Stéphane **Renouf**

CYBERSÉCURITÉ

LE KIT DE SURVIE

ellipses

PARTIE 1

INTRODUCTION À LA CYBERSÉCURITÉ

Chapitre 1
Le monde numérique et ses enjeux

Regardez autour de vous. Que voyez-vous ? Des écrans lumineux captivant l'attention, des conversations murmurées entrecoupées de notifications sonores, des informations circulant à la vitesse de la lumière. Le numérique n'est plus un simple outil, il est l'air que nous respirons, l'environnement dans lequel nous évoluons. Des smartphones nichés au creux de nos mains aux objets connectés qui peuplent nos maisons, en passant par les réseaux sociaux où nos vies se déploient en temps réel, le numérique a tissé une toile invisible mais omniprésente dans notre société et nos vies.

Communiquer avec nos amis à l'autre bout du monde, s'informer en temps réel des événements qui façonnent notre actualité, commander en quelques clics l'objet de nos désirs, partager nos passions et nos créations, apprendre de nouvelles compétences grâce à des ressources illimitées… Tout cela, et bien plus encore, est devenu possible grâce à un réseau mondial tentaculaire : **Internet**.

Ce réseau, c'est un peu comme un immense système nerveux planétaire, où des milliards d'informations transitent chaque seconde. Des données de toutes sortes (textes, images, vidéos, sons) voyagent à travers des câbles sous-marins (figure 1), des ondes radio, des satellites, reliant des individus, des entreprises, des gouvernements, des objets… Cette interconnexion constante a non seulement simplifié nos vies, mais a aussi profondément remodelé nos interactions sociales, notre économie et nos modes de pensée.

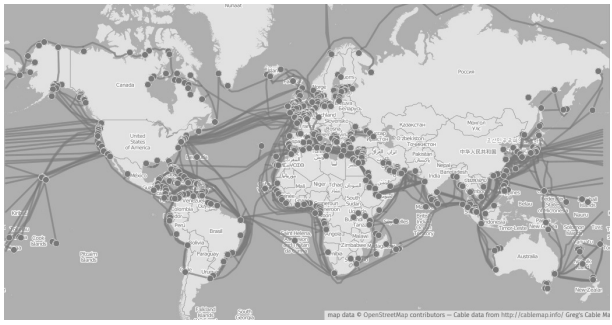

Figure 1 : cable data by Greg Mahlknecht, map by Openstreetmap contributorsOpenStreetMap contributors, CC BY-SA 2.0

L'omniprésence du numérique : une société hyperconnectée

Prenons un instant pour analyser une journée ordinaire. Combien de fois interagissons-nous, consciemment ou non, avec le monde numérique ?

- **Communication** : échanger des messages instantanés avec des amis, participer à des visioconférences, commenter des publications sur les **réseaux sociaux**, envoyer et recevoir des courriels. Ces plateformes sont devenues des lieux de rencontre virtuels où nos interactions sociales se prolongent et se transforment.
- **Information** : consulter des sites d'actualités pour suivre l'évolution du monde, effectuer des recherches approfondies sur le **Web**, visionner des tutoriels explicatifs sur des plateformes vidéo pour acquérir de nouvelles compétences. L'accès à l'information n'a jamais été aussi rapide et potentiellement illimité.
- **Divertissement** : écouter de la musique en streaming, regarder des séries et des films sur des plateformes en ligne, participer à des jeux vidéo multijoueurs avec des passionnés du monde entier. Le divertissement s'est dématérialisé et est accessible à tout moment et de n'importe où.
- **Commerce** : acheter sur des boutiques en ligne, réserver des voyages via des applications spécialisées, effectuer des paiements, gérer nos comptes bancaires avec des smartphones. Le **commerce électronique** a transformé nos habitudes de consommation et les modèles économiques traditionnels.
- **Éducation** : accéder à des plateformes d'apprentissage en ligne, se connecter à un espace numérique de travail, utiliser des outils numériques pour réaliser des devoirs, collaborer avec des camarades sur des documents partagés dans le « cloud ». Le numérique offre de nouvelles perspectives d'apprentissage et de partage de connaissances.
- **Localisation et mobilité** : utiliser des applications de navigation GPS pour nous guider, consulter les horaires des transports en commun en temps réel sur nos téléphones, partager notre position avec nos proches. Le numérique a modifié notre rapport à l'espace et nos déplacements.
- **Données structurées et leur traitement** : derrière chaque interaction numérique se cachent des **données structurées** (des informations organisées et stockées) qui sont traitées pour personnaliser nos expériences, nous proposer des publicités ciblées ou analyser des tendances.

Cette énumération n'est qu'un aperçu de l'étendue de l'influence du numérique. Il est intégré dans nos objets du quotidien (montres connectées, assistants vocaux, thermostats intelligents…), transforme des secteurs entiers (santé, transport, industrie, prévisions météorologiques, agriculture…) et façonne notre perception du monde.

Mise en pratique 1

Votre journée numérique

Prenez quelques minutes pour réfléchir à votre propre journée d'hier.
Listez toutes les interactions que vous avez eues avec le monde numérique.
Quels outils ou plateformes avez-vous utilisés ?
Pour quelles raisons ?

Mise en pratique 2

Cartographie de votre utilisation du numérique

Dessinez une carte mentale représentant les différentes sphères de votre vie quotidienne. Pour chacune d'elles (communication, études, loisirs, etc.), identifiez les outils et les services numériques que vous utilisez.

Données personnelles, vie privée et identité numérique : des concepts fondamentaux

Dans cet univers numérique interconnecté, chaque action, chaque clic laisse une empreinte : des informations qui nous concernent directement ou indirectement. Ces informations sont appelées **données personnelles**.

Voici quelques exemples de données personnelles :

- votre nom, prénom, date de naissance, adresse e-mail, numéro de téléphone, adresse IP ;
- vos photos, vidéos, publications sur les réseaux sociaux, messages privés, centres d'intérêt en ligne en font également partie ;
- vos historiques de navigation sur internet, achats en ligne, données de **localisation** et informations de santé sont aussi des fragments de vos données personnelles.

L'agrégation de ces données, au fil de vos activités en ligne, constitue votre **identité numérique**, une représentation de vous-même dans le monde virtuel. Il est crucial de comprendre que cette identité numérique n'est pas une simple abstraction ; elle peut avoir des conséquences bien réelles sur votre vie, influençant par exemple les publicités que vous voyez, les opportunités qui se présentent à vous, ou même votre réputation en ligne.

Mise en pratique 3

Mesurez votre visibilité numérique

Rendez-vous sur le site webmii.com, saisissez votre prénom et votre nom, puis observez le score qui vous sera attribué.

Ce score mesure votre **visibilité numérique** sur Internet, sur une échelle de 1 à 10. Si votre score est inférieur à 3, cela signifie qu'il y a peu d'informations publiques vous concernant, soit parce que vous êtes peu actif sur Internet, soit parce que vous avez choisi de limiter la diffusion de vos données personnelles. Si votre score est compris entre 4 et 6, vous êtes probablement actif sur certains réseaux sociaux ou mentionné dans quelques articles ou bases de données professionnelles, mais sans grande notoriété. Si votre score est compris entre 7 et 10, vous êtes très visible sur le web et fréquemment cités dans les médias, les blogs ou sur les réseaux sociaux.

Cet outil peut vous servir à surveiller votre empreinte numérique et à ajuster votre présence en ligne selon vos objectifs personnels ou professionnels.

La **vie privée** est le droit fondamental de chaque individu de contrôler la collecte, l'utilisation et la diffusion de ses informations personnelles. Dans le monde numérique, les frontières entre le public et le privé peuvent s'estomper, la protection de notre vie privée devient donc un enjeu majeur. Il est essentiel d'être conscient des informations que nous partageons volontairement ou involontairement et de comprendre comment elles peuvent être utilisées.

Le **règlement général sur la protection des données (RGPD)**, entré en application en mai 2018, est un texte législatif européen qui encadre la collecte et le traitement des données personnelles des citoyens de l'Union Européenne. Il renforce les droits des individus sur leurs données et impose des obligations strictes aux organisations qui les traitent. L'article 17 de ce règlement permet d'exercer le « droit à l'oubli » et de demander à un organisme d'effacer les données personnelles qui le concernent. Comprendre les principes du RGPD est essentiel pour naviguer de manière responsable dans le monde numérique et faire valoir vos droits. Ce règlement s'applique aussi aux organisations situées hors de l'UE dès lors qu'elles proposent des biens ou services à des personnes de l'UE et cela même si le traitement des données s'effectue en dehors de l'UE.

Mise en pratique 4

Où vivent vos données ?

Réfléchissez aux différents services numériques que vous utilisez (réseaux sociaux, plateformes de jeux, etc.). Essayez de déterminer où sont stockées les données que vous générez sur ces plateformes. Sont-elles stockées en France, en Europe, aux États-Unis ou ailleurs ? Quelles sont les implications en termes de protection de vos données si elles sont stockées en dehors de l'espace européen, où le RGPD ne s'applique pas directement ?

Mise en pratique 5

Scénarios RGPD : êtes-vous conforme ?

Imaginez différents scénarios concrets impliquant la collecte et le traitement de données personnelles au sein d'une organisation à l'aide d'une application mobile proposant un service). Pour chaque scénario, identifiez les types de données personnelles collectées, le but de cette collecte, et discutez des obligations que le RGPD imposerait à cette organisation (consentement, information des personnes, sécurité des données, droit d'accès, de rectification, d'effacement, etc.).

Les risques et menaces du monde numérique

Si le numérique offre de nombreuses opportunités, il expose également à des risques et des menaces qu'il est important de connaître pour s'en protéger.

Voici quelques exemples courants :

- **Les logiciels malveillants (malwares)** : ce sont des programmes conçus pour endommager votre ordinateur, voler vos informations personnelles (mots de passe, coordonnées bancaires…), ou prendre le contrôle de vos appareils (ordinateurs, tablettes, smartphones…) à votre insu. Il y en a de différents types :
  - → **Virus** : ils se propagent en s'attachant à d'autres programmes comme Rombertik en 2015 (ce virus est capable de détecter s'il est observé dans un environnement de sécurité, si c'est le cas, il tente de détruire le master boot record du disque dur ou de chiffrer les fichiers personnels, rendant l'ordinateur inutilisable ou les données illisibles).
  - → **Vers** : ils se répliquent et se propagent automatiquement à travers les réseaux. L'exemple le plus marquant est le ver Storm Worm, en 2006, déguisé en un e-mail alarmant annonçant une tempête meurtrière en Europe, il a rapidement infecté des millions d'ordinateurs sous Windows, principalement en Europe et aux États-Unis.
  - → **Chevaux de Troie** : ils se font passer pour des logiciels légitimes pour vous inciter à les installer comme Emotet en 2014 (un malware d'abord conçu pour voler des données bancaires).
  - → **Logiciels espions (spyware)** : ils enregistrent vos activités en ligne sans que vous le sachiez comme Pegasus en 2010 (ce malware, une fois installé, permet aux attaquants d'accéder à l'ensemble des données du téléphone : messages (même chiffrés), emails, photos, contacts, localisation, historiques de navigation, et ils peuvent activer à distance le micro et la caméra).
  - → **Ransomwares** : ils chiffrent vos fichiers et exigent une rançon pour vous en redonner l'accès comme CryptoLocker en 2013.

- **Le phishing (hameçonnage)** : il s'agit d'une technique utilisée par des personnes malveillantes pour vous tromper et vous inciter à leur fournir des informations confidentielles (identifiants, mots de passe, numéros de carte bancaire) en se faisant passer pour une entité de confiance (banque, poste, réseau social, administration…).
- **L'usurpation d'identité** : c'est le fait de se faire passer pour quelqu'un d'autre en utilisant ses informations personnelles (nom, prénom, adresse, etc.) dans le but de commettre des actes frauduleux (achats en ligne, ouverture de comptes bancaires…).
- **Le cyberharcèlement** : il s'agit d'actes d'intimidation, d'insultes, de moqueries ou de menaces répétés envers une personne via les outils numériques (réseaux sociaux, messageries…). Il peut avoir des conséquences psychologiques graves pour la victime.
- **Les fake news et la désinformation** : la diffusion rapide d'informations erronées ou manipulées sur internet peut avoir des conséquences importantes sur l'opinion publique et la société.

Mise en pratique 6

Un brainstorming des risques

Identifiez les différents risques et menaces que vous avez peut-être déjà rencontrés ou dont vous avez entendu parler dans le monde numérique.

Zoom Cyberculture

Le premier virus Creeper de Robert Thomas en 1971

Le programme Creeper, créé en 1971 par Bob Thomas est reconnu comme le premier virus informatique de l'histoire. Conçu à l'origine comme une expérience pédagogique pour démontrer la possibilité de faire circuler un programme d'un ordinateur à l'autre via le réseau ARPANET (précurseur d'Internet), Creeper infectait les ordinateurs centraux et affichait simplement le message « I'M THE CREEPER: CATCH ME IF YOU CAN » sans causer de dommages. Sa première version ne faisait que se déplacer d'une machine à l'autre.

Pourquoi la cybersécurité est-elle essentielle ?

Face à ces risques, la **cybersécurité** est devenue une nécessité. Elle englobe l'ensemble des techniques et pratiques mises en œuvre pour protéger nos systèmes informatiques, nos réseaux, nos données et nos identités numériques. Elle se manifeste donc à différents niveaux :

- **Pour les individus** : protéger ses données personnelles, sa vie privée, son identité numérique, éviter les pertes financières, prévenir le cyberharcèlement, naviguer en confiance sur internet.
- **Pour les organisations (entreprises, administrations, associations)** : protéger leurs informations confidentielles, assurer la continuité de leurs activités, maintenir la confiance de leurs clients et partenaires, se conformer aux réglementations en vigueur.
- **Pour la société dans son ensemble** : assurer le bon fonctionnement des infrastructures critiques (énergie, transport, santé…), lutter contre la criminalité en ligne, préserver la démocratie et la liberté d'expression.

En comprenant les enjeux du monde numérique et les risques qui y sont associés, vous faites le premier pas essentiel vers une navigation plus sûre et plus responsable. La cybersécurité est l'affaire de chacun d'entre nous.

Résumé

- Le numérique est omniprésent dans notre société et offre de nombreuses opportunités.
- Nos activités en ligne génèrent une multitude de données personnelles, celles-ci constituent notre identité numérique.
- Il est crucial de protéger sa vie privée dans le monde numérique.
- De nombreux risques et menaces existent en ligne (malwares, phishing, usurpation d'identité, cyberharcèlement…).
- La cybersécurité est essentielle pour se protéger individuellement, pour les organisations et pour la société dans son ensemble.

Chapitre 2
Les fondamentaux de la sécurité informatique

Il est temps de plonger au cœur des principes fondamentaux qui sous-tendent la sécurité de nos systèmes informatiques et de nos informations. Comprendre ces concepts est essentiel pour appréhender les menaces et les solutions que nous aborderons par la suite.

Imaginez la sécurité informatique comme une maison : pour qu'elle soit solide et résistante aux intrusions, elle doit reposer sur des fondations solides. Ces fondations, ce sont les principes de confidentialité, d'intégrité et de disponibilité.

Les principes de base de la sécurité : le triptyque CIA et la disponibilité

En cybersécurité, on parle souvent du triptyque **CIA** : **Confidentialité**, **Intégrité**, et **Authentification**. Ces trois principes constituent les objectifs fondamentaux de toute politique de sécurité informatique auxquels on peut rajouter la disponibilité.

Confidentialité (le secret bien gardé)

Celle-ci vise à s'assurer que seules les personnes autorisées peuvent accéder à certaines informations. C'est le principe du « secret bien gardé ». Imaginez un message personnel que vous envoyez à un ami : vous ne voudriez pas que n'importe qui puisse le lire. De même, les informations sensibles d'une entreprise (secrets commerciaux, brevets d'entreprises, données financières) doivent rester confidentielles pour éviter la concurrence déloyale et/ou la fraude.

Mise en pratique 7

Le jeu du message secret

Imaginez une méthode simple pour envoyer un message secret à un destinataire sans que quelqu'un d'autre puisse le lire.

Quelles sont les faiblesses potentielles de votre méthode ?

Comment pourriez-vous les renforcer ?

Mise en pratique 8

Qui a accès à quoi ?

Analysez les différents comptes numériques que vous utilisez (messagerie, réseaux sociaux, plateforme de stockage en ligne). Pour chacun, identifiez les informations que vous y stockez et les personnes qui ont potentiellement accès à ces informations (vous-même, vos contacts, l'entreprise fournissant le service).

Quelles mesures pouvez-vous prendre pour limiter l'accès à vos informations les plus sensibles ?

Intégrité (la fiabilité de l'information)

Elle garantit que les informations ne sont pas altérées, modifiées ou détruites de manière non autorisée. Cela signifie que les données doivent rester exactes, complètes et fiables.

Imaginez un document important sur lequel vous travaillez : il est crucial qu'il ne soit pas modifié par erreur ou par une personne malveillante sans que vous en soyez informé. De même, l'intégrité des données scientifiques ou des registres comptables est essentielle pour la prise de décision et la confiance.

Mise en pratique 9

Le message modifié

Rédigez un message sur la dernière série que vous avez visionné en donnant des détails sur les personnages, les lieux et le scénario. Puis adaptez ce message pour le réseau social Twitter/X (280 caractères au maximum), pour Instagram (240 caractères), WhatsApp (1 024 caractères) et Facebook (63 206 caractères).

Comparez les versions : vous verrez comment la nécessité de raccourcir, simplifier ou accrocher l'attention peut altérer l'information, soulignant l'importance d'une communication vigilante et adaptée à chaque plateforme.

Mise en pratique 10

Détection de falsification

Recherchez en ligne des exemples de « deepfakes » (vidéos ou audios manipulés de manière très réaliste).

Comment ces technologies remettent-elles en question l'intégrité de l'information ?

L'authentification

Il s'agit de s'assurer que la personne qui tente d'accéder à des ressources est bien celle qu'elle prétend être. Sans une authentification robuste, la confidentialité et l'intégrité des données seraient facilement compromises, car des acteurs non autorisés pourraient se faire passer pour des utilisateurs légitimes. L'authentification repose sur la présentation de **preuves d'identité**, qui peuvent prendre différentes formes :

- quelque chose que l'on connaît (un mot de passe, un code PIN) ;
- quelque chose que l'on possède (une carte à puce, un jeton de sécurité) ;
- quelque chose que l'on est (une empreinte digitale, une reconnaissance faciale).

Une authentification forte combine souvent plusieurs de ces facteurs (authentification multifacteurs) pour renforcer la sécurité.

Mise en pratique 11

Les trois secrets

Pour chaque type de preuves d'authentification, trouvez au moins deux exemples concrets que vous utilisez dans votre vie numérique quotidienne.

Quels sont les avantages et les inconvénients de chaque méthode en termes de sécurité et de praticité ?

Mise en pratique 12

Scénario d'authentification multifacteurs

Décrivez les différentes étapes du processus d'authentification à votre compte bancaire, si votre banque utilise l'authentification multifacteurs (par exemple, mot de passe plus code envoyé par SMS, ou mot de passe plus empreinte digitale). Expliquez pourquoi cette méthode est plus sécurisée qu'une simple authentification par mot de passe.

Recensez les services en ligne que vous utilisez qui proposent l'authentification multifacteurs.

Disponibilité (l'accès en temps voulu)

La **disponibilité** assure que les utilisateurs autorisés peuvent accéder aux informations et aux systèmes quand ils en ont besoin. Un système sécurisé ne sert à rien s'il est constamment hors service ou inaccessible.

Imaginez un site web d'urgence : il doit être disponible 24 heures sur 24 et 7 jours sur 7 pour que les personnes en danger puissent obtenir de l'aide. De même, la disponibilité des services en ligne est cruciale pour le bon fonctionnement des entreprises et des administrations.

Mise en pratique 13

La panne inattendue

Imaginez que le réseau internet de votre domicile tombe en panne pendant une journée entière.

Quelles seraient les conséquences sur vos activités, vos recherches, vos communications ? Faites une liste des services que vous ne pourriez plus utiliser.

Comment cette situation illustre-t-elle l'importance de la disponibilité des systèmes numériques ?

Mise en pratique 14

L'attaque par déni de service distribué (DDoS)

Recherchez en ligne des informations sur les attaques par déni de service distribué (DDoS).

Comment fonctionnent-elles ? Quels sont leurs objectifs ? Comment ces attaques affectent-elles la disponibilité des services en ligne pour les utilisateurs légitimes ?

Quelles sont, selon vous, les motivations des auteurs de ces attaques et quelles mesures de protection peuvent être mises en place ?

Les différents acteurs malveillants et leurs motivations

Pour naviguer dans ce paysage complexe, il faut comprendre les rôles et les intentions des différents protagonistes. La classification courante dite des « chapeaux » permet de distinguer trois catégories de « hackers » selon leur éthique et leurs intentions. Celle-ci provient des westerns américains, où les héros portaient des chapeaux blancs et les bandits, des chapeaux noirs :

- **Les « chapeaux noirs » (black hats)**, ce sont les acteurs malveillants du cyberespace. Ils exploitent les vulnérabilités des systèmes informatiques et des réseaux de manière illégale et non autorisée. Leurs motivations sont souvent

criminelles, visant le gain financier (vol de données bancaires, rançonnage), le sabotage (destruction de systèmes), l'espionnage illégal, ou simplement le désir de nuire.

Cette catégorie peut être élargie à d'autres acteurs malintentionnés :

- → **Les cybercriminels organisés**, il s'agit de groupes structurés de type mafieux possédant une expertise technique pointue et menant des attaques sophistiquées à grande échelle. Leur objectif principal est le profit financier, à travers le trafic de données volées, la fraude financière élaborée, ou l'extorsion via des ransomwares.
- → **Les « script kiddies »**, il s'agit d'individus, souvent peu expérimentés. Ils utilisent des outils et des scripts d'attaque développés par d'autres en utilisant le darkweb. Leurs motivations peuvent être la curiosité, le désir de se faire valoir, ou une intention de nuisance sans une compréhension approfondie des conséquences de leurs actes. Par exemple, l'attaque contre l'entreprise de télécommunication britannique TalkTalk a été menée par un jeune de 17 ans ayant utilisé des outils accessibles à tous pour divulguer des données personnelles de milliers de clients.
- → **Les initiés malveillants**, en effet, la menace peut également provenir de l'intérieur d'une organisation. Des employés actuels ou passés, ainsi que des partenaires ayant un accès légitime aux systèmes, peuvent abuser de cette confiance pour voler des informations, saboter des opérations, ou se venger.
- → **Les états-nations**, certains gouvernements mènent des cyber-opérations à des fins d'espionnage (collecte d'informations stratégiques), de sabotage (neutralisation d'infrastructures critiques), ou d'influence politique (diffusion de propagande, ingérence électorale). On parle alors de **cyber-espionnage** ou de **cyber-guerre**. Par exemple, depuis 2022, la Russie mène des cyber-attaques contre les infrastructures de télécommunications ukrainiennes, y compris contre le service Starlink fourni par SpaceX, dans le but d'entraver l'accès des Ukrainiens à Internet.
- → **Les « hacktivistes »**, il s'agit de groupes d'individus utilisant le piratage informatique comme un moyen de militantisme pour défendre des causes politiques, sociales ou environnementales, ils ciblent des organisations ou des gouvernements qu'ils jugent responsables. Par exemple, Julian Assange, fondateur de WikiLeaks, qui a publié de nombreux documents confidentiels pour dénoncer la corruption et les abus de pouvoir est considéré comme l'un des premiers hacktiviste.

À l'opposé des « chapeaux noirs », on trouve :

- **Les « chapeaux blancs » (white hats)**, ce sont des experts en sécurité informatique qui utilisent leurs compétences de manière éthique et légale. Ils travaillent pour identifier les vulnérabilités des systèmes et des réseaux afin de les corriger et de renforcer la sécurité. Ils peuvent être employés par des entreprises, des organisations gouvernementales, ou travailler en tant que consultants indépendants. Leur objectif est de protéger les actifs numériques et de prévenir les attaques malveillantes.

Il existe aussi ce que l'on peut qualifier de zone grise :

- **Les « chapeaux gris » (grey hats)**, ces individus se situent entre les « chapeaux noirs » et les « chapeaux blancs ». Ils peuvent parfois opérer sans autorisation pour tester la sécurité des systèmes, mais leurs intentions ne sont pas nécessairement malveillantes. Par exemple, ils peuvent découvrir une vulnérabilité et la révéler publiquement sans en informer au préalable le propriétaire, dans le but d'inciter à une correction rapide. Leur éthique est souvent sujette à débat au sein de la communauté des informaticiens et de la cybersécurité.

Comprendre ce spectre d'acteurs, leurs motivations (gain financier, idéologie, défi technique…), leurs méthodes est fondamental pour développer des stratégies de défense.

Mise en pratique 15

Profils de cybercriminels

Recherchez des exemples concrets d'attaques informatiques médiatisées. Essayez d'identifier le type d'acteur malveillant impliqué et analysez leurs motivations probables.

Mise en pratique 16

Retrouver les bons chapeaux

Accès à des systèmes sans autorisation, mais sans voler de données ni causer de dommages (c'est illégal !)		Chapeaux noirs
Chiffre les fichiers d'une entreprise et demande une rançon		Chapeaux gris
Informe le service informatique d'une université d'une faille de sécurité découverte.		Chapeaux blancs

Zoom Cyberculture

Anonymous

Ce groupe est un collectif mondial d'hacktivistes né autour de 2003 sur le forum anonyme 4chan. Ce terme désignait initialement les utilisateurs postant sans identification. Sans structure hiérarchique ni membres officiels, Anonymous fonctionne de manière décentralisée : chacun peut se revendiquer du mouvement en adhérant à ses idéaux, principalement la défense de la liberté d'expression, la lutte contre la censure, les injustices et la protection des droits humains.

Ce collectif s'est rendu célèbre par ses attaques et ses opérations de sensibilisation contre des institutions gouvernementales, des entreprises ou des organisations accusées de restreindre les libertés ou de commettre des abus. Leur symbole emblématique est le masque de Guy Fawkes, popularisé par le film « V pour Vendetta », qui incarne à la fois l'anonymat et la résistance à l'oppression. Parmi leurs actions marquantes figurent des opérations contre des gouvernements accusés de censure (comme la Turquie en 2012) ou encore le soutien à des mouvements sociaux comme Black Lives Matter. Les Anonymous continuent de marquer l'actualité numérique, oscillant entre image de justiciers du web et celle de cybercriminels selon les points de vue.

Les principales vulnérabilités

Les systèmes informatiques et les réseaux sont loin d'être parfaits, ils peuvent contenir des failles de sécurité, appelées **vulnérabilités**. Celles-ci peuvent être exploitées par des acteurs malveillants pour compromettre la confidentialité, l'intégrité ou la disponibilité des informations.

Les faiblesses logicielles

Ce sont des erreurs de programmation, des oublis de sécurité (des « oublis de verrouillage de porte » dans l'analogie de la forteresse), ou des bogues présents dans le code source des systèmes d'exploitation (comme Windows, macOS, Linux), des applications (logiciels que vous utilisez quotidiennement, navigateurs web, jeux vidéo, etc.) ou des micrologiciels (firmwares, les logiciels embarqués qui contrôlent le matériel, comme le BIOS d'un ordinateur ou le logiciel interne d'un routeur).

Ces faiblesses peuvent avoir des conséquences désastreuses. Un attaquant qui découvre une telle faille peut l'exploiter pour :

- **Exécuter du code malveillant** en injectant et exécutant des commandes sur votre ordinateur ou votre serveur à votre insu. Cela lui permet de prendre le contrôle de votre système. Ainsi, des vulnérabilités dans le code d'un site peuvent permettre des attaques comme **l'injection SQL** ou le **Cross-Site Scripting (XSS)**, compromettant la sécurité des utilisateurs et des données.

- **Accéder à des données non autorisées** en contournant les mécanismes de sécurité pour consulter, modifier ou supprimer des informations auxquelles il ne devrait pas avoir accès (vos fichiers personnels, les données d'autres utilisateurs, des secrets commerciaux). Par exemple, un bug dans un système d'exploitation pourrait permettre à un utilisateur mal intentionné d'obtenir des droits d'administrateur sans authentification appropriée, ce type d'attaque est qualifiée d'**escalade de privilèges**.
- **Provoquer un dysfonctionnement du système** en entraînant des plantages, des blocages ou rendant le système inutilisable (attaques par déni de service au niveau applicatif). Par exemple, un oubli de vérification dans une application pourrait permettre à un attaquant d'envoyer des commandes non valides qui corrompent la base de données.

Les erreurs de configuration

Les **erreurs de configuration** sont des failles de sécurité qui résultent d'une mauvaise configuration des systèmes, des réseaux ou des applications. C'est comme laisser les portes d'une forteresse ouvertes ou utiliser des serrures de mauvaise qualité. Ces erreurs créent des points d'entrée faciles à exploiter pour les attaquants.

Voici quelques exemples courants :

- **Mots de passe par défaut non modifiés**, de nombreux équipements (routeurs, caméras IP) sont livrés avec des mots de passe par défaut connus publiquement (par exemple « admin », « azerty », « 123456 »…). Ne pas les changer est une invitation ouverte aux intrusions.
- **Ports réseau ouverts inutilement**, en informatique, un port réseau fonctionne un peu comme une porte spécifique sur votre ordinateur, dédiée à un type particulier de trafic internet. Lorsqu'un ordinateur reçoit des données venant d'internet, celles-ci doivent être acheminées vers la bonne « porte » pour atteindre l'application correspondante.

  Par exemple, le port numéro 80 est généralement utilisé pour le trafic web classique, permettant à votre navigateur (comme Chrome ou Firefox) d'afficher les pages que vous consultez. Le port 443, quant à lui, est réservé aux connexions sécurisées, celles dont l'adresse commence par « https:// », garantissant que les échanges soient chiffrés et protégés.

  Ainsi, lorsqu'un paquet de données, que l'on peut imaginer comme un facteur, arrive sur votre machine, il regarde le numéro de port indiqué pour savoir à quelle application (navigateurs, logiciels de messagerie, transfert de fichiers, etc.) il doit livrer ces informations.

  Cela permet à différentes applications d'utiliser la connexion internet en même temps sans se mélanger. Laisser ouverts des ports non-utilisés expose le système à des attaques potentielles.
- **Permissions d'accès trop larges**, attribuer des droits d'accès excessifs à des utilisateurs ou des applications peut permettre à un attaquant qui compromettrait un compte de se déplacer latéralement dans le système et d'accéder à des ressources sensibles.

- **Services non nécessaires activés**, faire fonctionner des services qui ne sont pas utilisés augmente la surface d'attaque et peut aussi introduire des vulnérabilités supplémentaires. Par exemple, sur de nombreux serveurs, le service Telnet (port 23), aujourd'hui obsolète et non sécurisé, reste parfois activé sans raison, cela offre une porte d'entrée facile pour les attaquants, qui peuvent en profiter pour intercepter les identifiants ou lancer des attaques par force brute, augmentant ainsi la surface d'attaque inutilement.
- **Mauvaise configuration des pare-feu**, un pare-feu, c'est comme un **vigile** posté à la porte de votre maison. Son rôle principal est de **contrôler qui entre et qui sort**. Il analyse donc toutes les informations venant d'Internet et bloque les tentatives de connexion non autorisées. Il analyse aussi les informations envoyées par votre ordinateur sur Internet, il peut donc empêcher des programmes malveillants d'envoyer des données sans votre permission. Mais attention, un pare-feu mal configuré peut laisser passer du trafic malveillant ou bloquer du trafic légitime.

Les faiblesses humaines

Les **faiblesses humaines** sont considérées comme le maillon le plus faible de la chaîne de sécurité. Même les systèmes les plus sophistiqués peuvent être compromis par des erreurs de jugement ou des comportements imprudents des utilisateurs (identifiants et/ou mot de passe écrits sur un post-it…). C'est comme donner la clé de la forteresse à un étranger sans vérifier son identité. Nous allons examiner les vecteurs d'attaque les plus exploités en cybersécurité.

Mots de passe faibles

L'Agence Nationale de la Sécurité des Systèmes d'Information (**ANSSI**) insiste sur le fait que des mots de passe **faibles** constituent une porte d'entrée privilégiée pour les cyberattaquants. Utiliser des mots de passe **courts**, **évidents** (comme « 123456 », « azerty », votre date de naissance ou le nom de votre animal), ou **répéter le même mot de passe** sur plusieurs de vos comptes numériques expose vos informations personnelles et vos comptes à des risques considérables. Les principales attaques sont :

- **Attaques par force brute**, des logiciels automatisés (de type Hydra ou John The Ripper) peuvent tester des milliers, voire des millions de combinaisons de mots de passe en un temps très court jusqu'à trouver le bon. Il faut toujours garder en mémoire qu'un mot de passe simple est une cible facile.
- **Credential stuffing**, si un de vos comptes est compromis en raison d'un mot de passe faible, les cybercriminels vont tester cette combinaison (identifiant et mot de passe) sur tous les autres services que vous utilisez. La réutilisation des mots de passe permet une propagation rapide des compromissions.