INTRODUCTION À LA CYBERSÉCURITÉ : Vision Globale

Préambule

Ce document a été réalisé par un.e autodidacte passionné.e de cybersécurité Le but de ce projet personnel est le partage de connaissance gratuite et vulgarisée. Ce document n'a aucune prétention universitaire ou professionnelle derrière, ainsi il ne se veut pas exhaustif et parfait mais reflète une démarche d'exploration.

L'auteur.e est friand.e de rectifications/critiques en cas d'erreur. C'est pourquoi vous pouvez le.a retrouver sur GitHub : https://github.com/Zig-Zagouille/la-connaissance-c-est-pas-payant.

Introduction

La cybersécurité est une pratique, bien plus qu'un simple domaine, qui requiert une compréhension du comportement matériel de nos appareils de vie (voire étatique, exemple des complexes nucléaires). On peut parler de science qui ne fait qu'évoluer en même temps que les avancées technologiques et leur nouvelles vulnérabilités. Nous nous devons de protéger nos systèmes contre les attaques malveillantes mais aussi de riposter contre des dispositifs réduisant nos libertés (exemple de la surveillance de masse : n'est-ce pas légitime de s'en attaquer ?). Il en vient alors de comprendre ce qu'est l'éthique, oscillant entre légalité et légitimité.

Pour comprendre comment se protéger, il est primordial de se concentrer sur le comment attaquer; cette brève introduction dans la partie 1 à la cybersécurité a pour vocation de présenter rapidement ce qu'englobe la cybersécurité.

Partie 1 : Cybersécurité et Menaces

1. *C'est quoi la cybersécurité ?*

La cybersécurité, comme dit précédemment, ne se restreint pas uniquement à un domaine scientifique mais carrément à un ensemble de pratique, de prouesse technologique afin de se protéger, mener des tests d'intrusions éthiques (appelé audit de sécurité), s'attaquer à des agents réducteurs de nos libertés et comprendre les processus qui régissent les dispositifs matériels, les applications et leur bases de données, les réseaux, etc. La cybersécurité permet de garantir la protection matérielle et immatérielle de nos systèmes informatiques.

L'évolution technologique de nos systèmes informatiques évoluent à la même échelle que la mondialisation : tout est ou devient interconnecté, partagé dont nos données personnelles qui transitent d'entreprises en entreprises, de gouvernements en gouvernements ou encore de hackeurs non éthiques (parfois hacktivistes) à des particuliers. La cybersécurité devient donc une priorité de toustes pour se protéger des cyberattaques. Suivant, quelques exemple d'axe principal de cybersécurité :

1.1. Protection des Infrastructures Réseau

Une infrastructure réseau, il faut voir ça comme étant des gros piliers de fondation de nos systèmes informatiques, si elle ne sont pas solides, alors le système est vulnérable aux attaques. Le principe même de nos réseaux est la communication entre les différents dispositifs le composant. Par exemple, il faut bien gérer la transmission d'un mail d'une machine vers une autre, on passe notamment par ce qu'on appelle des protocoles (par exemple SMTP ou encore HTTP). Les infrastructures, en tant que support, permettent aux développeurs de déployer des applications, des bases de données ou tout autre services.

Sans ces infrastructures, tout s'effondre, c'est pourquoi nous devons contrôler les accès physiques et à distances (par exemple par de la cryptographie solide, limiter les accès selon l'utilisateur ou la portée (localité)), garantir le maintien du service (pouvoir y accéder à n'importe quel moment même en cas de surcharge), se protéger des intrusions externes et internes (par exemple par des systèmes détecteurs de comportements anormaux, des pare-feu).

1.2. Identité et Gestion des Accès

Vous n'aimeriez pas qu'on puisse accéder à vos photos privées sur un drive, n'est-ce pas ? Pour cela nous devons établir des règles d'accès par identité pour que seul un utilisateur ait la clé de sa chambre ! On parlera de IAM (Identity and Access Management). Il y a de multiples façons de gérer cela selon l'infrastructure existante, parmi des exemples :

-L'authentification multifactorielle (MFA) permettant de vérifier l'identité de l'utilisateur qui comprend un tas de possibilités allant de l'empreinte digitale à la validation sur un appareil référent. Imaginez être un attaquant voulant hacker un compte Google utilisant la MFA et qu'il voit : „veuillez valider la notification envoyée sur {X} appareil", ça complique déjà l'attaque !

-La surveillance des réseaux par les administrateurs réseaux. Cela peut se matérialiser par l'enregistrement d'un historique des connexions et des anomalies afin d'en faire un audit et repérer d'éventuels perturbateurs.

-Gestion de permissions par rôle ou fonction de l'utilisateur. Un modérateur n'a pas le même accès qu'un administrateur ou encore un simple utilisateur ou un nouvel utilisateur.

-Surveillance régulière de l'activité des rôles et répartition sur plusieurs personnes de confiance afin de limiter les risques interne de sécurité.

1.3. Détection, Prévention et Gestion des problèmes de sécurité

La détection et la gestion des incidents de sécurité impliquent des mécanismes et des processus permettant d'identifier, d'analyser et de répondre rapidement aux cyberattaques. Ces processus sont impératifs pour limiter les dommages potentiels d'une violation de sécurité.

Analyse du trafic réseau pour repérer des anomalies suspectes ou des traces d'attaques connues (par exemple si on observe dans le trafic des centaines de désauthentification en boucle, il pourrait s'agir de DoS ou DDoS). On peut automatiser une alerte en cas de reconnaissance d'une attaque ou en cas d'action inhabituelle.

Blocage automatiques des attaques en cours si elles sont détectées. Nous avons <Prévenir> et <Guérir>, et ici nous nous trouvons soit entre les deux si l'attaque a commencé à faire des dégâts physiques ou logiques ou soit sur prévenir si l'attaque a été détectée avant qu'elle ne puisse influer. On cherche à minimiser les risques et les dégâts potentiels.

Avoir préparé un plan de réponse aux attaques. On parle de se préparer aux attaques, de réfléchir à quelles attaques pourraient êtres utilisées contre le système (inutile de

sous-estimer, aucun système n'est infaillible comme aucun matériel n'est incassable !) mais on parle aussi de comment on y réagit si jamais les attaques réussissent à s'initialiser dans le système. Et puis en plus de parler de l'avant et du pendant, on parle aussi de l'après, c'est-à-dire comment on fait en sorte que les services du système redeviennent disponible et opérationnel sous un bref délai après l'éradication d'une attaque.

1.4. Cryptographie et Protection des Données Sensibles

Il serait déplacé de parler de Cybersécurité sans parler sans citer la cryptographie comme faisant partie de ses piliers fondateurs. Dans tout système informatique, il en convient qu'il y ait la nécessité de protéger des données sensibles et leur authenticité, même en cas d'intrusion malveillante, en rendant illisible le contenu sans avoir la clé de leur lecture explicite. C'est alors qu'un attaquant pourra récolter des données mais pas les déchiffrer, par exemple les donnait peuvent passer par des ondes à une certaines fréquences que tout le monde peut capter donc il est primordial de ne pas laisser en clair les informations (comme par exemple le faisait HTTP). Les mathématiques permettent constamment d'améliorer les techniques de cryptographie en élaborant des algorithmes toujours plus complexes les uns des autres

1.4.1. Chiffrement

Le chiffrement repose sur le fait de rendre l'information sous un format illisible par la majorité des cas une clé de chiffrement, rendant la lecture claire possible à toute les personne possédant cette clé de chiffrement.

Données en transit : Des données peuvent être échangées entre différents dispositifs, donc elles doivent effectuer un trajet et sont susceptibles d'être interceptées et traitées de manière malveillante. C'est le cas par exemple des informations bancaires ou tout autre mot de passe d'un dispositif à distance. Par exemple, des protocoles peuvent être employés pour chiffrer les données en transit. Un bon exemple est le protocol SSL/TLS qui permet de chiffrer des données en transit entre site web (donc lu sur navigateur de la machine du client) et le serveur distant du site web.

Données internes : L'enjeu par exemple des disques durs, des bases de données est d'être protégé contre le piratage. C'est pourquoi des algorithmes d'encryption sont utilisés. Par exemple il est possible de chiffrer l'accès au données internes de son téléphones (dans les paramètres pour les appareil prenant en charge), cela évite qu'en cas de prise physique du

téléphone qu'un attaquant comme un voleur ou un policier puisse accéder au données en clair, il n'y verra que du charabia, bien que technique de craquage sont possibles.

1.4.2. Authentification

La cryptographie s'intéresse à chiffrer les données mais aussi à vérifier si les personnes qui veulent y accéder sont légitimes. C'est pourquoi il existe des certificats numériques ou signature électronique par exemple utilisés par des réseau WIFI d'entreprise/universitaire (encrypté en WPA-E). Cela permet de vérifier que le demandeur d'accès a bien le droit d'accéder aux données.

Imaginons qu'un attaquant ait été reconnu légitime d'accès, il y a maintenant un autre paramètre de sécurité qui rentre en jeu : le hachage. Le hachage permet de vérifier que les données n'ont pas été falsifiées, modifiées (que ce soit volontaire ou non !). Le hachage a une forme unique et constante qui fait que si les données sont modifiées alors le hachage le sera aussi. Aucun système n'est infaillible, il est donc aussi possible de connaître de manière malveillante le hachage grâce à certaines techniques de crack. Exemple d'algorithme de Hachage populaire : SHA-256 ou encore MD5. Par exemple : <exemple de md5> pourrait donner fa51c1b799fa97a247e3f838f9c45bb4, bon courage pour le cracker !

1.4.3. Données Sensibles

Notamment en Europe majoritairement, il existe des réglementations, des obligations en termes de chiffrement des données personnelles. Les entreprises doivent respecter les lois en vigueur de chaque localité où elles sont présentes. C'est par exemple pour cela que pour un réseau social comme Instagram, les exigences en termes de données personnelles ne sont pas les mêmes en Europe ou au Etat-Unis, l'entreprise doit respecter sous peine de sanction voir de censure de la part d'une localité (par exemple l'Union Européenne). Personne ne veut que son adresse, ses mot de passe de compte bancaire, ou encore ses informations de santé soient rendues publiques ! C'est pourquoi il devrait être normal de lire les conditions de confidentialité de chaque service utilisé et de vérifier s'il respecte les normes en vigueur dans notre propre localité. Exemple de la tokenisation : la tokenization est un procédé qui permet de changer le code à 16 chiffres d'une carte bancaire par un token (jeton) associé uniquement à notre appareil. Par exemple les <cookies> de sites peuvent fonctionner comme ça, permettant de reconnaître une connexion comme n'étant pas la première et donc de personnaliser l'expérience selon l'appareil connecté et les donnés prises en compte (comme quoi il est important de 1) personnaliser son utilisation des cookies ou encore 2) de supprimer régulièrement des cookies pour chaque site souvent visité).

Voir article 9 du Code civil, RGPD (Règlement Général sur la Protection des Données en europe), la HIPAA en amérique (sur les informations médicales), le Règlement sur la Protection de la Vie Privée et les Communications Électroniques (PECR en angleterre) ou encore la Convention Européenne des Droit de l'Homme.

1.4.4. Gérer les clés de chiffrement de son système, chiffrement de bout-en-bout

La cryptographie repose sur des algorithmes mathématiques et donc n'est pas infaillible, c'est pourquoi cela demande une gestion accrue de son utilisation, notamment concernant les clés de chiffrement à un service spécifique d'un système. C'est pourquoi les clés de chiffrement ne doivent pas être exposées afin de ne pas être utilisées par des attaquants, leur rendant possible l'accès en lecture ou totale du système, leur accès doit aussi être limité (par exemple aux administrateurs réseau). Il peut être possible de changer régulièrement les clés de chiffrement par exemple en créant un système en utilisant plusieurs clés stockées (pas au même endroit) et en les utilisant périodiquement de manière automatique.

Le chiffrement asymétrique est possible, le principe est l'utilisation de deux clés : d'une clé privée (connue par une partie restreinte de personne) permettant l'accès au fondement du système et d'une clé publique. On peut aussi stocker la clés sur une machine physique choisi spécifiquement pour cette utilisation ou bien l'utilisation d'un logiciel de cloud de chiffrement (comme CloudHSM ou encore Azure).

Certaines applications de messagerie utilisent le chiffrement de bout-en-bout et ne sont pas à négliger. Le plus grand exemple est Signal, notamment utilisé par les communautés militantes. Des solution comme WhatsApp sont mauvaises car ne garantissent pas à tout prix le respect des données personnelles: exemple, l'Etat leur demande un partage des données personnelles (dans le contexte d'une enquête) il le feront, ce qui est problématique notamment dans un État répressif et un régime autoritaire. Des application SMS comme Silence permettra également le chiffrement de bout-en-bout entre deux utilisateurs ayant l'application, ne permettant plus à l'opérateur téléphonique d'avoir le content des appelles et SMS en clair (car désormais c'est le cas et très facile d'usurper une identité pour récupérer les données d'une victimes choisie, par un unique coup de téléphone à l'opérateur). Les utilisateurs doivent juste se partager initialement une clé de chiffrement puis les messages seront chiffrés avant d'être envoyés, le seront en transit puis déchiffrer en interne par le destinataire.

En tant qu'utilisateur il faut donc bien se renseigner selon l'utilisation qu'on veut porter à un système et le chiffrement n'est pas négligeable bien qu'il puisse ralentir l'utilisation en cas de données volumineuse à chiffrer.

1.5 Types d'Attaques les plus Populaires

Il existe de multiples manières de porter atteinte à un système. Ici dans cette partie, nous ne verrons qu'une vision brève des plus populaires. Les attaques peuvent détruire physiquement les appareils d'une entreprise cible, peuvent mettre à mal l'économie d'un pays, exposer la vie privée des cibles, etc. Il est important de rappeler qu'on parlera souvent de cible plutôt que de victime, les attaques malveillantes bien qu'illégale peuvent s'avérer légitime pour le bien commun : Qui n'a par exemple pas l'envie de déjouer un attentat d'extrême droite ? Qui n'a pas par exemple déjà pensé que ralentir des réseaux sociaux tel que X (twitter) qui ne respecte pas votre vie privée et influence les population par les algorithmes n'était pas une bonne idée ?

Les attaques peuvent être aussi légitimes et légales dans le cas de test d'intrusion dans un audit de sécurité pour sa propre entreprise afin de mettre en lumière ce qui est vulnérable et donc ce qu'il faut sécuriser.

1.5.1 Attaques par déni de service (DoS)

L'objectif principal d'une attaque par déni de service (DoS) est de bloquer l'accès à un service, le ralentir ou le rendre totalement indisponible. Ce procédé passe par la saturation volontaire du service en question.

L'attaque par déni de service (DoS) peut concerner beaucoup de systèmes allant du serveur WEB au réseau interne passant par un réseau WIFI. Le but est d'inonder le services avec un trafic excessif non-habituel, cela passe notamment par un envoi massif de requêtes afin que le système ne soit plus en mesure de les traiter et qu'il provoque des erreurs, un ralentissement ou une panne totale.

Par exemple, pour un site web selon la capacité proposé par son hébergeur, peut très facilement tomber inaccessible suite à une telle attaque. Ça peut aussi être le cas des services de messagerie ou encore les réseaux sociaux qui sont censés accueillir un certain nombre de clients (par exemple Twitter ou Meta ont déjà connu de telles attaques). Par exemple le concurrent de X (twitter) Bluesky a connu ces derniers jours, suite à la nomination d'Elon Musk dans la sphère Étatique Trumpiste, un gros ralentissement et des erreurs suite à son succès et donc une capacité qui n'était pas prévu pour environ 10 millions d'utilisateurs ! Une attaque peut faire varier la réputation d'un service aux yeux de la clientèle, faire baisser le courant des actions et donc faire chuter financièrement une entreprise.

Ces pratiques peuvent aussi être utilisées à raison politique et sociale par des hacktivistes afin de protester et ruiner un service qui se veut contraire à nos libertés et aux droits de l'Homme. Cela peut aussi être utilisé pour masquer une autre attaque simultanée : une attaque DoS est très visible et donc peut cacher l'analyse d'une autre attaque réalisée sur le même service. Un service qui provoque des erreurs en raison de la surcharge de sa capacité de traitement n'est plus en mesure d'être totalement sécurisé à d'autres attaques.

Cela peut s'appliquer à des appareillages cibles en surchargeant la mémoire, les capacité de traitement et surchauffer et endommager des composants à distance.

Un exemple contre un serveur est l'attaque par SYN Flood. Normalement, pour qu'un client se connecte à un serveur, il envoie une requête SYN, le serveur lui envoie sa réponse ACK-SYN et le client renvoie une réponse ACK. Dans le cas d'une attaque DoS, on ne peut très bien ne pas envoyer la réponse ACK et refaire la procédure des centaines de fois, surchargeant les délais de traitement des réponses du serveur ciblé. Ça s'attaque au protocole TCP qui permet la communication d'échange de messages sur un réseau entre les appareils ou le client et le serveur.

On peut également cibler d'autres protocoles comme HTTP pour créer des erreurs de traitement et donc injecter du code malveillant ou bien des requêtes erronées qui vont faire plomber le système, voir les attaques Buffer Overflow (Dépassement de Tampon) qui visent à écrire sur plus que sur l'espace alloué et donc de réécrire par dessus, et dans ce cas c'est un plantage systématique du système.

Attaque DDoS : Les attaques par DDoS sont une variante de l'attaque par DoS, elle vise l'utilisation de machines infectées (BotNet) qui serviront à envoyer les requêtes contrairement au DoS qui n'utilise qu'une seule machine. Les machines sont préalablement infectées par différents procédés, le cas des virus notamment. Le DDoS est très pratiqué actuellement, car il donne de véritables résultats, des millions de machines (de tout type allant du pc à l'imprimante connectée passant par la caméra connectée !) infectées peuvent être infectées, peut-être que votre machine l'est ! Très dure à contrer étant données que les machines proviennent de plein de localité différentes dans la majorité des cas lorsqu'elles ont été infectées à distance de manière non ciblée géographiquement.

Dans le cas des attaques DoS, un pare-feu peut filtrer les adresses IP qui provoquent une surcharge du trafic. Dans le cas des attaques DDoS, les services peuvent faire appel à des entreprises dédiées à ça pour faire rediriger le trafic directement sur leur propre serveur, les serveurs de l'entreprise dédiée

vont alors traiter de leur côté les machines attaquantes. Cela permet de libérer le service initialement ciblé. Des systèmes peuvent aussi utiliser des infrastructures en couche de serveurs. Puis une surveillance des attaques est possible, notamment avec Wireshark.

1.5.2 Attaques Injection

Il est possible d'injecter du code malveillant dans les sites ou applications vulnérables, c'est une attaque très couramment utilisée !

On parle notamment de l'injection SQL. Un attaquant peut injecter du code SQL dans une entrée utilisateur. Le langage SQL est utilisé pour communiquer avec des bases de données.

Un exemple : Imaginons qu'il y ait un formulaire de connexion, initialement on aurait :

SELECT * FROM users WHERE user = 'input_user' AND password = 'input_password';

et on connait le nom d'un utilisateur comme admin par exemple et qu'on injecte: admin' OR '1'='1 (on ne ferme pas les guillemet, on obtient :

SELECT * FROM users WHERE user = 'admin' OR '1'='1' AND password = 'input_password';

On a 1 =1 ET password qui donne False car on a pas le bon password et user = 'admin' est True donc True Or False donne toujours True donc l'accès est un succès. On peut souvent jouer avec les caractères suivant : ' " # ;)

Test : https://zig-zagouille.github.io/la-connaissance-c-est-pas-payant/SQL_injection_Simu.html (SQL classiques)

Ces attaques peuvent permettre de s'introduire, d'obtenir la base de données complète, de modifier, etc. Donc cette attaque peut être très dangereuse et causer de nombreux dégâts.

Les injections XSS (Cross-Site-Scripting) sont aussi très répandues contre des sites vulnérables à ce type d'injection. Ici on va pouvoir jouer avec du code javascript en les injectant dans des entrées utilisateurs comme des formulaires. Le nouveau code javascript malveillant sera alors exécuté par tous les utilisateurs visitant le site. Un exemple courant est de rediriger les utilisateurs vers un site comme une page de phishing où ils rentreront leur identifiant.

Test : https://zig-zagouille.github.io/la-connaissance-c-est-pas-payant/XSSinjectsimu.html

Il reste possible de contrer ces attaques en analysant les entrées utilisateur et donc ne pas traiter des entrées qui sont détectées comme étant du code malveillant.

1.5.3 Phishing

Le but du phishing est un des procédés de l'ingénierie sociale (social engineering) qui a pour but de manipuler psychologiquement la personne en lui faisant croire qu'elle se trouve sur une page de confiance et qu'elle peut entrer ses informations sensibles telles que des mots de passe. Par exemple, pour obtenir des login-password Instagram, on peut recréer la page officielle de connexion d'Instagram. Le phishing peut aussi être utilisé pour diriger la personne vers le téléchargement d'un malware, par exemple : on peut créer une page officielle de téléchargement de Windows et télécharger une version de Windows infectée.

Phishing les plus récurrent quotidiennement :

> -les mails du type mabanque@banqueee.fr au lieu de mabanque@banque.fr, il est alors primordial de vérifier l'adresse du destinataire (certaines messagerie filtre et mettent dans les Spam), les SMS du style <Vous avez reçu un nouveau coli de la poste, veuillez cliquer sur le lien>, ou encore le démarchage téléphonique se faisant passer pour tel ou tel service dans le but d'arnaquer.

Test : https://zig-zagouille.github.io/la-connaissance-c-est-pas-payant/instasimuphishing.html (voir console)

1.5.4 Malware (Logiciels malveillants)

Un malware est un logiciel malveillant souvent prenant la forme d'un logiciel normal ou n'étant pas directement visible. Parmi les plus connus :

> **Virus** : a pour but de se démultiplier dans le système (souvent les fichiers) et d'endommager l'appareil, il est toujours lié à un programme exécutable du système. Exemple : démultiplier à l'infini des dossiers dans des dossiers.
>
> **Vers** : a pour but de se démultiplier sur plusieurs ordinateurs en utilisant un réseau spécifique ou parfois carrément internet. Contrairement au virus, il n'a pas besoin d'être rattaché à un programme exécutable.

Cheval de Troie : logiciel qui a une forme normale mais qui utilise en fait des fonctionnalités non consenties, par exemple l'envoi des informations ou le contrôle à distance.

Ransomware : vient bloquer un système en le chiffrant et demande une rançon pour le débloquer.

Spyware : logiciel de surveillance, par exemple qui va récupérer des mot de passe, informations bancaires entrées par l'utilisateur.

Adware : sont là pour afficher des publicités et pop-ups incessantes à l'utilisateur.

Scareware : par exemple une page qui va vous alarmer d'une menace (souvent un virus) et vous demande de vous diriger vers un service de protection (et de télécharger des malware), une vraie bombe de Social Engineering !

-etc...

Les antivirus et les mises à jour peuvent permettre de les détecter, malgré le fait que parfois ils viennent justement des antivirus téléchargés ou de mises à jour de sécurité !

1.5.5 Attaques axées sur les protocoles

On s'intéresse donc à la vulnérabilité des protocoles de communication pour intercepter et manipuler des données en transit. Quelques attaques répandus :

DNS Spoofing : on peut rediriger le trafic des utilisateurs vers des sites malveillants, souvent de phishing.

Man-in-the-Middle (MITM) : C'est le fait d'intercepter des communications entre deux entités (serveur-client ou machine-machine par exemple) pour les lire, les modifier ou injecter des données malveillantes. Pour contrer ça, les réseaux peuvent utiliser des certificats, des signatures (qui ne sont d'ailleurs pas infaillibles !).

Jouer avec le décryptage SSL/TLS : exemple récurrent quand on n'utilise pas HTTPS, c'est l'utilisation de HTTP où l'on peut intercepter les données en clair.

1.6 Qui attaque ?

Les cyberattaques ne proviennent pas seulement de sources inconnues ou anonymes, mais aussi d'acteurs organisés avec des objectifs bien définis. Comprendre qui sont ces acteurs permet de mieux cibler les stratégies de défense.

1.6.1 Entreprise et Audit de Sécurité

Oui ! Une entreprise peut décider se s'attaquer elle-même dans le cadre d'un audit de sécurité en pratiquant du Pentest (du test d'intrusion) afin de tester les réponses du système aux attaques et donc adapter la sécurité en fonction. Ces attaques sont contrôlées donc ne visent pas à détruire le système involontairement mais le tester. Elles sont donc légales, éthiques, encadrées. Le métier qui en découle est Hacker Éthique, il peut être indépendant ou être salarié d'une entreprise.

1.6.2 Cybercriminels, Hacktivistes, Hacker éthiques

Les cybercriminels volent les données souvent dans le but de les revendre et de se faire de l'argent. Ils peuvent également prendre en otage des données contre une rançon. Parfois il peut s'agir de personne interne à un système, donc qui a déjà des accès à l'infrastructure pour attaquer de l'intérieur.

Les Hacktivistes sont là pour protester, mettre en avant des causes sociales et politiques qu'ils défendent. Par exemple, on peut citer les Anonymous qui pratiquent des attaques contre des États ou des institutions. Des Hacktivistes peuvent également s'attaquer à des données sensibles et être lanceurs d'alerte concernant par exemple des activités plus que discutables d'un haut membre d'une entreprise ou d'un gouvernement. Les attaques, bien que illégales, sont très souvent légitimes.

1.6.3 L'État

Les services de renseignement des État peuvent se servir des attaques discrètes pour espionner, saboter, perturber d'autres pays ou organisations. Ces attaques sont censées être ciblées mais certaines finissent parfois à se propager à l'échelle mondiale, ce qui fait que l'attaque est exposée et donc peut être contrée.