

## Résumé

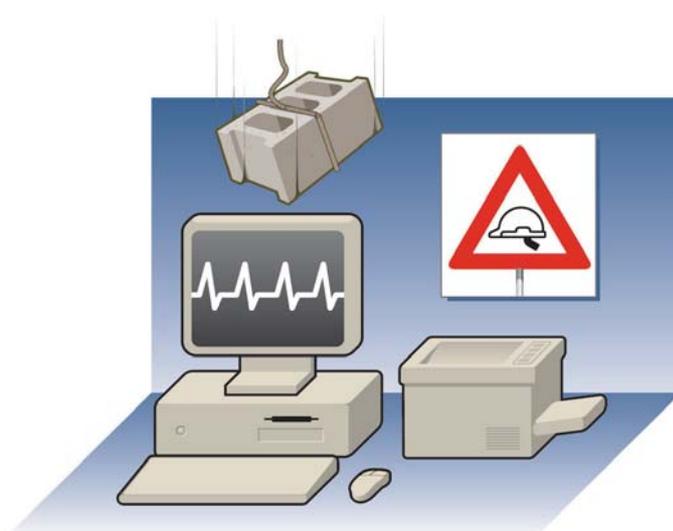
Par «vulnérabilités» on entend toutes les faiblesses des ressources informatiques qui peuvent être exploitées par des menaces, dans le but de les compromettre. Une telle exploitation peut causer des pertes importantes. De nouvelles vulnérabilités sont découvertes quotidiennement et peuvent concerner toute

ressource informatique.

Les vulnérabilités sont beaucoup trop nombreuses pour être énumérées exhaustivement, toutefois selon différents standards et écoles tels que BS7799, EBIOS ou encore GMITS, il est possible de les regrouper en trois familles.

## Table des matières

- 1 C'est quoi ? →
- 2 Qui est concerné ? →
- 3 Comment cela fonctionne-t-il ? →
- 4 Pourquoi se protéger ? →
- 5 Comment se protéger ? →



## 1 C'est quoi ?

**Par «vulnérabilités» on entend toutes les faiblesses des ressources informatiques qui peuvent être exploitées par des menaces, dans le but de les compromettre.**

Nous détaillerons trois grandes familles de vulnérabilités :

### 1.1 Les vulnérabilités au niveau organisationnel (Management)

L'absence d'une gestion correcte d'un système informatique peut rapidement conduire à sa compromission (ressources jugées critiques internes à l'organisation).

En effet, c'est au niveau de la gestion des solutions que doivent être définies les règles d'utilisation et d'implémentation de ces dernières. C'est également à ce niveau que doivent être mis en place les contrôles permettant de veiller au respect des règlements. La création et la distribution des procédures régissant le bon fonctionnement de la solution sont aussi régies à ce niveau.

### 1.2 Les vulnérabilités au niveau physique

Cette famille comprend toutes les vulnérabilités liées aux événements imprévisibles comme les pannes, les accidents ou encore les atteintes intentionnelles aux matériels. C'est en

réponse à cette famille de vulnérabilités que l'on analysera toutes les caractéristiques physiques des salles et équipements informatiques et que l'on parlera également de «Plan de Continuité».

### 1.3 Les vulnérabilités au niveau technologique

Cette famille de vulnérabilités est de loin la plus mouvante, en effet, elle comprend toutes les vulnérabilités liées à l'utilisation de technologies ou solution (hardware, software). Beaucoup de personnes sont actives dans la recherche des vulnérabilités et ainsi de nouvelles failles apparaissent quotidiennement. À cette famille de vulnérabilité appartiennent aussi toutes les failles liées aux problèmes d'interopérabilités, aux nécessités de migration et à l'introduction de nouveaux produits.

## 2 Qui est concerné ?

Tous les citoyens, PME et administrations confondus, utilisant les Nouvelles Technologies de l'Information et de la Communication (N.T.I.C), notamment Internet.

→ suite

## 3 Comment cela fonctionne-t-il ?

Il est impossible de caractériser de façon exhaustive le fonctionnement de toutes les vulnérabilités. Elles sont bien trop nombreuses. Le but de ce paragraphe n'est donc pas d'établir une liste exhaustive, mais de mentionner quelques vulnérabilités types, qui font courir un risque important aux systèmes d'informations et de communication.

### 3.1 Les vulnérabilités au niveau organisationnel (Management)

- Manque de maîtrise de la sécurité des systèmes d'information et de communication : des ressources humaines spécifiques doivent être affectées à la surveillance des systèmes d'information et de communication. Ces ressources doivent aussi procéder à la correction des manquements.
- Mauvaise utilisation des moyens en place : même si des règles ont été mises en place au niveau de la gestion des accès (mot de passe), l'absence de contrôles effectifs a pour conséquence beaucoup d'utilisateurs ayant tendance à ne pas changer leur mot de passe et à en utiliser certains de type « faibles ».
- Absence de procédures relatives à la sécurité des systèmes d'information et de communication : les règles à respecter sont rarement énoncées de façon claire.
- Manque d'information des utilisateurs : même si des procédures de sécurité des systèmes d'information et de communication existent, souvent les utilisateurs et les gestionnaires des systèmes semblent ne pas en avoir connaissance.
- Inadéquation entre la politique de sécurité et les risques : l'évaluation réelle des risques encourus n'est réalisée que rarement et donc les mesures de sécurité mises en place ne sont souvent pas en adéquation avec les risques encourus.
- Organisation interne : la multiplication des pôles informatiques avec leurs solutions dédiées soit disant moins coûteuses entraîne une complexité voire une impossibilité à gérer la sécurité des systèmes d'informations et de communication de façon centralisée.

### 3.2 Les vulnérabilités au niveau physique

- Non-redondance : que ce soit pour des raisons liées aux systèmes informatiques, logiciels ou conditions physiques (température, courant...), l'indisponibilité d'un serveur ou d'une base de données peut entraîner la rupture de services.
- Manque de contrôle d'accès aux éléments physiques : l'accès aux salles informatiques, connectiques ou autres doit être limité de manière à éviter des manipulations (in)volontaires, mais pouvant causer la perte globale de la salle informatique ou de la connectique d'une partie des utilisateurs.
- Mauvaise conservation de supports de sauvegarde : les supports de sauvegarde sont souvent stockés dans la salle informatique ce qui les rend inopérants en cas de sinistre.
- Mauvaise gestion des ressources : les ressources doivent être dimensionnées de façon correcte et doivent être surveillées de près.
- Absence de gestion du câblage : l'absence de documentation du câblage peut entraîner des déconnexions intempestives voire la mise à disposition de ressources sur des réseaux publics.

### 3.3 Les vulnérabilités au niveau technologique

- Interopérabilité des systèmes d'information et de communication : afin de permettre une communication aisée entre différents systèmes, des couches de communication supplémentaires sont souvent mises en place, qui peuvent entraîner l'apparition de nouvelles vulnérabilités.
- Fiabilité des mises à niveau et correctifs (patches) : souvent, la mise en place des correctifs se fait dans l'urgence et sans évaluation préalable.
- Complexité des règles sur les pare-feux et routeurs : la mise en place de filtrages et règles d'accès, à la demande, rend la vue d'ensemble quasi-impossible.

[→ suite](#)

## 4 Pourquoi se protéger ?

Les vulnérabilités constituent les récepteurs des menaces auxquelles sont soumis tous les utilisateurs de systèmes informatiques. En effet, l'exploitation d'une vulnérabilité par une menace peut causer des pertes importantes :

### ⚠ Pertes financières directes

- destruction de données cruciales,
- mise hors service de tout le système informatique,
- ...

### ⚠ Perte de réputation

- mise en cause de la crédibilité dans le cas de divulgation d'informations hautement confidentielles,
- ...

### ⚠ Perte de temps

- détection des failles de sécurité,
- installation de patch de sécurité,
- efforts pour rétablir les données détruites,
- ...

## 5 Comment se protéger ?

### Une bonne adresse.

Dans le domaine des vulnérabilités technologiques, il est conseillé de consulter le site :

« [www.sans.org](http://www.sans.org) »,

lequel tient à jour une liste des 20 vulnérabilités les plus en vogue ainsi qu'une liste des 10 vulnérabilités les plus exploitées par système d'exploitation (OS).

Vous trouverez ces informations à l'adresse suivante :

« [www.sans.org/top20](http://www.sans.org/top20) ».