Internet Society
Chapitre Malien

Mali Next Generation Leaders Program

LA CYBERSÉCURITÉ DANS LE NUMÉRIQUE

Rejoignez-nous

Tel: (+223) 66 83 44 86 / 66 74 35 72 / 63 46 67 38

Centre UVA/CISCO Sise à l'ENI
410, Av Vollenhoven - BP 242, Bamako Mali
E-mail : info@isoc.ml
www.isoc.ml
@isocml | #ISOCML
www.facebook.com/isocml

Mentor: Abdrahamane S Sidibé

Rédacteurs: Bekaye CISSE
Mahamadou TOUNGARA

Novembre 2023

Plus que jamais, la numérisation s'accélère dans tous les secteurs d'activités. Celle-ci se traduit par une dématérialisation massive des systèmes d'information vers le cloud, l'explosion de l'internet des objets, l'accumulation des données provenant des utilisateurs dans le big data. Les cyberattaques liées à la transformation digitale se multiplient chaque jour. Toutefois, la croissance continue de la menace, l'importance sans cesse accrue des systèmes d'information dans la vie de nos sociétés et l'évolution très rapide des technologies impose de passer à une autre étape pour conserver des capacités de protection et de défenses adaptées à ces évolutions. Elles nous imposent aujourd'hui de faire très attention et d'augmenter de manière très substantielle le niveau sécurité et les moyens de défenses de nos informations confidentielles.

Le principal risque induit par la transformation numérique est la professionnalisation de la cybercriminalité. La sécurité dans le numérique est nécessaire d'où la naissance d'un nouveau concept : la cybersécurité.

L'objet de la cybersécurité est de maîtriser les risques liés à l'usage du numérique et du cyberespace. Cela concerne toutes les infrastructures, tous les systèmes d'information, services et données ainsi que tous les acteurs qui dépendent du numérique.

Pourquoi la cybersécurité ?

D'après une statistique en 2021, les cybercrimes ont couté au monde 6000 milliard de dollars américains. Posons-nous la question suivante : Quel serait la perte envisageable d'ici 2030 ?

Le cybercrime est un sérieux problème de nos jours et pour éviter il est important de pratiquer les différentes techniques de la cybersécurité.

Les individus, les gouvernements, les entreprises etc… sont devenus des cibles des cyberattaques et des violations de données. Le nombre d'attaque s'accroitra avec l'évolution des technologies numériques, l'augmentation du nombre d'appareils et d'utilisateurs dans le numérique. Pour minimiser le risque d'une attaque et sécuriser nos informations confidentielles la cybersécurité doit être la préoccupation pour tous les usagers du numérique.

I. Les enjeux de la cybersécurité

Les enjeux de la cybersécurité peuvent être vus sur plusieurs aspects :

- Du point de vue de la souveraineté, le manque évident des frontières dans le cyberespace rend les Etats de plus en plus vulnérables face à l'apparition des nouvelles menaces informatiques. De ce point de vue, la cybersécurité est appelée à jouer un rôle essentiel dans la protection des ressources stratégiques de la nation y compris d'attaque menées par les acteurs gouvernementaux.

- Au niveau économique, les enjeux de la cybersécurité sont fondamentaux car les attaques deviennent massives. Les conséquences de ces attaques peuvent être critiques au niveau financier comme par exemple l'attaque du réseau interbancaire SWIFT entre Avril et Mai 2016, ayant conduit à des détournements frauduleux de plusieurs dizaines de millions de dollars ou encore l'attaque de type DDoS du 21 Octobre 2016 contre les serveurs Dyn et ayant paralysé pendant plusieurs heures une partie du réseau internet aux Etats Unis.

- Du point de vue industriel, la cybersécurité constitue un enjeu majeur à la fois en matière de protection des entreprises.

- Du point de vue sociétal, son enjeu est de trouver un compromis entre la protection de la vie privée de tout un chacun et la nécessité de vivre dans des sociétés sûres.

II. Définitions

La cybersécurité est l'ensemble des moyens mis en place pour assurer la protection et l'intégrité des données sensibles ou non au sein d'une infrastructure numérique tel que les smartphones, les ordinateurs, les serveurs contre les dangers du web. Ces dangers peuvent volontairement commis par les cybercriminels. Elle vise à protéger les données et leur intégrité des ressources contre tous les pirates.

Les victimes des cyberattaques sont diverses. Ils peuvent être des usagers simples, des entreprises tel que Sonny en 2014 et Yahoo en 2016, des domaines de recherche comme le cas de la NASA en 2011, des domaines militaires tel que l'OTAN en 2011 ou le département de la défense américaine en 2017, des gouvernements comme le gouvernement Israélien en 2009 et le ministère des affaires étrangères Saoudien en 2013, des banques, les centrales électriques bref tous ce qui est numérique.

La cyberattaque :

Une cyberattaque est un acte malveillant envers un dispositif numérique et commis par des individus mal intentionné appelé des hackers. C'est une action volontaire, offensive ou malveillante, mené au travers du cyberespace et destinée à provoquer un dommage aux informations et aux systèmes qui les traitent, pouvant ainsi nuire aux activités dont ils sont le support

D'après le « livre-blanc-cybersecurity » : En France, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) note dans sont rapport d'activité 2015 la forte croissance de la cybercriminalité : 4000 signalements d'attaques ont été reçus en 2015, soit 50% de plus qu'en 2014. La répartition des attaques selon les modes utilisés est illustrée sur la figure ci-dessous. A noter que plus de 60% des attaques visent la défiguration de site internet et plus de 10% de la compromission des systèmes informations.

Une cyberattaque permet bien souvent à son auteur de garder l'anonymat, et de masquer ses intentions.

La cyberguerre :

La cyberguerre consiste pour un pays à s'introduire de manière illégale dans le système informatique d'un autre pays.

En 2008, un cheval de Troie qui a pu être diffuser par l'ordinateur infecté d'un soldat américain basé au moyen orient a permis la fuite d'informations confidentielles sur des programmes d'armements et des informations des ministères de l'Economie et du Commerce extérieur américain.

Bien que l'application de la notion de guerre préventive rapportée à la sphère virtuelle puisse ouvrir des nouvelles perspectives, une cyberattaque n'est pas l'intention première d'une nation puissante. Elle est d'avantage utilisable pour le faible, comme moyen de contourner cette puissance à peu de frais. Les pays moins technologiques offrent peu de prise aux actions de cyberguerre. Une attaque contre ces nations n'offrirait pas assez effets et ne présenterait d'intérêt que dans le cadre d'objectifs ponctuels à forte valeur ajoutée. En revanche, les nations techno-dépendantes offrent une cible de choix ou l'effet domino joue à plein. C'est le cas de l'Estonie en 2007 qui a subi des attaques DDoS (Distributed Denial of Service) qui ont paralysé le pays progressivement, s'attaquant à tous les systèmes économiques, financiers et gouvernementaux les uns après les autres. 58 sites internet ont été piratés dont le site de la principale banque en ligne du pays. La paralysie a durée 3 semaines, la plupart des estoniens se trouvaient dans l'incapacité de retirer de l'argent aux distributeurs automatiques.

Le risque est de ne pas déterminer la provenance d'une cyberattaque et de n'avoir aucun moyen de riposter, faute de savoir qui est l'adversaire. Les états se trouvent potentiellement opposés à des organisations transactionnelles aux contours flous.

Le cyberespace :

Le cyberespace désigne un ensemble de données numérisées constituant un univers d'information et un milieu de communication, lié à l'interconnexion mondiale des ordinateurs. Il est souvent présenté comme un territoire virtuel, un espace à part, sans frontière, qui s'affranchirait des contraintes du monde physique.

La gouvernance du cyberespace fait l'objet de multiples définitions, qui recouvre à la fois la gouvernance de l'internet (son fonctionnement, ses protocoles, son architecture, ses noms de domaines) et une gouvernance sur l'internet (gestion des contenus, infractions, liberté d'expression). Cette gouvernance est complètement décentralisée, elles s'organisent dans de multiples forums ou participent toutes les parties prenantes (la société civile, la communauté technique, le secteur privé et le gouvernement).

Le cyberespace n'est pas un espace de non droit. Bien au contraire, il est soumis à un ensemble de juridictions et de souveraineté nationales. Chaque Etat peut appliquer ses lois sur leur territoire et donc sur les infrastructures physiques, les personnes, les entreprises basées sur leur territoire. Des lois sont prises au niveau national qu'international pour encore une meilleure gestion du cyberespace et contre des cyberattaques.

Multiplicités des acteurs et ensembles des enjeux et risques du cyberespace

Les réseaux qui constituent le cyberespace sont partagés entre une multiplicité d'acteurs, des organisations politiques des hackers, des entreprises, des gouvernements, des terroristes, des militaires etc... Ils sont présents dans tous les aspects de notre quotidien, notre économie et nos sociétés. Des enjeux et des risques sont présents dans tous les domaines. Les cyberattaques sont de plus en plus nombreuses, ciblées et sophistiquées et menacent la sécurité des infrastructures et des citoyens dans le domaine du numérique; les entreprises peuvent voir leurs données volées, divulguées, détruites ou leurs installations sabotées à distance ; les individus sont exposées à l'utilisation de leurs données personnelles et de leur intimité par des personnes mal intentionnées, des gouvernements ou des entreprises ; les policiers et les juges sont faces à des problèmes de chiffrement des communications en lignes par des terroristes et des criminels ; les militaires risques de voir leurs plans d'opération par des actions de sabotage.

III. Les techniques d'attaques

- **Rançongiciels :**
  Le rançongiciel est une technique utilisée par les cybercriminels qui consiste à voler les données sensibles et personnelles d'une personne ou d'une entreprise en leur demandant une rançon.
- **Hameçonnage ou fishing :**
  Le fishing consiste à se faire passer pour quelqu'un en volant son identité. Ce type de menace de cybersécurité implique l'envoi de faux emails provenant de sources apparemment légitimes afin d'obtenir des informations telles que les détails d'une carte de crédit ou des mots de passe.

Les attaques malwares :

- Les malwares peuvent inclure des virus informatiques, des spywares, des chevaux de Troie et tout autre programme ou fichier susceptible d'endommager l'ordinateur. Les malwares sont causés par des téléchargements qui paraissent légitimes ou bien via des pièces jointes dans des emails.
  Il peut arriver que certains fichiers puissent être corrompu par des virus.

- **The Man in the middle:**

  Appelé la technique de l'homme du milieu en français, ce pirate accède aux informations entre un usagers et le serveur du site internet. Dans ce type d'attaque l'hacker récupère l'adresse IP de l'appareil de l'internaute. Il est souvent dû à des réseaux wifi non sécurisé.

  Attaque des mots de passe : Ce type d'attaque est moins utilisé. Dans ce cas le pirate s'attaque au mot de passe en essayant plusieurs combinaisons.

- **Les attaques DDoS**

  Une attaque DDoS ou par déni de service distribué se produit lorsque des cybercriminels saturent un réseau ou ses serveurs en envoyant beaucoup trop de trafic ou de requêtes. Une telle attaque empêche le réseau de traiter les demandes valides et rend l'ensemble du système inutilisable. Cette dernière peut complètement mettre les entreprises à l'arrêt.

- **Les injections SQL**

  SQL signifie Structured Query Language. Une injection SQL vise à réaliser des actions sur les données d'une base de données et potentiellement à les récupérer. Il s'agit d'insérer du code malveillant via des instructions SQL, en tirant parti des vulnérabilités des applications basées sur les données. En opérant ainsi le pirate peut modifier la base de données et même la supprimée.

- **Social Engineering**

  Ce type d'attaque incite les utilisateurs à enfreindre les procédures de sécurité en utilisant des interactions humaines. Les cybercriminels combinent généralement des attaques d'ingénierie sociale avec d'autres, telles que le phishing, pour augmenter les chances de voir la victime cliquer sur un lien ou télécharger un fichier.

IV. Les solutions préventives

L'utilisation des mots de passe sécurisés permet une protection un peu sûre contre des attaques. Les mots de passes simples sont très vulnérables et sont faciles à pirater.

- **Installation des Pare-feu**

  Dans le cas d'une entreprise, installer un Pare-feu qui permet de filtrer toutes les informations venant du serveur vers l'appareil afin de garantir la sécurité des données entrantes ou utiliser des antivirus sophistiqués permettant de détruire les fichiers corrompus.

- **The Honey Pot :**

  En français Pot de miel ; il consiste à attirer des ressources dangereuses afin de les identifier et de les neutraliser.

La Coopération

Face aux multiples enjeux, la coopération entre les secteurs publics et privés, aussi avec la société civile est essentielle pour faire face aux risques et aux menaces liés à l'usage du numérique. Les entreprises, les gouvernements tout comme les institutions doivent élaborer des stratégies pour se protéger des risques mais aussi tirer parti des opportunités par le cyberespace.

Le Chiffrement et confidentialité dans les entreprises

Le cryptage et la confidentialité des données est un fondement clé de la cybersécurité. L'information étant le capital crucial qu'il s'agisse d'information client/administré, industrielles ou encore financière ; leur confidentialité est par conséquent critique pour la pérennité des organisations. Il est indispensable de garantir qu'une information volée ou perdue demeurent inintelligible pour toutes personnes qui ne doit pas y avoir accès. Il faut donc augmenter le niveau de cryptage sur tous les terminaux et sur tous les moyens de communication de communication entre ces terminaux.

La sensibilisation à la sécurité

La sensibilisation de la population sur les dangers liés au numérique permet de réduire le taux de victimes de la cyberattaque. Il y'a des utilisateurs, qui par leurs erreurs ou parce ce qu'ils sont vulnérables aux tentatives d'ingénierie sociale, sont souvent une cible de choix pour les attaquants. Aujourd'hui, la majorité des attaques réussies commencent par un courriel envoyé à quelqu'un qu'on essaie de convaincre de cliquer sur un lien, ou d'ouvrir une pièce jointe. Il faut donc toujours sensibiliser les utilisateurs du numérique au respect d'une certaine hygiène de la sécurité de leurs données. S'il y a un message universel à retenir en matière de sensibilisation des utilisateurs ce serait : « Réfléchissez avant de cliquer ».

Il faut participer ou assister à des forums de protection des données à caractère personnels.

V. Les métiers en cybersécurité

- **Hacker éthique :** Un hacker éthique a pour mission d'identifier et d'explorer les failles du système
- **Architecte Sécurité :** Il pour mission de concevoir les infrastructures de sécurité très robuste.
- **Responsable de la sécurité de l'information RSI :** Sa mission est d'évaluer la vulnérabilité du système d'information de l'entreprise. Il définit et met en œuvre la politique de sécurité de l'entreprise.