pas d'une architecture homogène. En revanche, les solutions MDM, quant à elles, permettent en quelques clics de déployer des applications ou des paramètres à des milliers de terminaux, tout simplement à partir d'une console d'administration et en mode OTA (*Over The Air*), c'est-à-dire que les terminaux sont en contact sans fil permanent avec le serveur MDM (par GSM, 3G ou Wifi).

Les avantages financiers

Les solutions MDM ont un fort impact sur les coûts de gestion d'une flotte mobile. Ainsi, le déploiement d'une solution MDM permet de réduire un certain nombre de coûts liés à :

- l'exploitation : diminution de la consommation de bande passante grâce à la compression des flux ;
- le support : la fonctionnalité de prise en main à distance permet de diminuer le temps d'intervention du helpdesk et le nombre de retour de terminaux en panne. Il s'en suit une baisse du temps de traitement des incidents et par conséquent une forte diminution des dépenses de support

(de l'ordre de 30 % selon l'étude réalisée par IDC [3]) ;

- le déploiement (grâce à la télédistribution).

Dans son étude [3], IDC estime que le retour sur investissement (ROI) est atteint généralement après six voire neuf mois d'utilisation, ce qui le conduit à qualifier les solutions MDM « d'investissement indispensable et rapidement rentabilisé ». Il faut néanmoins préciser que, dans le domaine de la sécurité, le ROI ne saurait être l'unique indicateur d'aide à la décision. Il convient en effet d'analyser le coût de la « non-sécurité », c'est-à-dire des pertes potentielles liées à « l'insécurité ». Ainsi, la perte d'un terminal contenant des données confidentielles peut se révéler plus coûteux pour l'entreprise que le déploiement d'une solution MDM qui, au moyen de la fonctionnalité d'effacement à distance, aurait permis de réduire voire supprimer le risque de perte de données.

Le marché des solutions MDM

Le marché compte une dizaine d'acteurs importants, dont les leaders, selon IDC, sont Sybase avec iAnywhere Afaria et Nokia avec Intellisync. Ces deux solutions sont compatibles avec les principales plateformes mobiles et autorisent notamment le recouvrement du code PIN du terminal. Si le produit de Sybase est plus complet (il permet de chiffrer les données stockées et dispose d'un antivirus et d'un pare-feu), la solution de Nokia est connue pour être plus simple d'usage et ergonomique.

Notons également l'existence d'un acteur français, Sparus, avec sa solution EveryWan. Pour l'instant réservé à Windows Mobile, il met l'accent sur la sécurité, avec une authentification mutuelle client/serveur par certificat SSL et le chiffrement des données. De plus, il dispose de fonctionnalités avancées de prise en main à distance.

L'adoption d'une solution MDM

Seulement 30 % des entreprises ont déployé une solution MDM pour la gestion de leur flotte mobile, selon une étude réalisée par *InformationWeek* [4]. Officiellement, elles n'ont pas assez de terminaux pour justifier l'investissement et elles manquent de personnel pour mener à bien le déploiement. Les équipes marketing des éditeurs de solutions MDM ont donc encore du travail...

Et pourtant, l'adoption d'une telle solution va devenir de plus en plus inévitable pour les entreprises qui n'ont pas encore « migré ». En effet, près de 40 % des entreprises ont une flotte hétérogène, et ce chiffre va très probablement augmenter à terme, en raison du large choix de terminaux sur le marché. Ces terminaux deviennent de plus en plus grand public, ce qui pousse les collaborateurs à vouloir utiliser le même terminal dans un but professionnel et privé, ou du moins à orienter les choix d'équipement de l'entreprise. Cela va conduire à une plus

grande hétérogénéité des flottes d'entreprises. Seule une solution MDM est en mesure de gérer efficacement des plateformes, des applications et des configurations différentes...

Il est difficile d'imposer à l'ensemble des collaborateurs un terminal unique ; par exemple, qui empêchera le PDG d'utiliser l'iPhone que son fils lui a offert pour Noël ? La sécurité impose que tous les terminaux soient « sous contrôle » avant de se connecter au système d'information, et il suffit d'un seul terminal pour créer une faille dans le système.

L'entreprise doit donc s'interroger sur sa politique en termes d'équipement mobile :

- Doit-elle fournir les terminaux à ses employés ou peut-elle les laisser utiliser le leur ?
- Est-il possible de contrôler quels programmes peuvent être ou non installés,
- Doit-elle faire désactiver le Bluetooth, s'il s'agit du terminal du collaborateur ?
- Quid de l'utilisation privée du terminal ?
- Peut-elle interdire les terminaux « privés », dans le cas où elle équipe ses collaborateurs ?

Toutes ces questions sont fondamentales et doivent être résolues au plus haut niveau avant tout déploiement. Les réponses intégreront ensuite la politique de sécurité des terminaux mobiles.

Sans solution MDM, il n'y a pas de point d'accès unique au système d'information pour les terminaux ; n'importe quel terminal peut se connecter. Or, rappelons-le, celui-ci est potentiellement dangereux. Soit parce qu'il peut être infecté par un malware (un virus ou un keylogger), soit parce qu'il contient des applications non autorisées, soit parce qu'il n'applique pas une politique de sécurité efficace (par exemple, un verrouillage avec un code PIN à 4 chiffres au lieu de 6), tout cela réduisant la protection des données stockées et la sécurité des accès aux applications.

Le déploiement d'une flotte mobile

Le NIST rappelle dans son guide que tout déploiement de flotte est précédé d'une « checklist » composée d'une série de mesures dont il faut vérifier la bonne application, à la fois côté utilisateur et côté organisation.

Côté utilisateur

Tout d'abord, l'accent doit être mis sur la protection physique du terminal. Quelles que soient les mesures de sécurité logicielles qui ont été mises en place, l'utilisateur doit veiller à ne pas perdre ni se faire voler son terminal. Il doit le conserver en permanence sur lui et, dans la mesure du possible, ne pas le prêter à des tiers. Par ailleurs, il faut prendre garde à « l'indiscrétion » de ses voisins dans les lieux publics (quand on rédige

des emails dans le métro, il est facile de lire par-dessus l'épaule).

Ensuite, l'entreprise doit veiller à ce que les fonctionnalités d'authentification de l'utilisateur sur le terminal soient activées et correctement configurées, étant donné qu'il s'agit généralement du premier obstacle que rencontrera l'attaquant. Lorsque l'authentification est réalisée par mot de passe, ce dernier doit bien évidemment suivre les recommandations traditionnelles (longueur, complexité). De plus, il est conseillé de configurer un délai de *timeout* assez court, au bout duquel le terminal se verrouille, forçant alors à se ré-authentifier.

Par ailleurs, les politiques de sauvegarde de données doivent s'intégrer à la gestion du terminal. La synchronisation de ce dernier avec le poste de travail n'est pas toujours pratique dans un contexte de mobilité. A ce titre, les solutions MDM proposent des fonctionnalités de sauvegarde automatique. Notons que sauvegarder des fichiers importants sur la carte mémoire n'est a priori pas une bonne solution, car en général la carte est volée ou perdue en même temps que le terminal...

À ce sujet, rappelons que les données stockées sur le terminal doivent être chiffrées [1], mais il faut être conscient que cette mesure n'est pas la panacée ; elle est par exemple inefficace pour le protéger des malwares.

C'est bien connu : « l'humain » est le maillon faible dans la sécurité d'un système. Il est donc capital de le sensibiliser aux risques liés à l'utilisation des terminaux. Il faut s'assurer que l'utilisateur connaisse et respecte les quelques règles basiques, comme celle qui consiste à ne pas ouvrir les messages provenant d'inconnus, ne pas télécharger de programmes suspects, faire attention aux questions posées par le terminal : en effet, le système d'exploitation va demander généralement une confirmation avant d'exécuter un malware ou de se connecter vers l'extérieur. L'utilisateur doit donc être attentif à ce genre de messages.

De plus, il est recommandé de contrôler, limiter, voire désactiver les différentes interfaces réseaux (Bluetooth, Infrarouge, Wifi). A ce sujet, les solutions MDM se révèlent particulièrement utiles puisqu'elles permettent de configurer les interfaces de toute une flotte en quelques clics.

En outre, en cas de perte ou de vol d'un terminal, l'utilisateur doit alerter le plus rapidement possible le support informatique pour que ce dernier bloque ou efface à distance les données qui y sont stockées. Il est aussi possible de prévenir l'opérateur afin qu'il intervienne à son niveau (blocage du numéro IMEI).

Par ailleurs, puisque les terminaux comportent nombre de fonctionnalités inutiles (applications, plug-in, services, jeux), l'entreprise doit être en mesure de les répertorier et de les désactiver, pour

limiter l'exposition du terminal aux failles potentielles.

Enfin, après analyse de l'utilisation des terminaux et des besoins, l'entreprise gagnerait à intégrer des solutions anti-malware (antivirus, antispam, pare-feu). Les serveurs MDM sont ici tout à fait indiqués pour faciliter la gestion de ces solutions tierces. Toutefois, qu'un antivirus soit déployé ou non, il est fortement recommandé de scanner les messages et les pièces jointes en amont, c'est-à-dire au niveau du serveur de messagerie.

Côté organisation

Avant le déploiement de la flotte, les étapes suivantes sont nécessaires :

- l'entreprise doit recenser les besoins et les applications à installer sur les terminaux ;
- en fonction de ces résultats, il faut évaluer et gérer les risques qui se présentent ;
- l'entreprise doit ensuite établir des politiques de sécurité détaillées et des procédures à suivre en fonction des différentes situations ;
- un plan de déploiement est à rédiger, quelle que soit la taille de la flotte ;
- finalement, il est nécessaire de former les utilisateurs, non seulement en ce qui concerne l'utilisation du terminal, mais aussi sur les procédures à suivre en cas de perte ou de vol, et pour assurer la sensibilisation à la sécurité.

Une fois les terminaux déployés, l'entreprise doit pouvoir contrôler et gérer la configuration des applications et du système d'exploitation. Les conseils ci-dessus peuvent être adaptés à la politique de l'entreprise et au contexte d'utilisation des

terminaux, tout en prenant en compte la politique d'équipement de l'organisation.

Les entreprises adoptent généralement des politiques de sécurité strictes pour leurs postes de travail (fixe ou portable), alors pourquoi n'en serait-il pas de même pour les terminaux mobiles ? Nombre d'utilisateurs et de responsables ne considèrent ce type de terminal que comme un téléphone « amélioré » et de ce fait ne sont pas prêts à appliquer des politiques de sécurité spécifiques aux terminaux.

Les limitations des solutions MDM

La fonction la plus populaire des solutions MDM est la possibilité de bloquer ou d'effacer à distance les données d'un terminal lorsque ce dernier est perdu ou volé. Mais pour que le terminal soit effectivement désactivé, il doit être en fonctionnement et en zone de couverture GSM... Un voleur averti s'empressera d'aller dans une zone non couverte (comme un parking souterrain) avant d'utiliser le terminal, de sorte que ce dernier ne puisse recevoir le signal d'effacement. De manière alternative, le voleur enlèvera la carte SIM avant de récupérer tranquillement les données.

Par ailleurs, le NIST a rappelé que l'effacement à distance n'est qu'un « hard-reset » du terminal, ce qui ne constitue pas un effacement sécurisé puisque les techniques forensics permettent de récupérer les données stockées sur la mémoire flash.

Enfin, le serveur MDM devient un composant sensible au sein de l'architecture de l'entreprise : il donne

accès aux différents services du système d'informations et il est également un point d'entrée pour de nombreux terminaux. Les éditeurs ont pris cet élément en compte et ont conçu leurs produits pour être installés soit dans une DMZ soit en interne (mais en passant par un reverse-proxy en DMZ). Il faudra ainsi veiller à assurer la sécurité du serveur MDM ainsi que la disponibilité et la répartition de charge.

Terminons par la limitation associée au chiffrement des données. On a vu dans la première partie de l'article que cette mesure se révèle particulièrement utile pour empêcher des tiers d'accéder aux données. Mais il faut que le chiffrement soit couplé avec un *timeout* court, au bout duquel le terminal se verrouille, de manière à éviter qu'un voleur ne puisse accéder aux données sans s'authentifier. Malheureusement, ceci pose un problème d'ergonomie : les utilisateurs accepteront difficilement d'avoir à entrer un mot de passe ou un code PIN trop fréquemment. Ici se manifeste la problématique classique de l'équilibre à trouver entre la sécurité et la mobilité. L'utilisateur veut une solution simple, rapide, ergonomique et adaptée aux contraintes de la mobilité. Or, la sécurité est rarement compatible avec ces aspirations. Et il est bien connu que les collaborateurs utilisent peu ou mal un système trop lourd ou qui ne les satisfait pas. Il appartient donc aux décideurs et aux RSSI de travailler à trouver les meilleurs compromis pour conserver les atouts apportés par la mobilité et la sécurité des informations qui sortent de plus en plus facilement des locaux de l'entreprise.

Le déploiement d'une flotte de terminaux mobiles en entreprise s'appuie d'abord sur une politique de sécurité, construite à partir des risques susceptibles de peser sur les terminaux et d'une politique d'équipement mûrement réfléchie. Les solutions de gestion de flotte constituent un outil indispensable dans la sécurisation et la gestion de la flotte mobile. Coûteuses à l'achat, elles constituent un investissement rapidement rentabilisé selon l'institut IDC. Toujours sur l'aspect financier, précisons pour finir que ce ne serait pas une très bonne idée de faire des économies sur l'achat des terminaux ; en effet ce dernier doit être suffisamment puissant pour pouvoir faire tourner en même temps le client MDM, le chiffrement à la volée, ainsi qu'une solution antivirus et un pare-feu.

Références :

- [1] newsletter décembre 2008, « La sécurisation des terminaux mobiles (1/2) »
- [2] Rapport du NIST sur la sécurité des terminaux mobiles, <http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf>
- [3] Livre blanc IDC « L'administration et la sécurité des terminaux Windows Mobile », septembre 2007
- [4] InformationWeek Analytics Reports, « Mobile Device Management: Time To Get Started », mai 2008



Inscription à la Newsletter : newsletter-subscribe@esec.fr.sogeti.com

Désinscription : newsletter-unsubscribe@esec.fr.sogeti.com

ESEC - Sogeti Infrastructures Services

6-8 rue Duret 75016 Paris - France

Tél. : +33 (0)1 58 44 26 79

Site : <http://esec.fr.sogeti.com>

Mail : esec@esec.fr.sogeti.com

Société par Actions Simplifiées au capital de 15 999 790€ - RCS Paris 479 942 583

Conformément à la loi « Informatique et libertés » du 6 janvier 1978, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent. Si vous souhaitez exercer ce droit et obtenir communication des informations vous concernant, veuillez vous adresser au directeur de la publication.

Sogeti ne peut être tenue pour responsable en cas avéré de détournement des liens communiqués à titre d'illustration dans ses propos.

Cette newsletter a été réalisée par des experts sécurité de l'ESEC.

Responsable de la publication : Edouard JEANSON

Auteurs :

David ISAL

Guillaume LAROCHE de ROUSSANE

Rédacteur en chef : Thomas BOUSSON

Recteur(s) : François-René HAMELIN, Mathieu ROBERT, Jean-Baptiste BÉDRUNE, Alexandre GAZET