

Sécurité des systèmes informatiques  
**Sécurité et procédures**

Olivier Markowitch

# Sécurisation matérielle

## Sécurisation matérielle des stations de travail

- permission de l'accès au clavier ou à l'écran tactile
- permission de l'accès au lecteur de disquettes ?
- permission de l'accès au lecteur de CD ?
- permission de l'accès au ports USB, ... ?
- permission de relancer la station et/ou de l'éteindre ?

# Gestion logicielle

## Sécurisation logicielle des stations de travail

- permission d'accéder au BIOS des PC ?
- réalisation de sauvegardes (*backups*) sur des supports appropriés
- limiter les permissions d'exécution des commandes sur les stations
- *brider* les logiciels

# Gestion du réseau

Si un accès vers l'extérieur est proposé (accès internet)

- mise en place d'un firewall, antivirus, etc.
- offrir des connections pour permettre aux portables d'accéder au réseau ?

# La sécurité dans les lieux publics

Ce contexte nécessite donc que l'on assure :

- la confidentialité (des mots de passe, des numéros de cartes bancaires, des documents, des emails, etc)
- l'intimité (privacy) : les utilisateurs ne doivent pouvoir avoir accès aux documents d'un utilisateur tiers, à ses emails, à son activité sur le web, etc. Gestion des cookies, adresses web, informations collectée par le proxy, etc.
- faire attention aux mineurs utilisant les ordinateurs publics

# La sécurité dans les lieux publics

Ce contexte nécessite donc que l'on assure :

- l'intégrité des données doit être assurée (en se protégeant des attaques, virus, vers, trojans, spywares, ...; en gérant les backups des données, en dupliquant les données - raid -, ...)
- la disponibilité (maintenance des ordinateurs et des serveurs, maintenance des applications, intégrité des applications, des fichiers systèmes, des données, des documents, ...)

# Plannification de la sécurité

La sécurité doit donc s'organiser et se planifier

Pour commencer cela nécessite la réalisation d'une analyse des risques, *risk assessment* qui identifie :

- les menaces (*threats*) : situations menant à la compromission de la confidentialité, accessibilité ou intégrité
- les vulnérabilités (*vulnerabilities*) : erreurs ou bugs dans une application qui peuvent être exploités afin de permettre des attaques (directement via l'ordinateur ou via le réseau)

Les logiciels sont de plus en plus complexes → ils contiennent de plus en plus souvent des bugs → vulnérabilités

# L'analyse de risques

L'analyse de risques dresse un inventaire des ressources et identifie leurs vulnérabilités et risques

Cela permet aussi de déterminer quelles ressources sont les plus importantes et sensibles

# L'analyse de risques

Pour chaque ressource indiquer l'importance de chacun des risques qu'elle encourt :

- *élevé* : si l'attaque résulte en un arrêt de l'organisation ou à des pertes légales et/ou financières telles que la mission de l'organisation ne peut plus être assurée
- *moyenne* : si l'attaque résulte en une perturbation du fonctionnement de l'organisation ou à des pertes légale et/ou financières telles que la mission de l'organisation peut encore être assurée de manière diminuée
- *faible* : l'attaque ne résulte ni en un arrêt de l'organisation, ni en des pertes légales ou financières

# L'analyse de risques : menaces

Les *sondes* : une sonde (*probe*) est un logiciel qui cherche de manière systématique (*scan*) une information non protégée (des accès à des comptes sur un ordinateur ou un serveur, etc.)

Les *compromissions de comptes* : découverte du mot de passe d'un utilisateur, permettant l'accès à des données normalement non autorisées

Les *sniffeur de paquets* : un sniffeur de paquets IP (ou *packets sniffer* est un logiciel qui intercepte les données circulant sur le réseau (on peut y trouver des noms d'utilisateurs, des mots de passe, etc.)

# L'analyse de risques : menaces

Les *denis de service* : les attaques par dénis de service (*denial of service*) sont telles qu'elles empêchent un serveur de répondre aux requêtes légitimes qui lui sont adressées (flooding, débranchement de composants physiques, etc.)

Les *codes malicieux* : trojan, virus, vers, etc. (peuvent aussi réaliser du déni de service)

Le *spoofing* : attaque consistant à prendre l'identité d'un matériel existant (forger une adresse IP ou une adresse mac, etc.)

# L'analyse de risques : vulnérabilités

Ne pas se baser sur la *configuration par défaut* des logiciels : le paramétrage par défaut des logiciels n'est pas toujours compatible avec les règles de bonne sécurité (car cela prévu pour permettre un usage aisé par le plus d'utilisateurs différents possibles)

Désactiver les *comptes invités* ou *guest accounts*, et désactiver le groupe *every one* sur windows))

Changer de nom d'utilisateur du compte administrateur et l'associer à un bon password

# L'analyse de risques : vulnérabilités

Si usage d'un mot de passe pour l'identification : imposer des règles sur son format et son usage

Prévoir l'installation régulière des correctifs (*patches*) pour les logiciels et le système d'exploitation (en les testant préalablement avant de les généraliser sur tout le système informatique)

Eviter d'avoir trop de services offerts par l'ordinateur (*stripper* l'ordinateur)

# L'analyse de risques : vulnérabilités

Installer et configurer correctement un firewall

Réaliser à intervalles réguliers et rapprochés des copies de sauvegardes (*backups*) et les vérifier !

Avoir en plus du backup une copie des spécifications du matériel associé ainsi que des médias d'installation des logiciels

Installer des logiciels adéquats de protection contre les codes malicieux et les maintenir à jour (par exemple : téléchargement régulier des nouvelles définitions de virus)

# L'analyse de risques : se tenir informé

Consulter régulièrement les CERT (Computer Emergency Response Team) : système de récolte d'informations sur les menaces et vulnérabilités (fondé par Carnegie Mellon University) associé à un mécanisme d'alerte (mailing list, newsgroups, etc.)

<http://www.cert.org>

<http://cert.belnet.be>

Autres liens d'informations :

<http://www.securityfocus.com>

<http://www.sans.org/top20>

# La police de fonctionnement

L'analyse de risque est conduite par une équipe de sécurité composée par des représentants :

- de l'équipe technique (équipe IT)
- des différents départements de l'organisation
- de l'équipe de gestion administrative de l'organisation

Sur base de l'analyse de risque, l'équipe de sécurité rédige une *police de fonctionnement* de l'organisation qui décrit les *procédures* de fonctionnement

# La police de fonctionnement

La police de fonctionnement décrit le rôle et la responsabilité de chaque utilisateur potentiel

Cette police de fonctionnement contient, entre autres, la police de sécurité qui indique les stratégies de protection

Les polices de fonctionnement et de sécurité sont des documents *vivants*, qui doivent donc être mis à jour régulièrement (et certainement après une attaque ou après une modification du système ou du réseau)

# La police de sécurité

La police de sécurité indique :

- les éléments qu'il faudrait sécuriser
- comment sécuriser ces éléments
- comment réagir lors de problèmes (attaques, ...)
- qui contacter en cas de problèmes

# La police de sécurité

La police de sécurité détermine les aspects du fonctionnement du système lié à la sécurité tels que :

- la gestion des accès à distance
- la gestion de l'identification (éventuellement la gestion des mots de passe)
- la gestion des protections contre les codes malicieux
- la gestion des sauvegardes
- la récupération après une attaque (disaster recovery)
- la formation des utilisateurs
- etc.

# La police de sécurité

Des règles d'usage liées à la sécurité y sont décrites : règlement d'usage des ordinateurs et du réseau par le personnel, règlement d'usage des ordinateurs et du réseau par le public

On y reprend aussi les règles et lois qui peuvent intervenir (règles relatives au copyright, etc.)

La police de sécurité décrit quelles sont les mesures prises pour garantir le respect de la police et ce qu'il se passe si quelqu'un brise une de ses règles

# La police de sécurité

Le plan d'une police de sécurité est usuellement :

(1) Description des objectifs de la police (il s'agit d'un résumé de ce qui suit)

(2) Portée du document : indication de ce qui sera protégé, suivant l'analyse de risques, et de qui doit respecter la police

(3) Attribution des responsabilités : qui est la personne responsable pour chacun des aspects repris dans la portée du document

# La police de sécurité

(4) Description de la sécurité physique : descriptions des mesures physiques de protection ainsi que des personnes ayant accès aux parties sécurisées physiquement

(5) Description de la sécurité système : description des mesures de protections des données stockées, de la sécurisation des ordinateurs et du système d'exploitation, des mesures de contrôle d'accès, des moyens d'identification, de la gestion des sauvegardes, etc.

# La police de sécurité

(6) Description de la sécurité réseau : description des mesures de protections des données accessibles via le réseau, des mesures de contrôle d'accès à distance, de la gestion des firewalls (restriction sur l'usage des ports/services, le filtrage des paquets, usage des serveurs proxy), etc.

(7) Description de la sécurité des applications : indique qui a le droit d'acheter des logiciels, qui a le droit de télécharger des logiciels, qui a le droit de configurer et d'installer des logiciels, qui gère la maintenance des logiciels (et comment), etc.

# La police de sécurité

(8) Description du plan en cas de désastre (*disaster recovery*) : procédure à suivre en cas d'attaque ou de panne :

- liste des personnes autorisées et compétentes pour restaurer le système (il en faut plus de une)
- indique la localisation des données stockées à l'extérieur du site de l'organisation (sauvegardes des données ainsi que de l'installation du système et des applications)
- indique la priorité dans les données à restaurer
- liste d'équipements matériels à sauver (si possible)
- inventaire du matériel, spécification de ce hardware

# La police de sécurité

(9) Formation des utilisateurs quant à la sécurité : indique quel niveau de conscience de la sécurité le personnel et le public est sensé avoir

(10) Description des sanctions imposées si la police de sécurité n'est pas respectée (déconnection du réseau, perte des droits d'accès, action légale, ou action disciplinaire pour le personnel)

Lien intéressant :

<http://www.sans.org/resources/policies>

# Audits et scanneurs

Des audits de sécurité, tels que des audits d'intrusion ou des audits de vérification de l'intégrité des données et fichiers, peuvent être réalisées

Nessus : scanneur de vulnérabilités

([www.nessus.org](http://www.nessus.org))

Satan : analyse de la sécurité réseau d'un système

([www.porcupine.org/satan](http://www.porcupine.org/satan))

Tripwire : analyse de vulnérabilités

([sourceforge.net/projects/tripwire](http://sourceforge.net/projects/tripwire))

Computer Associate et son produit « eTrust audit »

(<http://www3.ca.com>)

# Audits et scanneurs

**Sara : une variante de Satan**

([www-arc.com/sara](http://www-arc.com/sara))

**Saint : analyse de vulnérabilités**

([www.saintcorporation.com/saint](http://www.saintcorporation.com/saint))

**InterSect Alliance : analyse d'intrusions**

([www.intersectalliance.com](http://www.intersectalliance.com))

**AirSnort : casse les clés WEP en monitorant les transmissions**

([sourceforge.net/projects/airsnort](http://sourceforge.net/projects/airsnort))

**Chkrootkit : scanne le système à la recherche de trojans, vers et vulnérabilités**

([www.chkrootkit.org](http://www.chkrootkit.org)

[freshmeat.net/projects/chkrootkit](http://freshmeat.net/projects/chkrootkit))