CAHIERS AFRICAINS DES DROITS DE L'HOMME ET DE LA DÉMOCRATIE
AINSI QUE DU DÉVELOPPEMENT DURABLE
REVUE AFRICAINE INTERDISCIPLINAIRE

ISSN : 2791-1063 (Imprimé)
ISSN : 2791-1071 (En ligne)

25ème année - Numéro 71 - Volume 1 - Avril-Juin 2021

LES FACTEURS DE LA VULNÉRABILITÉ D'UN RÉSEAU INFORMATIQUE DES ENTREPRISES : CAUSES ET CONSÉQUENCES

Par

Héritier BUEYA MAVANGA
Assistant à l'Institut Supérieur Pédagogique de Kangu à Tshela

RÉSUMÉ

*Dans le domaine de la sécurité informatique, une **vulnérabilité** ou **faille** est une faiblesse dans un système informatique permettant à un attaquant de porter atteinte à l'intégrité de ce système, c'est-à-dire à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient.*

Ces vulnérabilités sont la conséquence de faiblesses dans la conception, la mise en œuvre ou l'utilisation d'un composant matériel ou logiciel du système, mais il s'agit souvent d'anomalies logicielles liées à des erreurs de programmation ou à de mauvaises pratiques. Ces dysfonctionnements logiciels sont en général corrigés à mesure de leurs découvertes, mais l'utilisateur reste exposé à une éventuelle exploitation tant que le correctif (temporaire ou définitif) n'est pas publié et installé.

C'est pourquoi, il est important de maintenir les logiciels à jour avec les correctifs fournis par les éditeurs de logiciels. La procédure d'exploitation d'une vulnérabilité logicielle est appelée exploit.

INTRODUCTION

Le présent article décrit les concepts de vulnérabilité d'un réseau informatique des entreprises, par « *vulnérabilité* » 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.

Toutes les entreprises, même les plus sécurisées, redoutent toujours les attaques des hackers à travers des failles informatiques. De plus, les attaques se passent souvent de manière inaperçue. En effet, 8 entreprises sur 10 qui subissent des piratages informatiques ne le savent pas.

Les réseaux informatiques sont devenus des ressources vitales et déterministes pour le bon fonctionnement des entreprises. De plus, ces réseaux sont ouverts de fait qu'ils sont pour la plupart raccordés à l'internet.

Cette merveilleuse ouverture qui permet de faciliter la communication, engendre malheureusement des risques importants dans le domaine de la sécurité informatique. Les utilisateurs de l'internet ne sont pas forcément pleins de bonnes intentions, ils peuvent exploiter les vulnérabilités des réseaux et systèmes pour réaliser leurs attaques.

Les conséquences de ces attaques peuvent être lourdes pour un particulier (pertes d'informations, ou pire encore vol d'informations, atteinte à la vie privée…) et pour une entreprise (perte du savoir-faire, atteinte à l'image de marque, perte financière…) et pour cela, les administrateurs déploient des solutions de sécurité efficace capable de protéger le réseau de l'entreprise.

1. RÉSEAU INFORMATIQUE

Le réseau informatique, c'est un ensemble d'ordinateurs et autres équipements informatiques reliés entre eux via des supports de transmission dans le but d'échanger les ressources (matérielles et logicielles).

Les différentes applications d'un réseau informatique demeurent le partage des fichiers, le partage des applications, le partage des ressources, la communication entre les processus, le partage de la connexion interne, communication entre utilisateur, les jeux.

Le réseau informatique est caractérisé par typologie, topologie, l'architecture, méthode d'accès, le protocole, le système d'exploitation, le serveur, le poste de travail, le support de transmission.

Le choix de certains matériels physiques à utiliser dans un réseau informatique dépend de certaines caractéristiques physiques ou standards.

2. SÉCURITÉ D'UN RÉSEAU INFORMATIQUE[1]

La sécurité d'un réseau informatique est l'ensemble des techniques qui assurent que les ressources du système d'information (matérielles ou logicielles) d'une organisation sont utilisées uniquement dans le cadre où il est prévu qu'elles soient.

[1] https://www.commentcamarche.net/contents/

2.1. La sécurité informatique vise généralement cinq principaux objectifs[2] :

- **L'intégrité**, c'est-à-dire garantir que les données soient bien celles que l'on croit être ;
- **La confidentialité**, consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées ;
- **La disponibilité**, permettant de maintenir le bon fonctionnement du système d'information ;
- **La non répudiation**, permettant de garantir qu'une transaction ne puisse être niée ;
- **L'authentification,** consistant à assurer que seules les personnes autorisées aient accès aux ressources.

2.2. Méthodes[3]

Il existe de nombreuses méthodes permettant de mettre au point une politique de sécurité. Voici une liste non exhaustive des principales méthodes :

- **MARION** (*Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux*), mise au point par le CLUSIF ;
- **MEHARI** (*Méthode Harmonisée d'Analyse de Risques*)[4] ;
- **EBIOS** (*Expression des Besoins et Identification des Objectifs de Sécurité*), mise au point par la DCSSI (*Direction Centrale de la Sécurité des Systèmes d'Information*)[5].

2.3. Test d'intrusion[6]

Un test d'intrusion consiste à tester la sécurité d'un système informatique en effectuant des attaques dans le but d'identifier les vulnérabilités du système et de proposer des correctifs de sécurité.

Les tests d'intrusion et les tests de vulnérabilités diffèrent de par leurs objectifs. Un test de vulnérabilité repose sur des scanners automatiques qui permettent d'identifier rapidement les failles les plus courantes.

---

[2] https://web.maths.unsw.edu.au/~lafaye/CCM/secu/secuintro.htm
[3] https://www.piloter.org/systeme-information/securite-informatique.htm#methodes
[4] https://www.clusif.asso.fr/fr/production/mehari/
[5] http://www.ssi.gouv.fr/fr/confiance/ebios.html
[6] https://www.vaadata.com/blog/fr/test-dintrusion-approche-methodologie-types-de-tests-et-prix/

Le test d'intrusion va plus loin. Il inclut, notamment la recherche de failles logiques, non détectables par des outils automatiques et une phase d'exploitation manuelle des vulnérabilités identifiées. C'est une méthode d'audit de sécurité éprouvée plus complète, qui permet de mesurer l'impact réel de tout type de faille.

Un test d'intrusion peut inclure des tests en boite noire, en boite grise ou en boite blanche. Les tests en boite noire ciblent la surface d'attaque accessible à n'importe quel attaquant externe, tandis que des tests en boite grise vont concerner des éléments disponibles uniquement à des clients, des partenaires ou des salariés d'une entreprise. L'audit en boite blanche quant à lui permet d'analyser le niveau de sécurité en disposant des mêmes accès qu'un administrateur du système (serveur, application…).

2.3.1. Méthodologie de test d'intrusion

Un test d'intrusion repose sur une méthodologie en quatre phases, qui constituent un processus cyclique : Reconnaissance, Mapping, Discovery, Exploitation.

❖ **Mapping**

La phase de mapping permet de répertorier l'ensemble des fonctionnalités de la cible de l'audit. Cette étape permet aux pentesters d'avoir une meilleure visibilité sur les éléments les plus critiques et les plus exposés.

Cette étape est particulièrement indispensable lorsque l'objectif de l'audit de sécurité est de conduire des tests sur toutes les fonctionnalités d'une cible.

❖ **Discovery**

La phase de discovery est une phase d'attaque : les pentesters recherchent des vulnérabilités via des recherches manuelles complémentées par des outils automatisés. L'objectif est de découvrir le maximum de failles possibles sur la cible.

❖ **Exploitation**

La phase d'exploitation consiste à tester les exploitations possibles, des failles identifiées lors de la phase précédente. Cette étape permet de rebondir en utilisant certaines failles comme un pivot, dans le but de découvrir de nouvelles vulnérabilités. L'exploitation des failles de sécurité permet notamment d'évaluer leur impact réel et donc leur niveau de criticité.

2.3.2. Mesures de sécurité et bonnes pratiques à implémenter

L'objectif final du test d'intrusion est de fournir des recommandations concrètes permettant d'améliorer le niveau de sécurité de la cible.

L'étape suivante est donc la prise en compte de ces recommandations pour corriger à minima les vulnérabilités les plus critiques. Certains correctifs peuvent également être intégrés dans les projets d'évolutions fonctionnelles et techniques ou implémentés sur d'autres systèmes présentant des similitudes avec la cible des tests.

Un test d'intrusion permet aussi de faire évoluer certaines pratiques, de mettre en place de nouveaux processus permettant de renforcer la sécurité et d'améliorer le niveau de vigilance de l'entreprise face aux risques.

3. LES FACTEURS DE LA VULNÉRABILITÉ D'UN RÉSEAU INFORMATIQUE[7]

Une vulnérabilité est une faute accidentelle ou intentionnelle (avec ou sans volonté de nuire), dans la spécification, la conception ou la configuration du système, ou dans la façon selon laquelle il est utilisé. La vulnérabilité peut être exploitée pour créer une intrusion.

- Une attaque est une faute d'interaction malveillante visant à violer une ou plusieurs propriétés de sécurité. C'est une faute externe créée avec l'intention de nuire. Une attaque peut être ou non réalisée par des outils automatiques.
- Une intrusion est une faute malveillante interne, mais d'origine externe, résultant d'une attaque qui a réussi à exploiter une vulnérabilité.

Il existe une grande variété de vulnérabilités visant les applications Web. Toutefois certaines sont plus connues et plus dangereuses que d'autres. Plusieurs bases de données répertoriant ces vulnérabilités avec des statistiques indiquant leur importance relative existent. Nous citons par exemple les bases de données de vulnérabilités telles que CVE (Common Vulnerabilities and Exposures), NVD (National Vulnerability Database) ou VUPEN (Vulnerability Penetration testing). Ces bases de données répertorient tous types de vulnérabilités, incluant celles ciblant les serveurs et applications Web.

[7] https://www.sekurigi.com/2018/04/les-failles-informatiques-les-plus-courantes/

La multiplication des vulnérabilités et des attaques sur des sites web sur Internet ont poussé de nombreuses organisations à poser un regard critique sur la qualité de la sécurité de leurs applications web.

Ainsi, plusieurs communautés ont vu le jour, dans le but d'améliorer la sécurisation des applications web. Les travaux dans ce contexte se sont traduits aussi par la proposition de taxonomies et de classifications pour les vulnérabilités et les attaques web les plus répandues. Parmi ces communautés, nous citons OWASP (Open Web Application Security Project) et WASC (Web Application Security Consortium).

Nous détaillerons trois grandes familles de vulnérabilités :

❖ **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.

❖ **Les vulnérabilités au niveau physique**

Cette famille comprend toutes les vulnérabilités liées aux évènements 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 ».

❖ **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.

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.

❖ **Les vulnérabilités les plus courantes sont :**

✓ **La vulnérabilité « SQL Injection» :** les hackers procèdent par la technique des injections SQL pour s'introduire discrètement sur le système de l'entreprise dans le but de s'approprier illégalement des informations confidentielles. Les pirates injectent un « malware » par le biais de codes JavaScript, dans le but de porter atteinte à l'entreprise.

✓ **La vulnérabilité « Cross Site Scripting» ou « XSS » :** c'est le type d'attaque le plus fréquent sur les sites Internet. Les impacts pour ce type d'attaque sont multiples, pour ne pas citer que la redirection vers un site d'hameçonnage, le vol des sessions utilisateurs ou encore le vol de données sensibles.

✓ **La vulnérabilité « Broken Authentification and Session Management » :** cette vulnérabilité permet aux hackers d'usurper l'identité d'un utilisateur dont l'identifiant a été volé et utilisé à son insu. Ce type de cas arrive surtout pour les entreprises avec des réseaux dont les requêtes HTTP ne seraient pas en SSL.

✓ **La vulnérabilité « Cross Site Request Forgery » :** ce type de vulnérabilité repose également sur le principe d'injection de codes malveillants.

✓ **Les vulnérabilités web**

Les vulnérabilités web représentent des risques non négligeables en matière de sécurité informatique.

4. LES CAUSES DE LA VULNÉRABILITÉ

❖ **Failles au niveau des protocoles d'administration**

Pour ce type de faille, les négligences en matière de sécurité se trouvent au niveau des éléments actifs comme les switchs, les routeurs ou encore les imprimantes. Souvent, les mots de passe d'administration par défaut pour accéder à ces types d'équipement restent inchangés. Ce type de faille est souvent exploité par les hackers pour porter atteinte à l'entreprise.

❖ **Failles au niveau des bases de données**

Les bases de données constituent une cible privilégiée des pirates informatiques. Ce type de faille s'explique souvent par l'utilisation de mots de passe qui sont en fonction du nom du serveur. Certains administrateurs de bases de données usent de cette technique lorsqu'ils gèrent un grand nombre de serveurs, afin de mémoriser plus facilement les mots de passe. Les hackers exploitent cette faille pour accéder aux fichiers de la base de données pour pouvoir ensuite obtenir d'autres comptes utilisateurs avec des mots de passe faibles. Ces mots de passe faibles peuvent être facilement décryptés par la technique de cassage. Ces comptes piratés seront par la suite utilisés par le hacker pour poursuivre son attaque sur l'ensemble du réseau.

❖ **Failles au niveau du partage de fichiers**

La plupart des entreprises, pour ne pas dire toutes les entreprises, utilisent le partage de fichiers. Le plus souvent, la restriction est rarement préconisée. Pourtant le partage de fichiers non sécurisés représente une porte sans serrure pour les hackers et leur permettant d'obtenir des informations sensibles, voire confidentielles, de l'entreprise. Pour les imprimantes les plus récentes par exemple, des failles permettant aux pirates informatiques de récupérer des données numérisées ou photocopiées dans l'entreprise existent, si aucune mesure de sécurité informatique adaptée n'a été prise en amont.

❖ **Failles au niveau de la gestion des droits**

Dans beaucoup d'entreprises, les restrictions d'accès sont parfois trop laxistes, et parfois même inexistantes. Des études menées par les experts en sécurité informatique ont déduit que 50% des menaces proviennent directement des employés de l'entreprise. Non pas parce qu'ils sont malintentionnés, mais souvent ils ne sont conscients des risques que représente leur laxisme en matière de **sécurité informatique**. Bref, ils constituent le maillon faible de la chaine de sécurité informatique. Par exemple, en permettant à un stagiaire d'utiliser la session de son encadreur au sein de la boîte. L'entreprise s'expose à des risques comme **le vol d'informations stratégiques ou confidentielles**.

❖ **Défauts de gestion de mot de passe :**

L'utilisateur de l'ordinateur utilise des mots de passe faibles qui pourraient être découverts par la force brute. L'utilisateur de l'ordinateur stocke le mot de passe sur l'ordinateur sur lequel un programme peut y accéder. Les mots de

passe des utilisateurs réutilisation entre de nombreux programmes et sites Web.

❖ **Bugs logiciels :**

Le programmeur laisse un bug exploitable dans un logiciel. Le bug logiciel peut permettre à un attaquant d'abuser d'une application.

5. LES CONSÉQUENCES DE LA VULNÉRABILITÉ[8]

L'impact d'une atteinte à la sécurité peut être très élevé. Le fait que les responsables informatiques ou la haute direction, peut (facilement) savoir que les systèmes et applications informatiques ont des vulnérabilités et ne réalise aucune action pour gérer le risque informatique est considérée comme une faute dans la plupart des législations. Vie privée, loi force les gestionnaires d'agir pour réduire l'impact ou de la probabilité de ce risque de sécurité.

Vérification de la sécurité des technologies de l'information est un moyen de laisser d'autres personnes indépendantes certifient que l'environnement informatique est géré correctement et réduire les charges, au moins avoir fait preuve de la bonne foi. Test de pénétration est une forme de vérification de la faiblesse et des contre - mesures adoptées par une organisation: un chapeau blanc pirate tente d'attaquer les actifs de technologie de l'information d'une organisation, pour savoir comment il est facile ou difficile de compromettre la sécurité informatique.

La bonne façon de gérer, de manière professionnelle le risque informatique est d'adopter un système de gestion de sécurité de l'information , tels que ISO/IEC 27002 ou des risques informatiques et de les suivre, selon la stratégie de sécurité prévue par la haute direction.

L'un des concepts - clé de la sécurité de l'information est le principe de la défense en profondeur : à- dire de mettre en place un système de défense multicouche qui peut:

- empêcher l'exploit ;
- détecter et intercepter l'attaque ;
- trouver les agents de menace et de les poursuivre en justice.

[8] https://fr.other.wiki/wiki/Vulnerability_(computing)

Système de détection d'intrusion est un exemple d'une classe de systèmes utilisés pour détecter les attaques. La sécurité physique est un ensemble de mesures visant à protéger physiquement l'actif de l'information : si quelqu'un peut obtenir un accès physique à l'actif de l'information, il est assez facile de rendre les ressources disponibles à ses utilisateurs légitimes.

CONCLUSION

Le risque infectieux informatique est bien réel et représente l'une des plus grandes menaces de demain mais il convient de le considérer non plus isolément mais dans la perspective plus large de la sécurité des réseaux, des applicatifs, des protocoles. En d'autres termes, la lutte contre le risque viral ne peut se faire sans une veille technologique de tous les instants. La découverte périodique de failles exploitables par des programmes infectieux et la publication des correctifs correspondants doivent être connus du responsable de la sécurité informatique de l'entreprise.

La sécurité des systèmes d'information prend tout son sens dans un contexte tel que celui dans lequel nous avons travaillé et représente aujourd'hui une tâche de fond à prendre en compte par toute entreprise qui désire disposer d'un ensemble d'outils et de méthodes qui lui permettent d'assurer la gouvernance de son système d'information.

Après la définition d'une politique de sécurité et la connaissance des principes de base de la sécurité, l'implémentation d'un processus de sécurité s'avère indispensable afin d'instaurer un réseau sécurisé. Bien évidement la sécurité à 100% reste un idéal à atteindre, surtout devant le large éventail des menaces qui mettent en danger l'exploitation d'un système d'information dans une entreprise.

Ainsi, il est important de bien formaliser une politique de sécurité en prenant en compte les risques réels qu'encourt un système informatique et en évaluant les coûts que peuvent engendrer les problèmes résultants de ces risques par rapport au coût nécessaire à la mise en place des solutions palliatives à ces problèmes. Enfin, l'élaboration d'une charte d'utilisation du réseau informatique et surtout une sensibilisation des utilisateurs du réseau sur le bien-fondé de ces mesures de sécurité ainsi que leur importance.

BIBLIOGRAPHIE

I. OUVRAGES

- ACISSI, *Sécurité informatique Ethical Hacking apprendre l'attaque pour mieux se défendre,* (3ème édition) Broché – 12 septembre 2012.
- GALLARD Jean-Christophe, *Sécurité et Réseaux*, CNAM, France, 2005.
- PUJOLLE Guy, *Les réseaux locaux,* Eyrolles, 2003.
- ROLIN Pierre, *Sécurité réseau informatique*, éd. Hermès, 5e édition.
- THEOLEYRE Fabrice, *La sécurité des réseaux les pare - feu*, INSA LYON, 2006.

II. WEBOGRAPHIE

- https://fr.wikipedia.org/wiki/Vulnérabilité_(informatique)
- https://repo.zenk-security.com/
- http://www.clusib.be/wp/wpcontent/uploads/2012/11/Risquesinformatiques_fr.pdf.pdf
- https://dl.ummto.dz/bitstream/handle/ummto/6275/MihoubiMohamed_MedjaniN.pdf?sequence=1
- http://www.offensive-security.com/
- www.clusif.fr
- http://www.ducrot.org/securite.pdf