COMITÉ ÉTIQUE

Comment colmater les brèches des systèmes informatiques ultra sécurisés suite aux cyberattaques mondiales ?

Rapport réalisé par Meryem ICEN - Président de Comité

DEFINITIONS

Cyber-attaque

Une cyber-attaque est une atteinte à des systèmes informatiques réalisée dans un but malveillant.

Elle cible différents dispositifs informatiques : des ordinateurs ou des serveurs, isolés ou en réseaux, reliés ou non à Internet, des équipements périphériques tels que les imprimantes, ou encore des appareils communicants comme les téléphones mobiles, les smartphones ou les tablettes.

Introduction

Contexte

« Cyberattaque mondiale : le bilan s'alourdit : NotPetya, un virus très dangereux mais pas rentable»

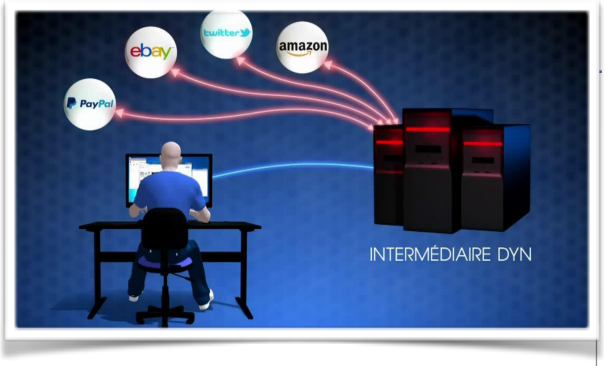
Il existe quatre types de risques cyber aux conséquences diverses, affectant directement ou indirectement les particuliers, les administrations et les entreprises : la cybercriminalité, l'atteinte à l'image, l'espionnage, le sabotage. »

Le but de ces cyberattaques est donc d'atteindre à la vie d'autrui ou d'une entreprise en accédant à leurs informations confidentielles ou des fichiers administratifs

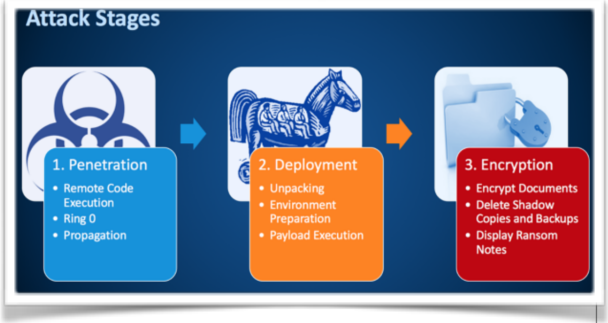
pour s'en servir ensuite de manière illégale cela permet aux hacker de soutirer de l'argent aux victimes des cyberattaques en utilisant des logiciels du type : « rançongiciels » (NotPeyta, WannaCry qui sont des virus) .

Aujourd'hui, les cyberattaques se multiplient et touchent divers plateforme tel que Uber et Yahoo mais celles-ci ont également toucher l'armée française une dizaine de fois en 2017. Cependant ces attaques ont lieu dans le monde entier particulièrement aux Etats-Unis et en Ukraine.

Comment renforcer les systèmes informatiques ultra sécurisé afin de lutter contre les cyberattaques mondiales ?



Dans un premier temps, nous présenterons les quatres différents types de cyberattaques et leurs conséquences sur la société et l'économie ainsi que les principaux acteurs de ces attaques. Dans un second temps, nous étudierons les différents systèmes mis en place pour lutter contre les cyberattaques ainsi que leurs résultats. Enfin, nous proposerons les solutions possibles ainsi que l'implication des différents pays du monde et les organisations mondiales afin de lutter contre toutes ces attaques.



Concernant les quatre types de cyberattaques, nous trouvons la cybercriminalité, l'atteinte à l'image, l'espionnage ainsi que le sabotage. Ils constituent les risques ainsi que le but des cyberattaques.

La cybercriminalité se base sur le hameçonnage (pishing) ainsi que le « rançongiciels ».

L'hameçonnage, phishing ou filoutage est une technique malveillante très courante sur Internet. » L'objectif du hameçonnage consiste a usurper l'identité d'autrui afin d'obtenir les informations personnels de la victime (identifiants bancaires) à des fins d'usage criminels. Pour obtenir les informations d'une personne, le « cybercriminel » envoi un mail frauduleux dans lequel il invite sa victime à mettre a jour ses informations personnelles (tel que les identifiant bancaire). Ce mail comporte un lien de site internet falsifié, qui permettra au cybercriminel de se procurer ces informations et de les réutiliser.

Les attaques par « rançongiciels » ont le même fonctionnement que le hameçonnage. Le procédé se déroule toujours via un mail envoyé par le cybercriminel qui cette fois-ci contient des pièces jointes ou des liens piégés qui permettent, lors de l'ouverture du fichier, l'installation d'un virus qui va demander le versement d'une rançon en échange de la clé de déchiffrement. L'objectif du « rançongiciel » est de chiffrer les données de la victime pour ensuite lui soutirer de l'argent en lui faisant du chantage.

L'atteinte à l'image se base sur des attaques par déni de service ou attaque par déformation.

L'atteinte à limage a été « Lancées à des fins de déstabilisation contre des administrations et des entreprises et régulièrement relayées par les réseaux sociaux, les attaques de déstabilisation sont aujourd'hui fréquentes et généralement peu sophistiquées, faisant appel à des outils et des services disponibles en ligne. De l'exfiltration de données personnelles à l'exploitation de vulnérabilité, elles portent atteinte à l'image de la victime en remplaçant le contenu par des revendications politiques, religieuses, etc.

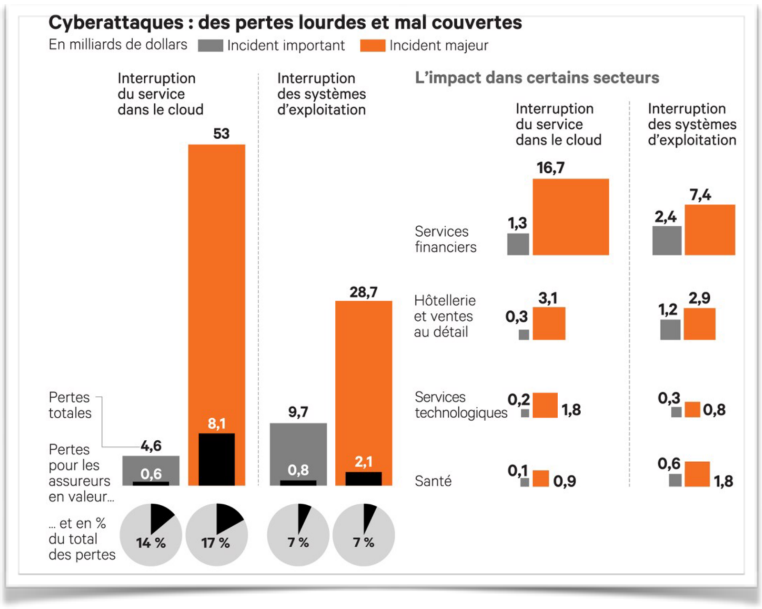
Les attaques par déni de service ciblent les organisation disposant d'un système informatique relié à internet. Le déni de service a pour but de rendre le site internet d'une organisation indisponible à des fins de revendications ou encore d'extorsions de fonds. Cela permet au cybercriminel d'« exploiter une vulnérabilité logicielle ou matérielle » ou « solliciter une ressource

particulière du système d'information de la cible, jusqu'à “épuisement “. ».

Les attaques par déformation sont réalisés pour but de modifier les contenus des sites internet « et donc violer l’intégrité des pages en les altérant. ». Le cybercriminel se sert des défauts de sécurité des sites internet pour ensuite procéder à des modifications tel que l’ajout d’informations fausses ou de revendications.

L’espionnage est «Très ciblées et sophistiquées, les attaques utilisées pour l’espionnage à des fins économiques ou scientifiques sont souvent le fait de groupes structurés et peuvent avoir de lourdes conséquences pour les intérêts nationaux. De fait, il faut parfois des années à une organisation pour s’apercevoir qu’elle a été victime d’espionnage, l’objectif de l’attaquant étant de maintenir discrètement son accès le plus longtemps possible afin de capter l’information stratégique en temps voulu. ». Concernant l’espionnage, il existe deux techniques d’attaques qui sont : l’attaque par point d’eau (Watering Hole) et l’attaque par hameçonnage (que nous avons déjà vu). Cette attaque permet de piéger des sites internet pour « infiltrer discrètement les ordinateurs de personnels œuvrant dans un secteur d’activité ou une organisation ciblée pour récupérer des données. ». Cette attaque est faite dans une discrétion totale de la part du cybercriminel.

L’attaque par hameçonnage dans le domaine de l’espionnage permet d’ « infiltrer le système d’information d’une organisation d’un secteur d’activité ciblé ».



Le sabotage en informatique est le fait de rendre inopérant tout ou partie d’un système d’information d’une organisation via une attaque informatique. ». C’est une sorte de « panne organisée », le sabotage est la plus dangereuse cyberattaque car la panne frappe « tout ou partie des systèmes, selon le type d’atteinte recherchée. Il existe de nombreux

type d'attaques pour le sabotage qui permettent de détruire les systèmes informatiques et cela peut provoquer « des conséquences dramatiques sur l'économie d'une organisation, sur la vie des personnes, voire sur le bon fonctionnement de la Nation s'ils touchent des secteurs d'activité clés. »

Récemment, selon un article du célèbre journal français le Parisien, une cyberattaque mondial a eu lieu en 2017 via un virus « NotPetya » : « Les premiers ordinateurs infectés par NotPetya l'ont été mardi, principalement en Ukraine et Russie. Une mise à jour automatique du logiciel comptable ukrainien MEDoc pourrait être à l'origine de la propagation. Les machines infectées, connectées en réseau, en auraient ensuite infecté d'autres. Contaminés, les ordinateurs affichent tous un seul message : une demande de rançon de 300 dollars en bitcoins. » 29 juin 2017, 17h12. Cette attaque a apporter moins de 10000 euros au pirates.

Voici quelques exemple d'organisation de cybercriminels majeur qui ont été «démasqué» :

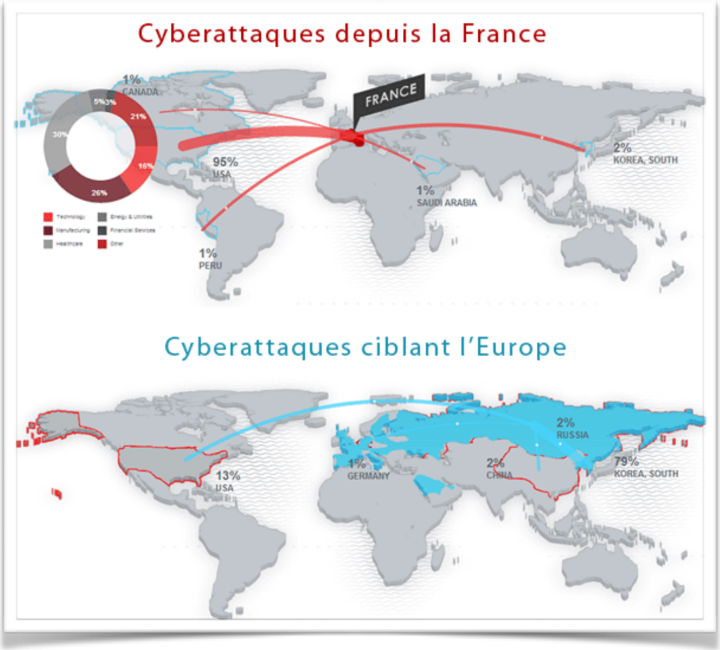
- Le groupe anonymous : le groupe de pirates connu sous le nom d'Anonymous a conduit des attaques contre des cibles commerciales et politiques pendant plusieurs années et les organismes d'application de la loi avaient du mal à pénétrer dans l'organisation afin de la démanteler. L'un des premiers grands succès fut les arrestations de membres d'Anonymous menées par les autorités dans plusieurs pays. Les individus arrêtés ont été accusés de mener des attaques contre des sites situés au Chili, en Colombie ainsi que dans d'autres pays.

- Sabu : En mars 2012, les autorités ont peut-être connu leur plus grand succès contre Anonymous, quand les agents fédéraux ont arrêté Sabu, le célèbre leader du groupe rejeton d'Anonymous, LulzSec. L'arrestation de Sabu a provoqué des ondes de choc parmi la communauté souterraine et a commencé à révéler peu à peu le groupe. Sabu, dont le vrai nom est Hector Xavier Monsegur, a coopéré avec le FBI et son jugement a été repoussé plusieurs fois, notamment en février dernier.

L'Europe (plus précisément la France te le Royaume-Uni), les Etats-Unis, le Japon et la Chine, ont mis en place un système de cybersécurité/cyberdéfense .

La cybersécurité est un dispositif permettant de lutter contre les cyberattaques.

Dans le monde



En Europe, Europol compte déjà 200.000 victimes, réparties dans 150 pays. L'organisation européenne de la cybersécurité (ECSO) a été créée en juin 2016 avec pour objectif d'aider les projets qui permettraient de développer, de promouvoir ou d'encourager les initiatives sur la cybersécurité en Europe. »

Un projet de directive du Parlement et du Conseil Europeen est en cour de validation.

« Il concerne des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union qui imposerait un niveau de sécurité minimum pour les technologies, les réseaux et les services numériques dans l'ensemble des États membres. Le texte propose également d'obliger certaines entreprises et organisations à signaler les incidents de sécurité informatique majeurs dont elles sont victimes La stratégie de cybersécurité de l'UE définit l'approche adoptée par l'UE pour prévenir au mieux les perturbations et les attaques informatiques et y apporter une réponse. Elle passe en revue une série d'actions visant à augmenter la cyber-résilience des systèmes informatiques, à réduire la cybercriminalité et à renforcer la politique de l'UE en matière de cybersécurité et de cyberdéfense à l'échelle internationale, pour protéger le cyberespace, dans les domaines tant civil que militaire »

En juillet 2016, le Parlement européen et le Conseil de l'Union européenne ont adopté la directive sur la sécurité des réseaux et des systèmes d'information connue sous l'appellation "directive NIS" .

Aux Etats-Unis, en février 2015, une nouvelle agence dédiée a la cybersécurité a été créer. Elle se nomme la CTIIC (The Cyber Threat Intelligence Integration Center).

Le Département de la Défense des États-Unis met à jour régulièrement sa cyberstratégie. Les cinq priorités de l'Administration américaine dans le domaine de la cybersécurité deviennent :

1 Protéger les infrastructures critiques des États-Unis;

2 Améliorer la capacité des États-Unis à identifier les cyberattaques et à rapporter celles-ci afin que le pays puisse y répondre rapidement et efficacement de manière coordonnée ;

3 Développer les partenariats internationaux afin de continuer à promouvoir la liberté sur Internet ;

4 Sécuriser les réseaux des différents États en définissant des objectifs clairs et mesurables, et responsabiliser les agences fédérales pour qu'elles atteignent ces objectifs ;

5 Éduquer pour façonner une main-d'œuvre avertie, sensibilisée aux enjeux de la cybersécurité.

D'autre dispositifs tel que le CNAP ainsi qu'un « un comité d'experts pour renforcer les mesures et adresser les problématiques gouvernementales et privées dans ce domaine (cybersecurité) », également un projet de lois baptisé SHIELD Act.

Au Japon, « Le 10 juin 2013, le Conseil Stratégique en Sécurité Informatique du Japon a adopté une première version de Plan stratégique en Cybersécurité ayant pour objectifs de créer un cyberespace dynamique et résilient et de faire du Japon un leader dans ce domaine à partir de 4 principes de base :

1 Maintenir un accès libre à l'information ;

2 Adresser les nouveaux risques informatiques ;

3 Répondre aux cybermenaces à partir d'une analyse de risque ;

4 Coopérer avec les parties prenantes conformément à une compréhension commune des enjeux de responsabilité sociale.

Le gouvernement japonais entend coopérer dans le domaine de la cybersécurité au sein de la région Asie-Pacifique, avec l'Amérique du Nord dans le cadre des accords Japon – USA et plus généralement avec chaque pays partageant les mêmes valeurs que le Japon.

Enfin, la Chine a adopté sa première loi fondamental sur la cybersécurité lors du Congres Nationale du Peuple chinois le 7 novembre 2016.

Elle formalise la notion de souveraineté nationale dans le Cyberespace et introduit des définitions proches de celles données en

France pour les opérateurs d'importance vitale et leurs infrastructures critiques.

Voici les différents but de cette loi sur la Cybersécurité pour but de maintenir la sécurité des réseaux informatiques, de sauvegarder la sécurité nationale et les intérêts publics, de protéger les droits des citoyens (et les données à caractère personnel), des sociétés et autres organisations intervenant en Chine ainsi que de promouvoir un développement sain des technologies de l'information dans les secteurs économiques et sociaux. Enfin, elle encourage la définition de standards de sécurité informatique plus rigoureux que les standards actuellement reconnus ».

SOLUTIONS

Cependant, pour éviter tout risque d'être victime de cyberattaque, concernant les particuliers, voici quelques conseils pour échapper à ces attaques :

1. Effectuer toutes les mise a jour demandés par l'ordinateur.
2. Effectuer des sauvegardes de vos données.
3. Installer un antivirus.
4. Vérifier la provenance des pièces jointe avant de les ouvrir.

L'OTAN ainsi que L'ONU sont deux organisations qui luttent contre les cyberattaques. L'ONU a effectuer un sondage concernent la lutte contre les cyberattaque dans le monde

Au total, 134 pays sur les 193 pays membres ont accepté de répondre au sondage envoyé par l'ONU. Sans surprise, les pays africains sont à la traîne sur ces sujets. Si dans l'ensemble, l'Europe et l'Amérique du Nord sont parmi les mieux classés au sein de l'index, l'Asie et l'Amérique du Sud présentent des résultats plus disparates avec certains pays jouant le rôle de leader, tandis que d'autres accusent de graves lacunes.

Sitographie

- Le Figaro. Disponible sur : http://www.lefigaro.fr/secteur/high-tech/pratique/2017/05/15/32002-20170515ARTFIG00286-comment-s-assurer-contre-les-cyberattaques.php
- Le Parisien. Disponible sur : http://www.leparisien.fr/high-tech/cyberattaque-mondiale-notpetya-un-virus-tres-dangereux-mais-pas-rentable-29-06-2017-7098114.php
- France Info TV. Disponible sur : https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/cyberattaque-la-plateforme-uber-victime-d-un-vaste-piratage-fin-2016_2479629.html
- Europe I. Disponible sur: http://www.europe1.fr/technologies/des-dizaines-de-cyberattaques-contre-les-armees-francaises-en-2017-3557255
- https://www.kaspersky.fr/blog/cybercriminalite-10-exemples-darrestations-majeures/733/
- France Info TV. Disponible sur : https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/cyberattaque-la-plateforme-uber-victime-d-un-vaste-piratage-fin-2016_2479629.html