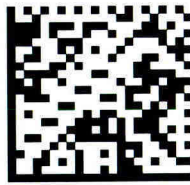


NOM BOUKHELOUA

Prénom Rémi

Promo 2020

Date 11.01



20150257: BOUKHELOUA Rémi

M1:

ST2ICS-DE (11/01/2019)

Grand amphi

## MATIÈRE Cyber sécurité

1. La cyber sécurité vise à garantir la disponibilité, l'intégrité, la traçabilité ~~et la~~ et la confidentialité du réseau, et des ses utilisateurs et des données et messages qui y circulent. Au vu du développement de l'économie digitale, les entreprises ont pour ~~but~~ <sup>but</sup> la mise à disposition auprès de ses clients d'un certain nombre de services incluant de plus en plus de données confidentielles et sensibles. Elles n'ont donc plus uniquement leurs informations à protéger mais aussi ~~de~~ de plus en plus d'informations venant de leurs clients. De plus, de par l'augmentation de l'importance du numérique, le nombre de postes reliés à Internet a augmenté. Cela fait d'autant plus de postes "vulnérables" à sécuriser. Avec le développement de l'économie digitale, le rôle de la cyber sécurité a donc fortement augmenté.

Enfin, le digital est aussi un moyen de véhiculer une certaine image de marque. Inutile <sup>et donc</sup> qu'une violation de la plateforme ~~soit~~ <sup>soit</sup> fait aurait un impact sur la confiance du client et donc sur cette image de marque. Avec le développement de l'économie digitale, le rôle de la cybersécurité a donc fortement augmenté.



3. Parmi les composants techniques et organisationnels constituant un système d'information concernant la sécurité du système d'information, on retrouve notamment :

- l'administration des serveurs
- l'administration des postes de travail et réseaux
- A** - la sécurisation des postes de travail et réseaux
- la mise à disposition du réseau
- la sécurité du réseau
- la construction d'un code ou d'une charte d'utilisation décrivant droits et devoirs des utilisateurs.

D'un point de vue ~~technique~~ <sup>technique</sup> ~~non technique~~, on retrouve les postes et serveurs à sécuriser, un ~~firewall~~ <sup>pare-feu</sup> ~~qui permet de~~ la mise en place d'une whitelist/blacklist, les éléments liés au réseau du SI (DMS, routeurs, switch...) et les outils informatiques (antivirus, IPS / IDS, ~~et~~ logiciels).

**S. 1.** Equifax est une société qui propose d'évaluer la **B** capacité de une personne ou d'une autre entreprise à rembourser un crédit au ~~bas de~~ <sup>avant</sup> la souscription à une assurance. (évaluation de la note de crédit)

**S. 2.** • Un scénario redouté par Equifax est le vol d'informations confidentielles.

• Un second scénario redouté par Equifax serait une violation de l'intégrité du système et notamment de la base de données étant donné que les pirates ont réussi à pénétrer dans leur SI et accéder ~~à~~ <sup>aux</sup> cette ~~donnée~~ <sup>donnée</sup> information dans la BDD.

perte de disponibilité étant donné que les pirates se sont introduits dans leur SI et qu'il est question d'un manque à gagner sur une période.



5.3. Val de données : L'impact d'une telle violation est financier (perte du CA), juridique (diminution responsabilité dans la divulgation), social (impact <sup>forte</sup> diminue la vie des concernés par cette fuite) et une baisse de confiance ~~des~~ des clients et investisseurs (image de marque). ~~Ce~~ Le scénario est de l'ordre de la confidentialité principalement. Des lors qu'il occasionne une perte de plus de 100k\$, sa gravité est caractérisée de majeure ~~(4 et 5)~~ 4. Etant donné la présence d'un patch de patch mais j'estime sa vraisemblance à 3  $\frac{1}{2}$ .

~~Violation de l'intégrité : L'impact d'une telle violation serait financier, juridique et nuirait à l'image de marque d'Equifax. Ce scénario concerne principalement l'intégrité.~~

~~Des Externe Il ne peut être séparé des premier vers à vis de sa gravité. Il le note donc à 4. Ce pendant, étant donné que rien n'a été détecté depuis, j'estime sa vraisemblance plus bas à 1 (rare). A noter que cela se situe en interne, cf l'ouvrage mentionné.~~

Disponibilité : L'impact d'une telle violation serait financière (manque à gagner), juridique et nuirait à l'impact de marque d'Equifax. Ce scénario concerne évidemment la disponibilité du service ~~de~~ digitale. Il ne peut être séparé du 1<sup>er</sup> vers à vis de sa gravité et de sa vraisemblance étant donné qu'ils ont les mêmes conséquences. (4 et 3).



5.4. Niveau de risque :

Gravité Vraisemblance	Léger (1)	Moyen (2)	Critique (3)	Intélab (4)
Rare (1)	1	2	3	4
Commune (2)	2	3	4	5
(3)	3	4	5	6
Récurrent (4)	4	5	6	7

5.5 Les deux scénarios ayant la même gravité et la même vraisemblance, ils partagent le même risque de 6.

5.6. Afin de réduire les risques liés à cette partie du SI (application web), il faut appliquer le patch disponible depuis mars. Cependant, il resterait des risques résiduels comme l'existence de l'autre ~~faible~~ vulnérabilités liées au site ou au patch.

2. Les quatre critères qui doit garantir la sécurité d'un système d'informations sont la disponibilité, l'intégrité, la preuve et la confidentialité. Ce sont les paramètres qui sont utilisés lors de l'analyse des risques. La sécurité d'un SI est définie par ~~la sécurité~~ l'infrastructure et la capacité des ~~utilisateurs~~ responsables à prévenir l'usage des utilisateurs.

4. La norme ISO 27002 est relative à l'administration ~~d'un système~~ des postes utilisateurs et nomades ainsi qu'à leur sécurisation.