

Cybersécurité

Vers un monde plus sûr...

Cybersécurité

Vers un monde plus sûr... ou pas...

Qu'est-ce que la (cyber)sécurité pour vous ?



Organisation générale

- Introduction Générale
 - Risque global et dualité temporelle
 - Les données en danger
 - IoT : anatomie d'un risque majeur
 - Au-delà du virtuel
- Les problématiques de la gestion de la sécurité
 - La sécurité, c'est quoi ?
 - Pourquoi est-ce si complexe ?
- Quelques thématiques
 - La sécurité des systèmes
 - La sécurité des réseaux
 - La sécurité physique
- Les étapes classiques d'une attaque
- Étude de cas
- Quelques préconisations

4

Ce n'est pas forcément (si) technique

Cybersécurité et ingénierie sociale

ou l'art de convaincre

- Crédibilité,
- Urgence,
- Pouvoir,
- Peur,
- Confiance,
- Persuasion,
- Perception.





Typ[o]
Cliqueriez-vous ?



www.facebook.com

www.face-book.com

www.facebook.com

www.facehook.com

www.facebook.com

www.facebook.com

www.facebook.com

Zoom sur l'hameçonnage...

- L'hameçonnage, qu'est-ce que c'est ?

L'hameçonnage (phishing en anglais) est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe...) et/ou bancaires en se faisant passer pour un tiers de confiance.

Source: economie.gouv.fr

- Est-ce vraiment efficace ?

- Oui : beaucoup de « hacks » parmi les plus importants sont initiés par l'hameçonnage

- Pratiques classiques :

- Mails (phishing)
 - SMS (smishing)
 - Appels téléphonique (vishing)
 - Faux sites Web

- Objectifs :

- Vol d'identifiants
 - Installation de malwares



Quelques exemples...



impots.gouv.fr

un site de la direction générale des finances publiques

Bonjour,

Après les derniers calculs annuels de l'exercice de votre activité, nous avons déterminé que vous êtes admissible à recevoir un remboursement de 50.80 €.
Veuillez nous soumettre s'il vous plaît la demande de remboursement d'impôt pour nous permettre de la traiter dans un plus bref délai.

>> Pour accéder au formulaire , cliquez ici .

Un remboursement peut être retardé pour diverses raisons. Par exemple, une soumission de dossiers non valides ou une inscription après une certaine limite.

Philippe BERGER,
Conseiller fiscal adjoint

© Direction générale des finances publiques - 2014

Quelques exemples...



Madame, Monsieur,

À la suite de la nouvelle réglementation concernant la fiabilité des opérations sur internet vous étiez avertis de l'obligation d'y adhérer.

Or, nous n'avons pas, ce jour, d'adhésion de votre part, afin d'éviter une suspension de vos opérations, nous vous invitons à procéder à l'adhésion en suivant le lien ci-dessous.

Adhésion : [Faites votre demande d'adhésion en cliquant ici](#)

Cordialement,
Votre caisse du Crédit Mutuel.

Ce message est envoyé automatiquement. Merci de ne pas répondre.

⚠ Ce message et toutes les pièces jointes sont confidentiels et établis à l'intention exclusive de son ou ses destinataires. Si vous avez reçu ce message par

L'hameçonnage téléphonique ou vishing

Parce que l'attaque informatique directe n'est pas la seule option

<https://www.boursorama.com/videos/actualites/boursorama-banque-apprenez-a-vous-proteger-de-la-fraude-180616fa048ca8f8de6190d770a2bd97>

Pourquoi clique-t-on ?

- Étude 2023 (source DGSI)
 - 29 % Compliments
 - 28 % Autorité / Serviabilité
 - 25 % Curiosité / Confiance
 - 24 % Pression
 - 18 % Demande d'argent

Le temps : le sens de la relativité en cybersécurité

- **Le temps de réaction en faveur des hackers**
 - Vulnérabilités 0-day
 - Durée pour produire une mise-à-jour
 - Durée pour mettre en place une mise-à-jour
 - Politiques de mise-à-jour
- **L'âge du logiciel n'est pas forcément gage de sécurité**
 - Découverte de failles sur des logiciels en place depuis des années
 - Logiciel et matériel : un couple gagnant...

Cybersécurité et la notion de temps

- Septembre 2014
 - Découverte de la faille Bash « Shellshock » :
 - Cette faille touche l'un des programmes de base de plusieurs millions de machines UNIX. Elle permet de prendre la main à distance sur les machines.

14

Cybersécurité et la notion de temps

- Septembre 2014
 - Découverte de la faille Bash « Shellshock » :
 - Cette faille touche l'un des programmes de base de plusieurs millions de machines UNIX. Elle permet de prendre la main à distance sur les machines.
 - Bug existant depuis 1989

15

Failles Linux, pourquoi est-ce important ?

- 47% of professional developers use Linux-based operating systems. (Source Statista)
- Linux powers 39.2% of websites whose operating system is known. (source W3Techs)
- Linux powers 85% of smartphones. (source Hayden James)
- The Linux market size worldwide will reach \$15.64 billion by 2027. (source Fortune Business Insights)
- The world's top 500 fastest supercomputers all run on Linux. (source Blackdown)
- 96.3% of the top one million web servers are running Linux. (source ZDNet)

2014 !?! Oui, mais c'était avant !

Octobre 2023

Source: https://www.it-connect.fr/lattaque-marvin-le-retour-dune-vulnerabilite-vieille-de-25-ans-dans-le-rsa/?utm_content=cmp-true

Une faille de sécurité découverte en 1998 dans le standard de cryptographie à clé publique "PKCS #1 v1.5" refait surface...

En exploitant cette vulnérabilité, un attaquant peut déchiffrer du RSA, falsifier les signatures et même déchiffrer les sessions enregistrées sur un serveur TLS vulnérable.

Le risque temporel dans l'industrie et la santé

- Le rapport de 2022 de Claroty sur la sécurité industrielle indique que sur les 300 industriels contactés :
 - La moyenne d'âge des équipements de contrôle industriel utilisée est de 26 ans
 - 55% des sondés n'ont plus de mises-à-jour de sécurité de leurs ICS
- Selon le Canadian Association of Radiologists (CAR) Life Cycle Guidance (2021), la durée de vie des appareils de radiologie classiquement utilisé varie entre 8 et 14 ans
- Selon Forbes (<https://www.forbes.com/sites/davidchou/2023/10/04/medical-device-security-is-a-top-challenge-for-healthcare-cio/>):
 - It costs a healthcare system \$11M to recover from a cyberattack, according to IBM's [2023 Cost of a Data Breach](#) report
 - Medical devices often have a long life cycle, and many run on outdated and unsupported operating systems, lacking the capability to update to a newer version.
 - Unlike standard IT devices that can typically receive updates through a central system, medical devices often don't have built-in tools for software upgrades when a security patch becomes available.

18

Etat des lieux des vulnérabilités en 2023

Vulnerability Threat Landscape 2023



Source: <https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one>

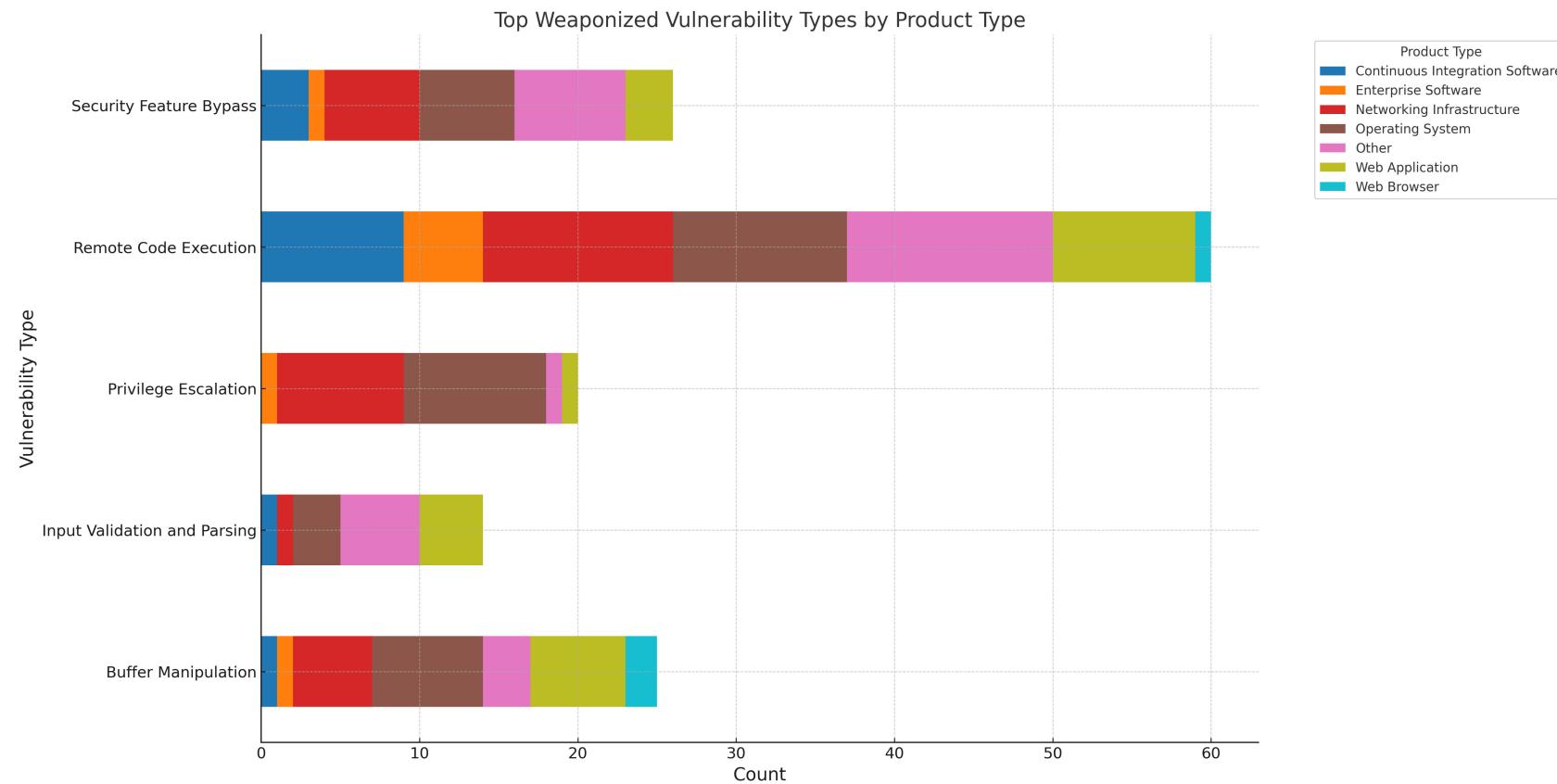
Etat des lieux des vulnérabilités mi-2024

Mid-Year 2024: Overview of the Evolving Cybersecurity Vulnerability Landscape



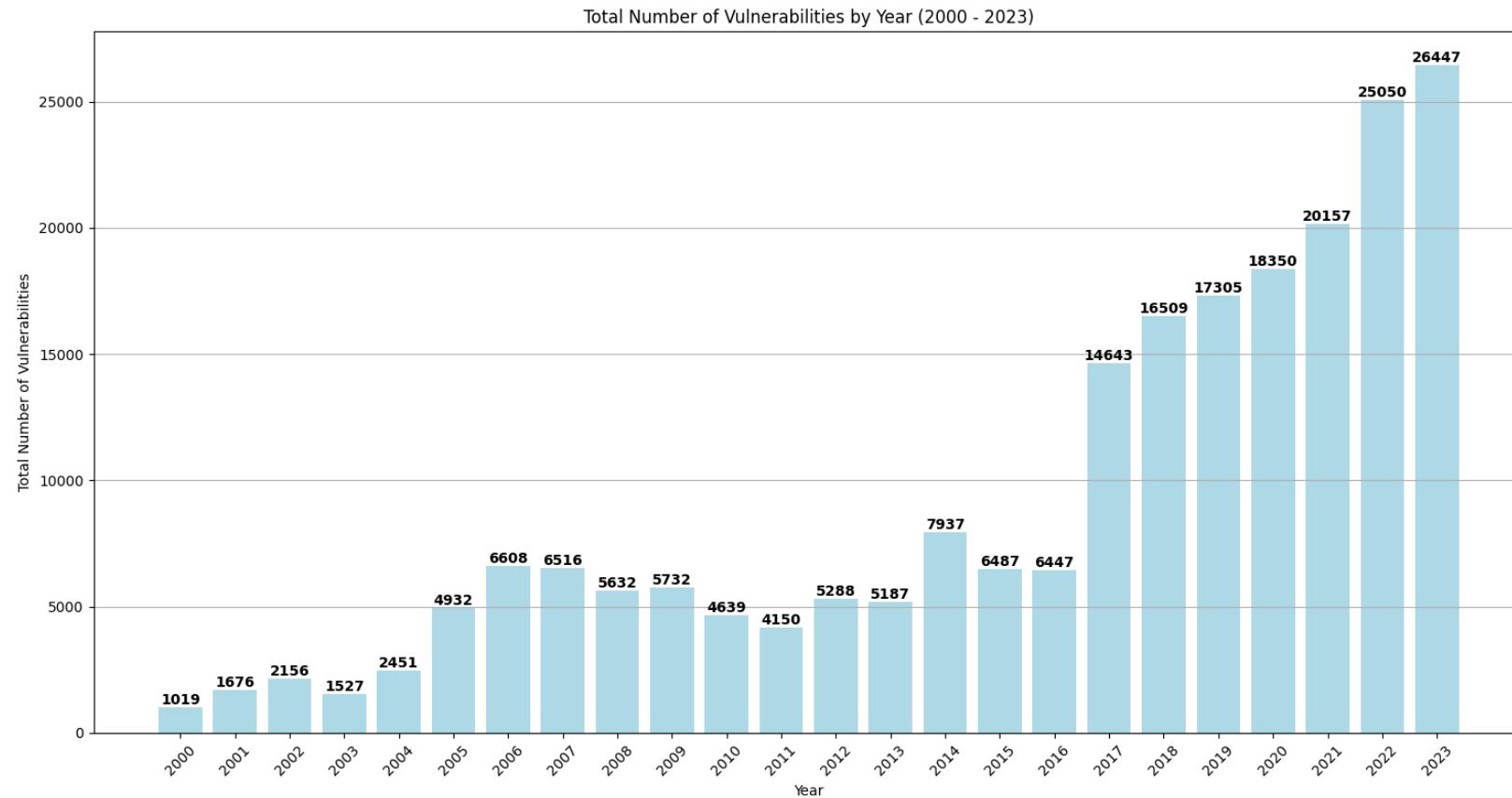
Source: <https://blog.qualys.com/vulnerabilities-threat-research/2024/08/06/2024-midyear-threat-landscape-review>

Usage & types d'exploitation



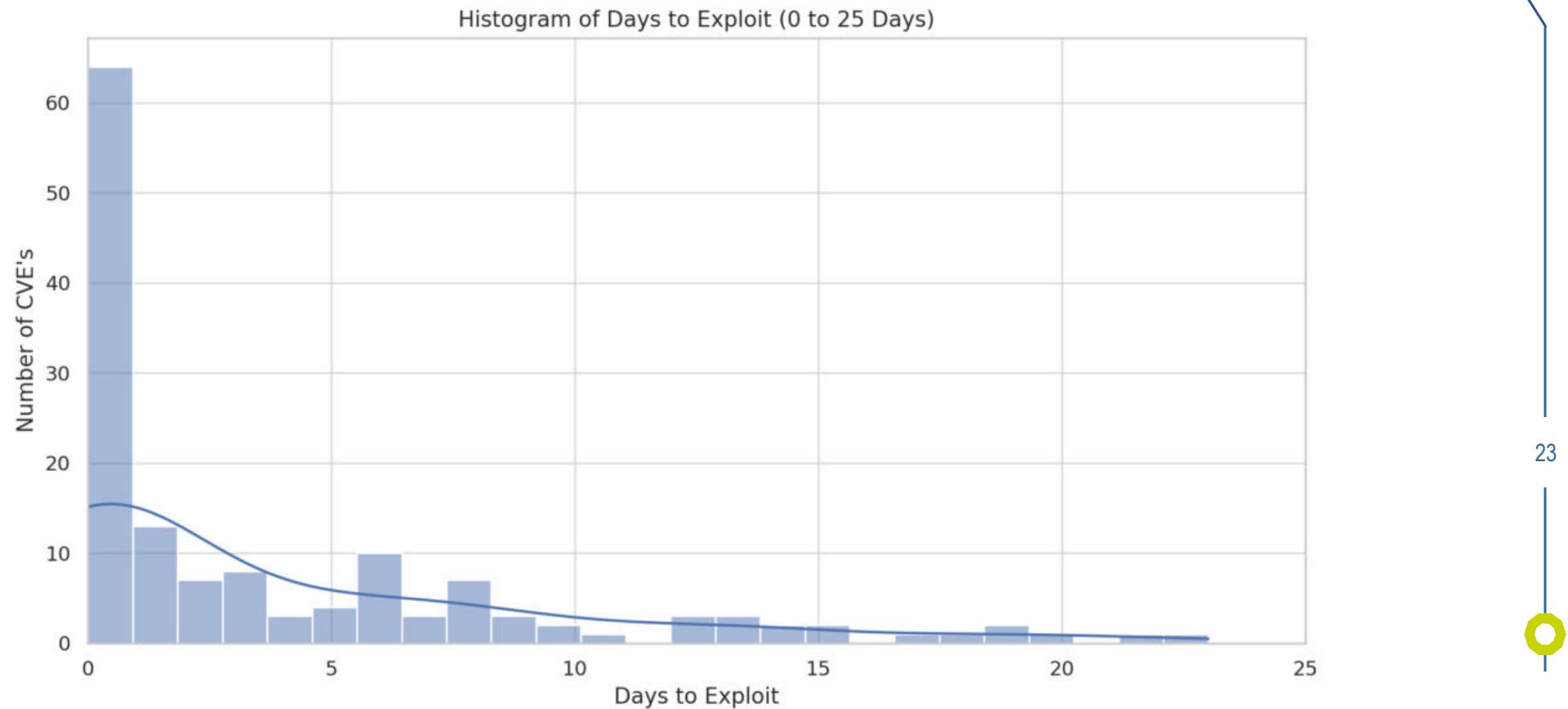
Source: <https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one>

Evolution du nombre de vulnérabilités découvertes



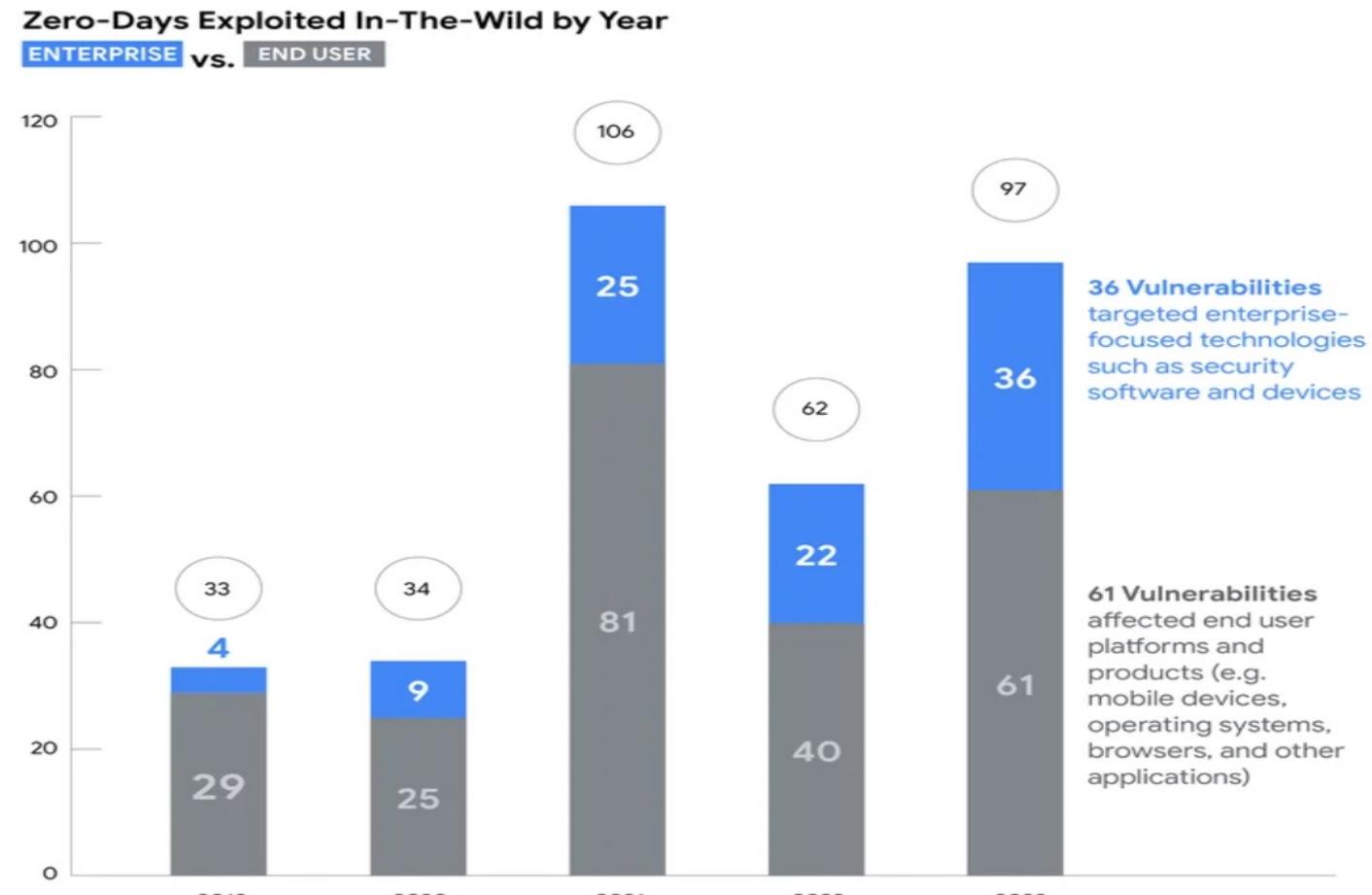
Source: <https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one>

75% des vulnérabilités exploitées en moins de 20 jours



Source: <https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one>

Le risque 0-day



Source: <https://blog.google/technology/safety-security/a-review-of-zero-day-in-the-wild-exploits-in-2023/>

Oui mais... des correctifs existent non ?

- Selon une étude de Synopsys qui a réalisé un sondage auprès de 1000 professionnels IT répartis aux U.S., en U.K., en France, en Finlande, en Allemagne, en Chine, à Singapour et au Japon en 2023
 - 20% des organisations admettent mettre jusqu'à 3 semaines pour patcher des problèmes de sécurité critiques

Selon Kimm Yeo, senior solutions manager chez Synopsys' software integrity

"There are multiple different factors involved when it comes to patching, and it's very time consuming."

"There are a lot of vulnerabilities sitting in the backlog... How do you know this is critical enough that you need to give it top priority, especially when there's a lack of security experts or insights into the vulnerability itself?"

- Selon le rapport rapport conjoint du CISA et de la NSA en octobre 2023, la (non) gestion des patchs est classée 5ième dans le Top 10 des mauvaises configurations en termes de cybersécurité

25

Sources:

<https://www.axios.com/2023/10/10/patching-security-flaws-slow>

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a>

PII & PHI ?!?



26

PII & PHI : Des données sensibles

- Données personnelles, données de santé et données financières sont des cibles courantes des pirates informatiques :
 - Nom, numéro de sécurité social
 - Adresse
 - Numéro de carte de crédit, de compte bancaire
 - Dossiers médicaux

27

PII & PHI : Des données sensibles

- Novembre 2017 :
 - Uber dévoile avoir payer \$100,000 à des hackers pour qu'ils détruisent les 57 millions de données volées concernant ses clients et chauffeurs : noms, numéros de téléphone, adresses mail, numéros de plaques d'immatriculation
- Mars 2018 :
 - Une fuite de donnée chez Under Armor compromet les informations personnelles de 150 millions d'utilisateurs de l'application MyFitnessPal

PII & PHI : Des données sensibles

Mars 2021

(source CNIL)

La fuite de données comprend notamment les informations suivantes, renseignées lors du test :

- les nom et prénoms ;
- la date de naissance ;
- le sexe ;
- le numéro de sécurité sociale ;
- l'adresse postale, électronique ou le numéro de téléphone ;
- les caractéristiques du test utilisé ;
- le résultat du test.

PII & PHI : Des données sensibles

Février 2024

(source: <https://www.zdnet.fr/actualites/prest>)

Le

m

Sé

m

a

s

Cher client,

Nous vous informons que Viamedis l'organisme auquel nous sous-traitons la gestion du tiers payant de la complémentaire santé vient de subir une cyberattaque.

Dès que Viamedis a pris connaissance de cet acte de violation, la plateforme a été déconnectée.

Une plainte a été déposée auprès du procureur de la République. Une notification et une déclaration aux autorités compétentes ont été effectuées (CNIL, ANSSI).

Les données personnelles exposées sont limitées et sont les suivantes pour vous-même et votre famille : état civil, date de naissance et numéro de sécurité sociale, nom de votre assureur santé et garanties de votre contrat.

Ni information bancaire, ni données médicales, ni remboursements santé, ni coordonnées postales, ni numéro de téléphone, ni email ne sont stockés sur cette plateforme. Ces informations ne sont donc pas concernées par cet acte malveillant.

Les équipes techniques sont mobilisées, des investigations sur l'impact de l'attaque sont en cours en lien avec les autorités compétentes.

PII & PHI : Des données sensibles

- Octobre 2024

Un piratage massif de Free en octobre

« Le 21 octobre, la base de données de Free, portant sur 19,2 millions de clients français », soit la majorité des 22,8 millions d'abonnés de l'entreprise, « dont 5,11 millions incluant un numéro IBAN, a été mise en vente aux enchères par un hacker sur un forum cybercriminel », a rappelé le ministère public, indiquant avoir confié l'enquête à la Brigade de lutte contre la [cybercriminalité](#) (BL2C) de la préfecture de police.

31

Source: https://www.20minutes.fr/faits_divers/4133883-20250115-vols-donnees chez-free-hacker-age-17-ans-interpelle

PII & PHI : Des données sensibles

Octobre 2022: Bluebleed

(source Génération Nouvelles Technologies)



Suite à une mauvaise configuration d'un conteneur de stockage Azure, les informations de certains clients et prospects de Microsoft fuient :

- 65000 entreprises
- 111 pays
- 2,4 To de données
- Données concernées : nom, mails, contenus de mails, numéros de téléphone, fichiers joints

PII & PHI : Des données sensibles

Juillet 2023

(source France tv info)

Des dossiers confidentiels du CHU de Rennes auraient été mis en ligne, vendredi 28 juillet, après un vol de données informatiques survenu en juin. Ils pourraient contenir des informations privées sur les patients et le personnel.

PII & PHI : Des données sensibles

Août 2023: Hack de Pôle Emploi

(source thebigdata.fr)

Une faille de sécurité chez un prestataire provoque la fuite de 10 millions de données d'allocataires.

Les données sont en vente pour \$900 sur le Dark Web.

Les données comprennent :

- Nom, prénom
- Numéro de sécurité sociale

Le monde de la finance : un terrain sensible

- Le top 5 des vols de données bancaires (2022)

Source: <https://www.upguard.com/blog/biggest-data-breaches-financial-services>

- First American Financial Corp (2019) : 885 millions de données financières et personnelles
- Equifax (2017) : plus de 40% de la population américaine potentiellement impactée
- Heartland Payment Systems (2008) : 130 millions de numéros de cartes bancaires volées
- Capital One (2019) : 100 millions de données d'applications carte de crédits (numéros de sécurité social, numéros d'assurance social canadien, numéros de compte bancaires)
- JP Morgan Chase (2014) : 83 millions de comptes

PII & PHI : Des données sensibles

Septembre 2023: It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy

(source <https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/>)

- Marques de voitures concernées : 25 marques différentes
- Points importants :
 - I. Toutes collectent beaucoup trop de données (des données personnelles aux informations de conduite en passant par les messages vocaux)
 - II. 84% partagent ou revendent les données collectées
 - III. 92% ne donnent presque aucun contrôle sur les données personnelles collectées
 - IV. Il a été impossible de savoir si les marques adressaient un minimum de sécurité sur les données collectée

*Privacy Not Included

moz://a

WHERE DOES ALL YOUR DATA GO?



PII & PHI : au-delà de la divulgation...

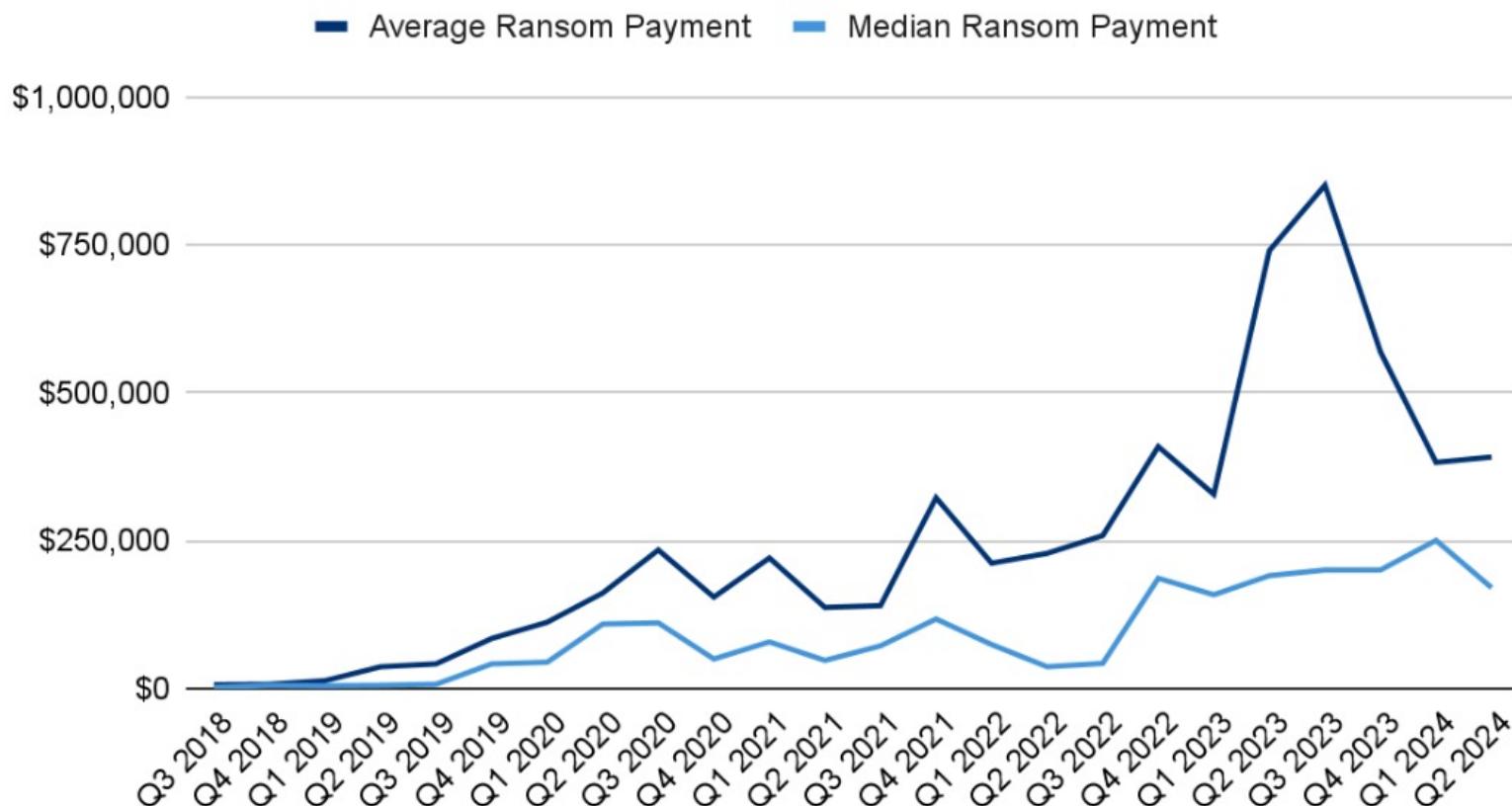
- Avril 2019 :
 - Des chercheurs israéliens sont parvenus à développer un logiciel malveillant capable **d'altérer les résultats d'un scanner médical afin d'afficher ou de supprimer des cellules cancéreuses** très facilement. Mais leurs recherches mettent avant tout en exergue la vétusté des infrastructures hospitalières face aux risques de cyberattaques.

Ransomware !?!



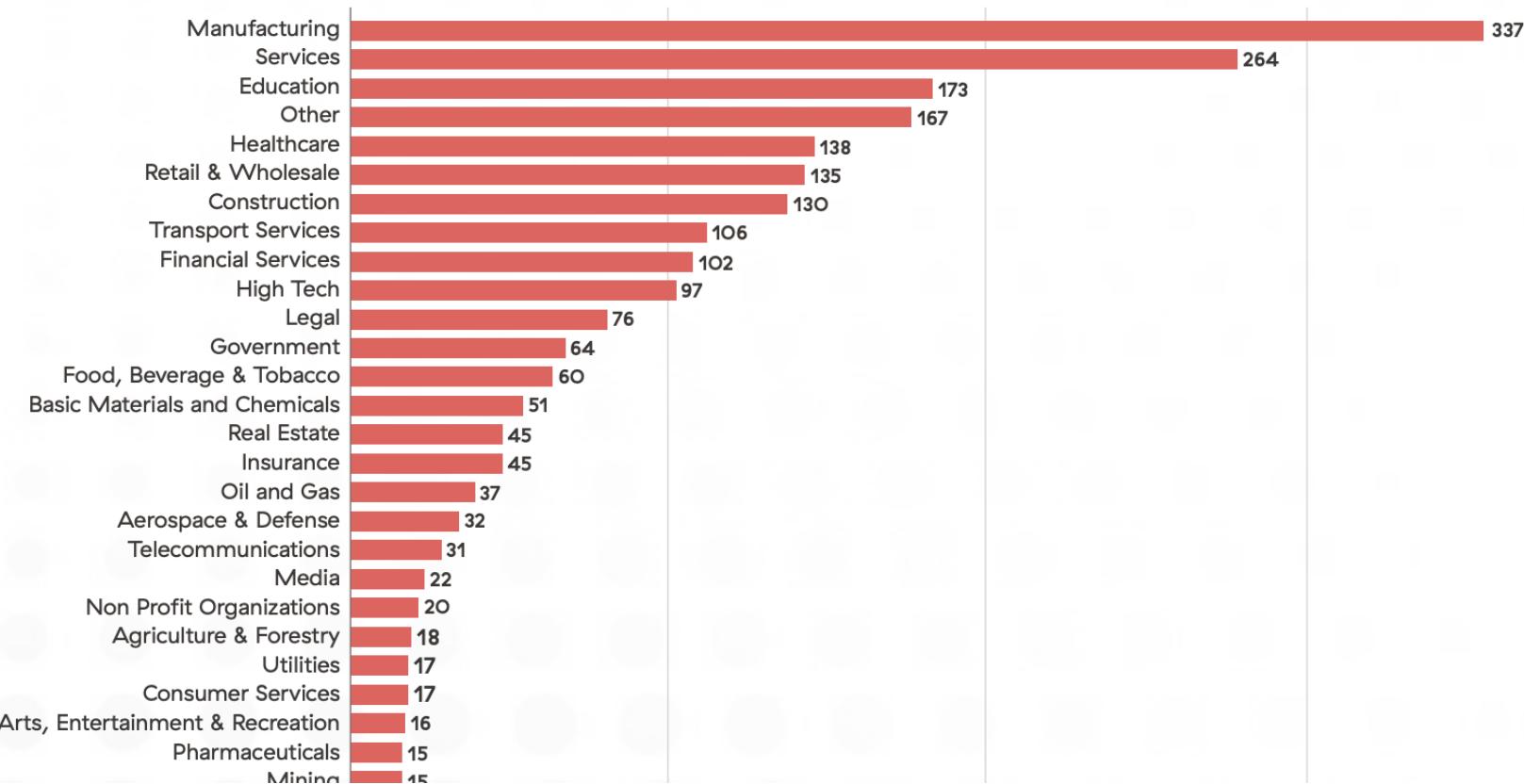
Le ransomware est-ce rentable ?

Ransom Payments By Quarter



Source: <https://www.coveware.com/blog/2024/7/29/ransomware-actors-pivot-away-from-major-brands-in-q2-2024>

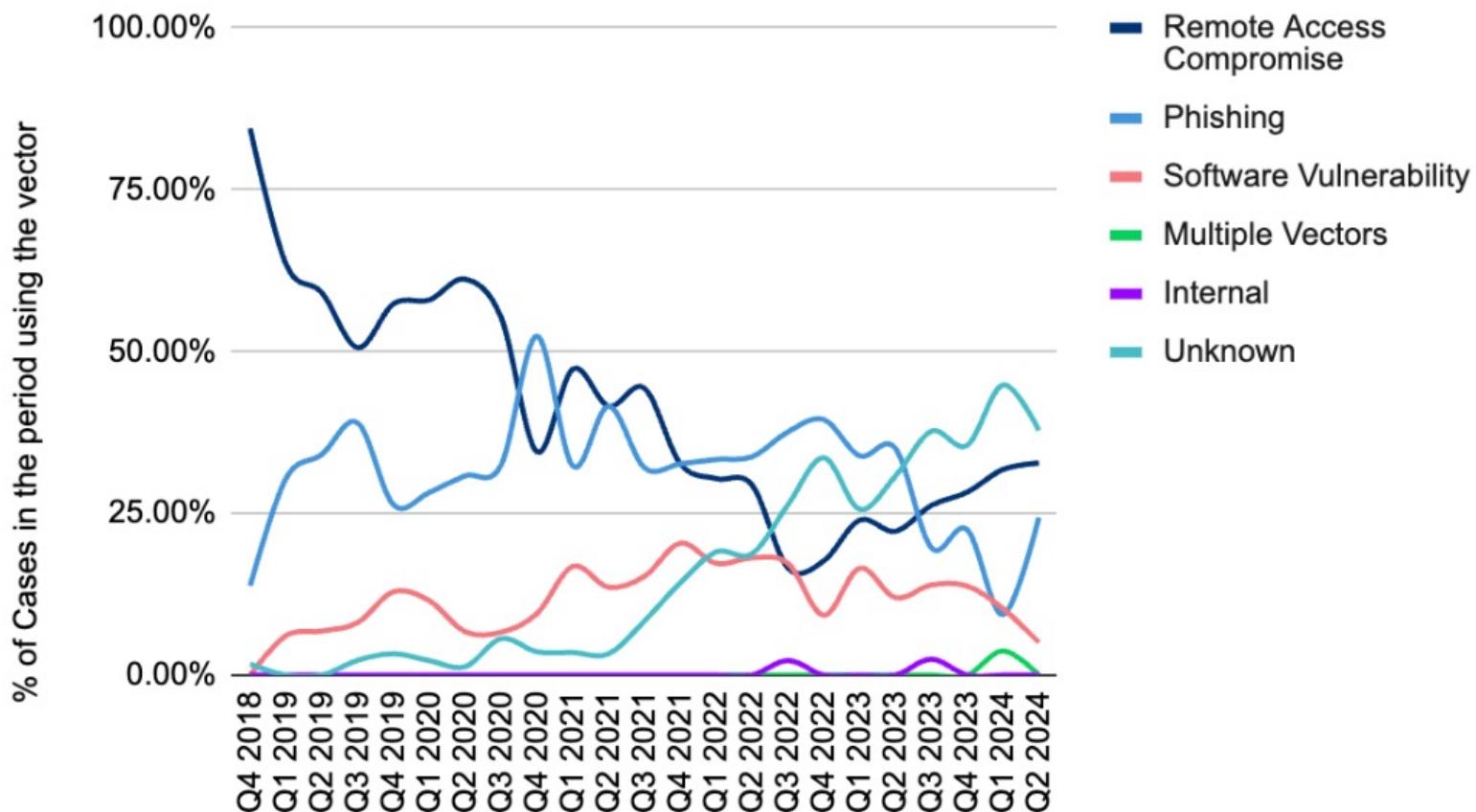
Ransomware, les cibles en 2023



Source: <https://www.zscaler.com/resources/industry-reports/2023-threatlabz-ransomware-report.pdf>

Ransomware, les moyens d'entrer...

Ransomware Attack Vectors



Source: <https://www.coveware.com/blog/2024/7/29/ransomware-actors-pivot-away-from-major-brands-in-q2-2024>

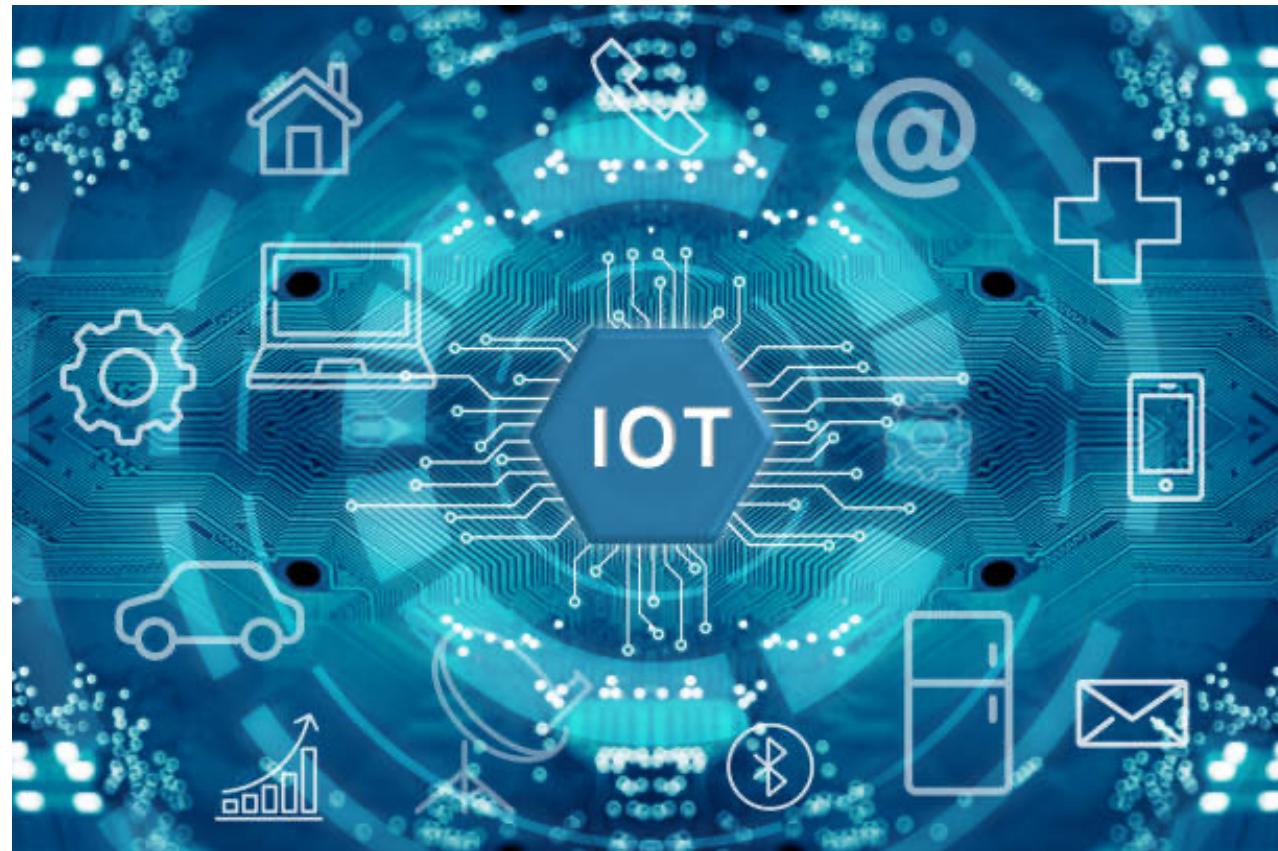
Ransomware, quelques chiffres

- Source DGSI
 - +27 % d'attaques par ransomware en 2023
 - 94 % des attaques réussies par mail
 - 627 attaques de boîtes mails par minute Q4 2023
 - 3357 attaques de boîtes mails par minute Q1 2024
 - 1 entreprise sur 5 met les clés sous la porte après une cyberattaque

43

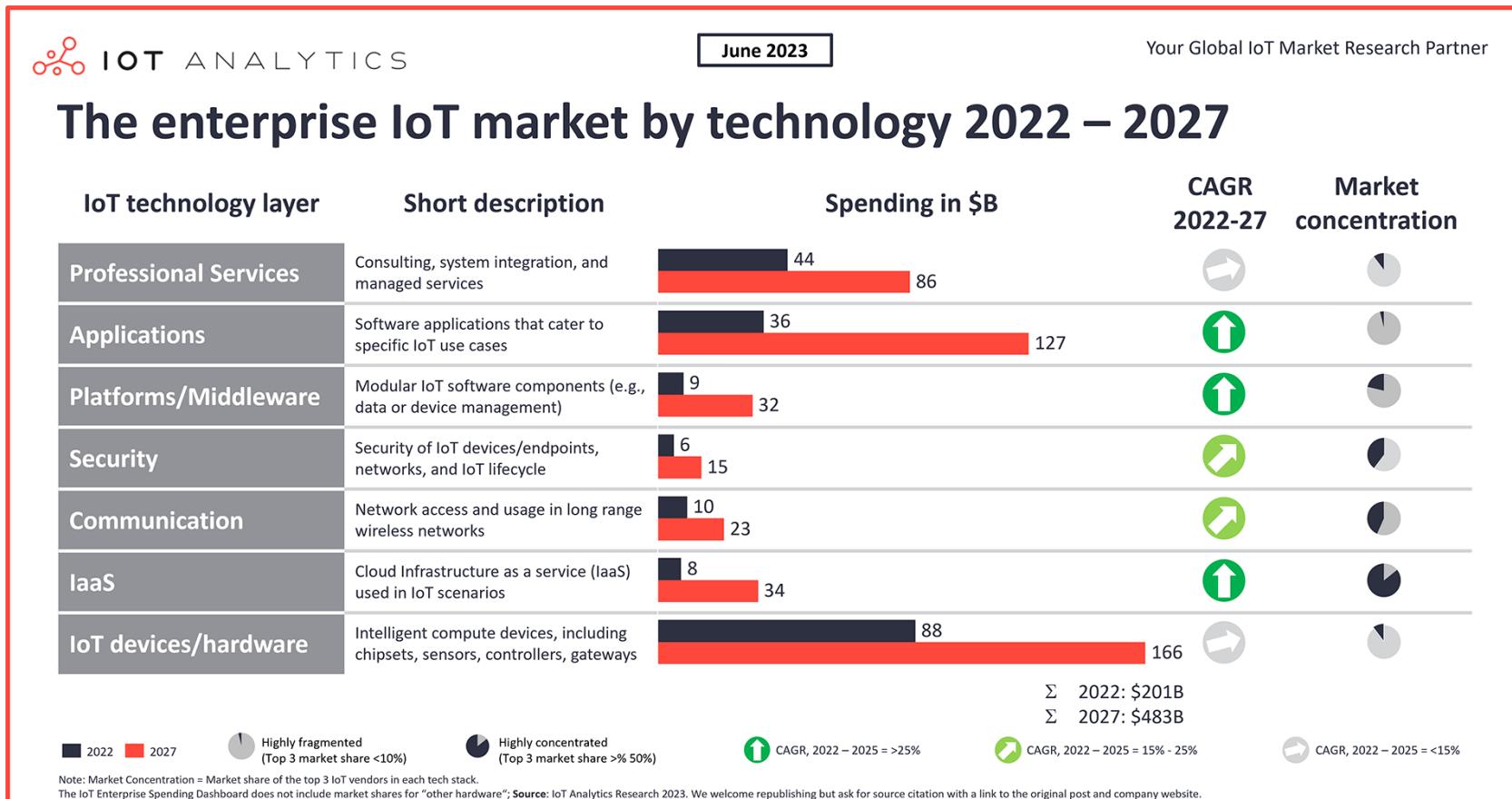


Internet of Things !?!



44

IoT & Cybersecurité : quel est le marché ?



IoT & Cybersecurité : quelques exemples parlant...

- **Cisco:** Anatomy of an IoT Attack
https://www.youtube.com/watch?v=7egBsN_4B2A
- **Reportage :** Security in Med equipment
<https://www.youtube.com/watch?v=smhPhmNsvVc>

IoT & Cybersécurité : Et si la fiction devenait réalité ?

Un thermomètre?

. Avril 2018

Un casino piraté depuis le thermomètre connecté de son aquarium

« Il y a beaucoup d'objets connectés, des thermostats, systèmes de réfrigération, des systèmes de HVAC [climatisation] et des gens qui apportent leurs appareils Alexa dans les bureaux ... Il y a juste beaucoup d'objets. Cela étend la surface d'attaque et la plus grande partie de celle-ci n'est pas couverte par les défenses traditionnelles, » Nicole Eagan.

Source: siecledigital.fr

IoT & Cybersécurité : Et si la fiction devenait réalité ?

Fiat lux et facta est

- . Février 2020 :
 - . Checkpoint dévoile une vulnérabilité du système Philips Hue permet à un hacker de prendre le contrôle des ampoules connectées...
 - et d'escalader l'attaque au niveau du réseau informatique domestique
- . Août 2023:
 - . Une vulnérabilité dans le système d'authentification des ampoules connectées TP-Link Smart Bulbs permet à un attaquant de récupérer les identifiants WiFi

IoT : un danger pour les autres



Octave Klaba ✅

@olesovhcom

...

This botnet with 145607 cameras/dvr (1-30Mbps per IP) is able to send >1.5Tbps DDoS. Type: tcp/ack, tcp/ack+psh, tcp/syn.

2:31 pm · 23 Sep 2016

IoT-driven DDoS attacks increased by 300% in the first half of 2023 alone, causing an estimated global financial loss of \$2.5 billion. In 2023, 90% of complex, multi-vector DDoS attacks were based on botnets. The trend shows no signs of slowing down: the number of IoT devices engaged in botnet-driven DDoS attacks rose from around 200,000 a year ago to approximately 1 million devices, while there are twice as many vulnerabilities being targeted by botnet malware.

Source: <https://thehackernews.com/2023/09/ddos-20-iot-sparks-new-ddos-alert.html>

IoT & Cybersécurité : Oups...

Avril 2021 :

(Source : wired.com)

100 Million More IoT Devices Are Exposed—and They Won't Be the Last

The Name:Wreck flaws in TCP/IP are the latest in a series of vulnerabilities with global implications.

All of the vulnerabilities, discovered by researchers at the security firms Forescout and JSOF, now have patches available, but that doesn't necessarily translate to fixes in actual devices, which often run older software versions. Sometimes manufacturers haven't created mechanisms to update this code, but in other situations they don't manufacture the component it's running on and simply don't have control of the mechanism.

IoT & Cybersécurité : backdoors ?!?

Backdoor found in two healthcare patient monitors, linked to IP in China

By [Lawrence Abrams](#)

January 30, 2025

06:31 PM

10



51

IoT & Cybersécurité : Et dans la santé...

Novembre 2022: L'hôpital sous la menace des hackers

(source France Info)

Toutes les chambres d'hôpital contiennent un moniteur de surveillance relié à un autre dans la salle des infirmiers. Un dispositif indispensable pour visualiser en un coup d'œil des signes vitaux tels que la fréquence cardiaque. A l'aide de deux de ces moniteurs, Charles Blanc Rolin (chercheur en cybersécurité) montre combien il est facile de "*faire penser au médecin que le patient va bien alors que ce n'est pas le cas, ou inversement*".

Après avoir désactivé le premier moniteur, il envoie tout simplement au second... de fausses valeurs (par exemple un rythme cardiaque de 160 battements par minute au lieu de 50).

IoT & Cybersécurité : heureusement, il y a des patchs

Novembre 2022: Alerte Microsoft : ce serveur web open source oublié pourrait permettre aux pirates d'accéder "silencieusement" à votre système

(source ZDNet)

Le serveur web Boa, qui est souvent utilisé pour accéder aux paramètres et aux consoles de gestion et aux écrans de connexion de nombreux appareils IoT recèle de nombreuses failles de sécurité.

Abandonné en 2005, le serveur web Boa continue d'être mis en œuvre par différents fournisseurs à travers une variété d'appareils IoT (internet des objets) et de kits de développement logiciel (SDK) populaires...

53

Heureusement, ce n'est que du logiciel et de la donnée !?!

```
function flatten(e, t) {
    var r, i = 0;
    e = e.length;
    if (e == null) {
        return [];
    } else if (e < 0) {
        return [];
    } else if (e == 1) {
        if (r = t.apply(e[0], t)), r === t) break;
    } else if (e > 1) {
        for (i = 0; i < e; i++) {
            if (r = t.apply(e[i], t), r === t) break;
        }
    } else if (e > 0) {
        for (i = 0; i < e; i++) {
            if (r = t.call(e[i], i, e[i])), r === t) break;
        }
    } else {
        for (i = 0; i < e; i++) {
            if (r = t.call(e[i], i, #([i])), r === t) break;
        }
    }
    return r;
},
trim: b && b.call("toString") ? function(e) {
    return null == e ? "" : b.call(e)
} : function(e) {
    return null == e ? "" : (e + "").replace(c, "")
},
makearray: function(e, t) {
    var n = e || [];
    return null != e && (n[object] == t) ? n : e == "string" ? typeof e != [e] : n[0] == e ? n : n[0] == "#([0])" ? e : n;
},
isarray: function(e, t, n) {
    var r;
    if (t) {
        if (n) return n[0](t, e, n);
        for (r = e.length, n = 0; r > n; r = e.next(n)) {
            if (r > 0 && r < e.length) n++;
        }
    }
    return r;
}
}
```

54

Les processeurs impactés

- Janvier 2018 : Google lève le voile sur deux problèmes de sécurité majeurs concernant les processeurs Intel
- Meltdown : permet une élévation de privilèges, puisqu'elle permet à un processus d'accéder à des ressources mémoires protégées au niveau du noyau du système d'exploitation.
- Spectre : permet à un programme d'accéder aux espaces mémoires d'un autre programme et donc de récupérer des informations confidentielles.



55

Les processeurs impactés

- Avril – Mai 2019 : ZombieLoad
 - Une nouvelle faille de sécurité pour les puces Intel
 - Possibilité de lire des données récentes ou en cours d'utilisation sur le même cœur processeur
 - Un correctif est disponible sur les processeurs les plus récents
 - Une baisse de performances de 3 à 9 % attendue
- Janvier 2020 : Cache-out
 - Une nouvelle vulnérabilité découverte permettant une fuite de données
 - Un nouveau micro-code est en préparation
 - Les fournisseurs Cloud doivent mettre en place des contre-mesures préventives



Uniquement Intel ?



Septembre 2021

(source clubic.com)

**AMD : une nouvelle vulnérabilité de type
Meltdown découverte sur les Zen+ et Zen2**

Même si la menace a été repérée dès octobre 2020, sa découverte est restée secrète, afin de permettre à AMD de corriger la faille.



Et récemment ?

- Mars 2022 : variante de Spectre: ***Branch History Injection***
- Juillet 2022 : ***Retbleed***, une nouvelle variante est divulguée. Sa mitigation affecte les performances Intel jusqu'à 39% sur les puces Intel et 14% sur les puces AMD
- Août 2022 : La vulnérabilité **Squip** est dévoilée. Elle touche les processeurs Intel des générations 10 à 12 et les architectures AMD Zen 1 à 3
- Août 2023: La vulnérabilité **Downfall** est rendue publique. Plusieurs générations de processeurs Intel touchés. La correction peut réduire les performances de 50%
- Mars 2024: Variante de Spectre: GhostRace (Intel, AMD, ARM)
- Juillet 2024: Variante de Spectre: Inderator qui touche les processeurs Intel de la famille Alder & Raptor Lake

Des impacts au-delà du monde informatique...



59



Des impacts industriels...

- 2010 : Stuxnet
 - Une cyberattaque ciblant le programme nucléaire iranien cause une perte de contrôle des centrifugeuses.
 - L'attaque a à priori retardé le programme iranien de quelques années
- 23 décembre 2015 : une cyber-attaque contre une centrale électrique en Ukraine
<https://www.youtube.com/watch?v=PafvyydhITw>
- Juillet 2015 : Des hackers publient une vidéo où ils montrent comment une jeep connectée peut être piratée
<https://www.youtube.com/watch?v=MK0SrxBC1xs>
 - Août 2017 : Trend Micro publie un article sur la vulnérabilité du standard CAN utilisé dans la plupart des véhicules modernes

Des impacts industriels...

- Juillet 2020 : un ransomware paralyse Garmin. Au-delà des produits de sport, les pilotes et compagnies aériennes sont également concernés
- Mars 2021: Oldsmar en Floride : une station d'épuration hackée. Les hackeurs tentent de porter la teneur en hydroxyde de sodium (soude caustique) de l'eau distribuée de 100 à 11000 ppm
- Mai 2021 : victime d'un ransomware, Colonial Pipeline doit arrêter son système de distribution pendant plusieurs jours provoquant pénuries en hydrocarbures et augmentation des prix
- 2023 : l'attaque d'une pulperie au Canada provoque le versement de 2.5 millions de litres d'eau contaminée dans une rivière exterminant poissons et flore aquatique. La cible de cette attaque était le ICS (Industrial Control System) de l'usine.

61

**Mes données sont à l'abri..
Elles sont dans le Cloud !**



62



Mes données sont dans le Cloud...

- . Août 2015 : touché par la foudre, un data-centre de Google perd des données :
 - . Google joue la transparence mais minimise l'incident : cela ne concerneait que 0,000001% de l'espace alloué sur un certain type de stockage de « europe-west1-b », l'une des trois zones européennes de stockage que proposait Google en 2015.

Plus récemment...

9 Mars 2021

(Divers sources)

Incendie dans le datacentre de Strasbourg d'OVH



Bilan à ce jour

SBG-2 détruit

SBG-1 4 salles sur 12 détruites

SBG-3 et SGB-4 indemnes

Mes données sont dans le Cloud...

Offre	Type de backup	Datacenters stockant les données primaires	Datacenter(s) stockant les backups	Statut du backup
Public Cloud	NC	SBG1, SBG2, SBG3 ou SBG4	SBG1 et SBG3	Statut final à confirmer (restauration espérée d'ici le 26 mars)
Private Cloud	Gratuit ou payant	SBG1, SBG3	Backup dans le même datacenter, respectivement SBG1 et SBG3	Serveurs de backup détruits pour SBG1, et intacts pour SBG3
Serveurs bare metal	Backup FTP gratuit ou payant	SBG1, SBG2, SBG3 ou SBG4	RBX (datacenters d'OVH à Roubaix)	Disponible immédiatement
VPS	Backup FTP gratuit ou payant	SBG1, SBG2, SBG3 ou SBG4	RBX (datacenters d'OVH à Roubaix)	Disponible immédiatement
VPS/PCI	Backup payant	SBG1, SBG2, SBG3 ou SBG4	Stockage sur site dont 20% sur SBG2 qui a été détruit	Statut final à confirmer pour les 80% du backup restant (restauration espérée d'ici le 26 mars)

Mes données sont dans le Cloud...

Novembre 2022: Des dizaines de milliers d'entreprises suisses victimes indirectes d'une cyberattaque

(source RTS.CH)

Plus de 45'000 PME et près d'un millier de fiduciaires suisses ne peuvent plus utiliser leur logiciel de gestion "Winbiz cloud", accessible en ligne.

La faute à une attaque informatique qui a touché l'hébergeur bernois Infopro.

[L'entreprise victime] ne peut plus émettre de factures, de bulletins de commandes ou de fiches de salaires.

Mes données étaient dans le Cloud...

Août 2023: L'opérateur Cloud Danois CloudNordic hacké

(source DCMag)

Dans un message publié sur son site web, le danois CloudNordic résume très simplement son histoire : « *Les attaquants ont réussi à chiffrer les disques de tous les serveurs, ainsi que les systèmes de sauvegarde principal et secondaire, ce qui a fait planter toutes les machines et nous avons perdu l'accès à toutes les données.* »

Les données sur les serveurs et les systèmes de sauvegarde ont été chiffrées, et le ransomware s'est fait connaître en exigeant le paiement d'une rançon de quelques bitcoins, pour une valeur d'environ 1,5 million de dollars. Que CloudNordic a refusé de payer.

Mais les données n'ont pas pu être récupérées. Ce qui se traduit par la perte des données CloudNordic et de ses clients. Et par l'impossibilité de les récupérer puisque les sauvegardes ont également été victimes de l'attaque. Pour résumé CloudNordic a perdu TOUTES les données de ses clients !

Mes données dans le Cloud sont sécurisées...

Septembre 2023: Microsoft publie accidentellement plus de 38 To de données privées

(source: <https://www.lemondeinformatique.fr/actualites/lire-microsoft-publie-accidentellement-plus-de-38-to-de-donnees-privees-91590.html>)

Des chercheurs en sécurité de Wiz ont trouvé un répertoire GitHub exposé sur le web appartenant à la division de recherche en intelligence artificielle de Microsoft. Ce dernier contient 38 To de données incluant des mots de passe, des clés privées et des messages Teams de 359 employés du géant américain.

Des enjeux nationaux



Un enjeu pour la sécurité nationale

. 2015 :

- Le New York Times révèle que de nouvelles règles « secrètes » permettent désormais au président américain de disposer de tous les pouvoirs pour prévenir ou riposter à une cyberattaque de grande ampleur.

Un enjeu pour la sécurité nationale

· Mai 2019 :

- Ciblé par une cyberattaque, Israël répond avec des missiles

"We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work." — Israel Defense Forces (@IDF) 5 mai 2019

Un enjeu pour les accès Internet

- Octobre 2022 (source: JdG – journaldugeek.com)
 - Dans la nuit du 17 au 18 octobre, un câble de fibre optique majeur a été sectionné dans les Bouches-du-Rhône. Il s'agit indiscutablement d'un acte de vandalisme selon Zscaler, une entreprise de cybersécurité qui exploite cette infrastructure de SFR ; et ce sabotage a eu des conséquences sur la connectivité web un peu partout dans le monde.



Tout peut être une excuse...

Novembre 2022: Coupe du monde au Qatar : la Cnil conseille aux supporters français d'utiliser des téléphones vierges pour prévenir les risques d'espionnage

(source FranceInfo)

La raison : Le gouvernement qatari exige des ressortissants étrangers l'installation de deux applications mobiles (Hayya et Ehteraz) qui, selon des experts, s'apparentent à des logiciels d'espionnage.

Une arme offensive

- Janvier 2022 :
 - Une cyberattaque ciblant le gouvernement ukrainien compromet 90 sites Web et déploie des logiciels malveillants se faisant passer pour des ransomware dans le but d'endommager des douzaines de serveurs étatiques
 - Biélorussie : une cyberattaque contre le réseau ferroviaire identifiée pour ralentir le déploiement des forces russes
- Février 2022 :
 - Des sites gouvernementaux ukrainiens sont bloqués et des « wipers » sont utilisés dans des attaques contre des institutions financières ukrainiennes
- Mars 2022 :
 - Une attaque sur le fournisseur de service satellite Viasat perturbe les connexions internet en Europe y compris les communications militaires ukrainiennes

Les Cyber-teams au centre du conflit en Ukraine

- VULKAN NTC, la société de conseil en informatique russe recyclée dans la cyberguerre :

Pour maximiser l'efficacité de ses attaques, **Vulkan s'appuie sur un logiciel baptisé Scan-V**. Sa mission ? **Rechercher sur le web des vulnérabilités et failles de sécurité** qui sont ensuite répertoriées pour une éventuelle exploitation. Un autre système, appelé **Amezit**, se présente comme un **plan de surveillance et de contrôle d'internet** dans les régions sous juridiction russe. Il s'agit également d'une **machine à désinformation, capable de créer de faux profils sur les réseaux sociaux et de partager des fake news**.

Abordons enfin un autre système, à savoir **Crystal-2V**. Il se manifeste comme **un programme de formation pour les cyberattaquants**. On y trouve notamment des **méthodes pour perturber les activités d'infrastructures ferroviaires, portuaires et aériennes**. Il est d'ailleurs indiqué que "*le niveau de confidentialité des informations traitées et stockées dans le logiciel est Top Secret*".

- <https://www.youtube.com/watch?v=zX9emwKYemE>

En résumé...

La sécurité au quotidien



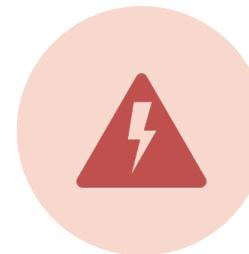
LES DIAPOS PRÉCÉDENTES NE SONT QUE DES EXEMPLES.



TOUT LE MONDE, À TOUT MOMENT, PEUT ÊTRE VICTIME DE PROBLÈMES LIÉS À LA SÉCURITÉ DES SYSTÈMES D'INFORMATION.



BEAUCOUP DE PARTICULIERS ET D'ENTREPRISES NE SONT PAS CONSCIENTS QU'ils PUISSENT ÊTRE DES VICTIMES.



LA SÉCURITÉ A UN COÛT MAIS QUEL EST LE COÛT DE NE PAS SE PROTÉGER. PRENDRE UN RISQUE EST SOUVENT UNE OPTION CHOISIE PAR DE TROP NOMBREUSES PERSONNES.

Mais au fait...
Que cherche-t-on à protéger ?



Un peu de terminologie...

- Un **Bien** : toute donnée, tout matériel, tout composant qui doit être protégé,
- Une **Vulnérabilité** : un défaut ou une faiblesse touchant un Bien,
- Une **Menace** : un danger possible,
- Un **Exploit** : quelque chose qui utilise une Vulnérabilité dans un Bien,
- Une **Risque** : l'impact résultant de la compromission d'un Bien ; un risque est généralement la composition d'une Menace, de Vulnérabilité(s) et de leur(s) impact(s).

Un nom, différents types...



White Hat

Autorisé à hacker
un système



Grey Hat

Non-autorisé à
hacker un système



Black Hat

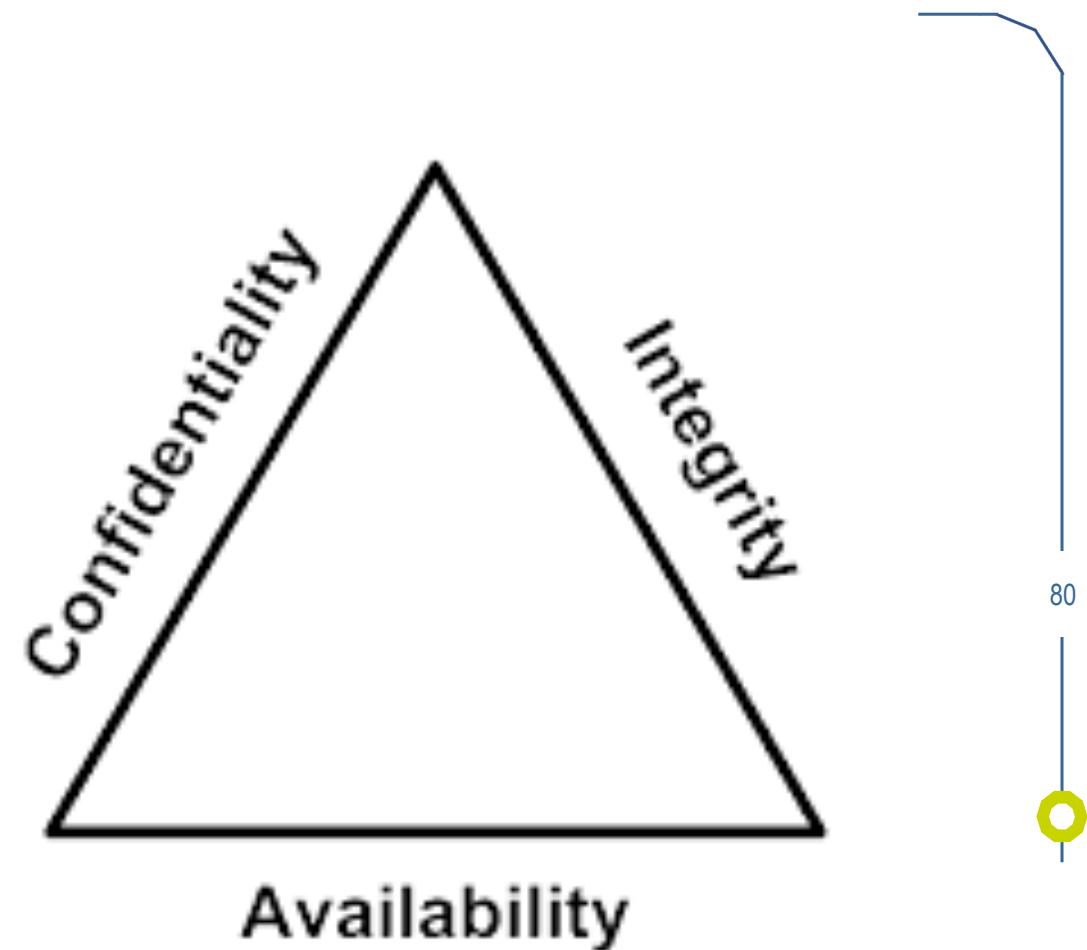
Non-autorisé à
hacker un système

79

Les trois dimensions de la sécurité

Beaucoup d'experts ajoutent également d'autres principes :

- L'authentification
- L'autorisation
- L'accountabilité
- La non-répudiation
- La fiabilité
- La survie



La confidentialité

- De manière générale, la confidentialité fait référence à la protection des données contre les accès non autorisés
- Comment la confidentialité peut être compromise ?
 - Violation de données
 - Captures de données
 - Menaces internes
 - Ingénierie sociale
 - Attaques brute force
- Quelques moyens pour garantir la confidentialité
 - Chiffrement des données
 - Contrôles d'accès
 - Mise en place de rôles
 - Mise en place de politiques de gestion des données
 - Formation des employés

81

L'intégrité

- Objectifs: Préservation de l'exactitude et de l'intégralité des données
- Comment les données peuvent être compromises ?
 - Corruption des données lors du stockage ou de la transmission
 - Malware
 - Modification volontaire suite à un accès indésirable
- Quelques moyens de garantir l'intégrité
 - Gestion des accès
 - Mise en place de rôles
 - Utilisation de sommes de contrôle et de codes de hachage
 - Dans une certaine mesure, le chiffrement

82

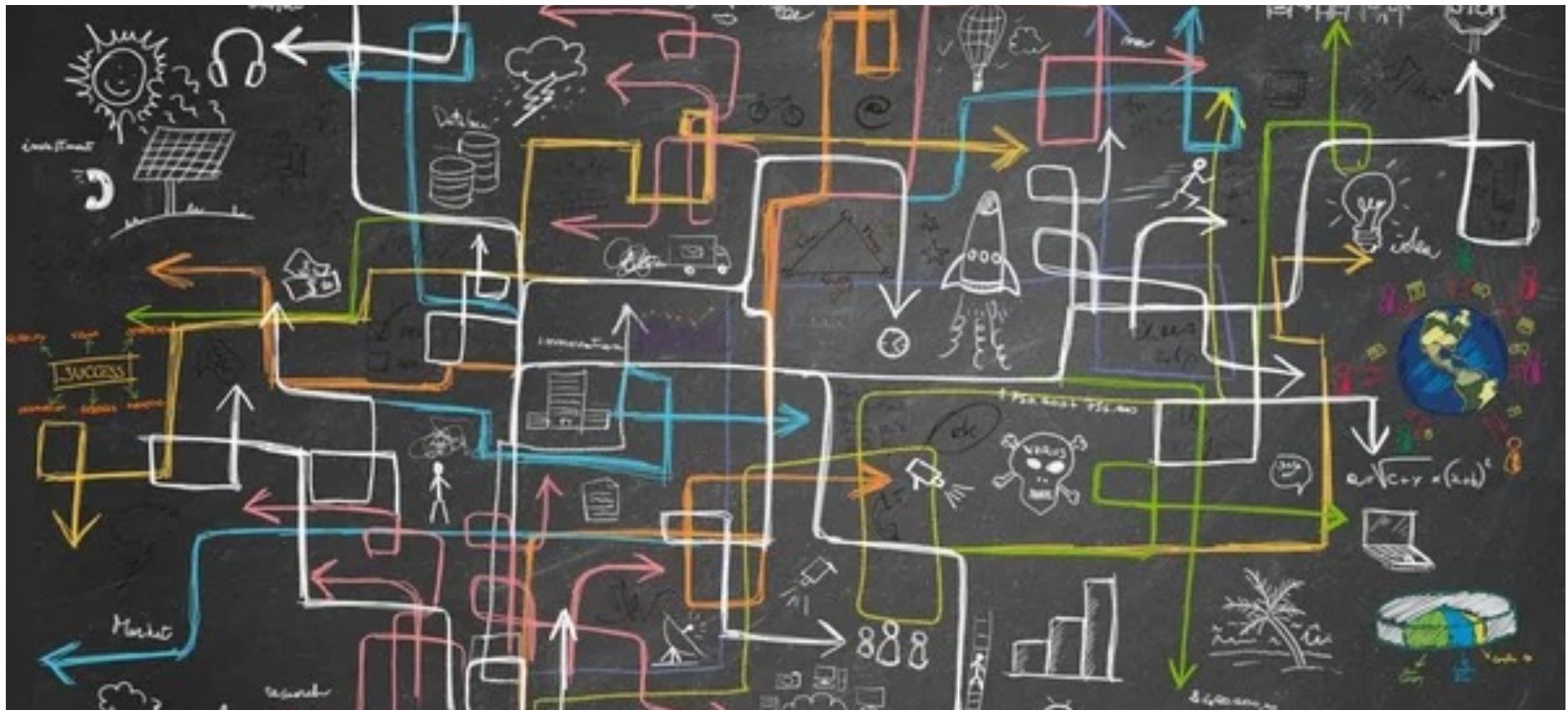
La disponibilité

- La disponibilité fait référence à la garantie que les systèmes et les données sont accessibles aux utilisateurs autorisés lorsqu'ils en ont besoin
 - Cela implique que les données et les systèmes soient opérationnels et en bon état de fonctionnement
- Comment la disponibilité peut être compromise ?
 - Pannes matérielles et logicielles
 - Pannes réseau
 - Pannes d'alimentation électrique
 - Désastres naturels
 - Ransomwares
- Quelques moyens de garantir la disponibilité
 - Mise en place systèmes redondants
 - Sauvegardes
 - Utilisation d'équilibreurs de charge
 - Tests réguliers des systèmes et maintenance
 - Monitoring
 - Mise en place de PCA / PRA

83



La cybersécurité : Pourquoi est-ce si complexe ?



Pourquoi est-ce si complexe ?

- Des systèmes d'information de plus en plus complexes :
 - Utilisant de multiples services (serveurs de bases de données, serveurs Web, serveurs de fichiers, messageries,...)
 - Nécessitant de nombreuses authentifications
 - Comportant de nombreux bugs logiciels et matériels
 - Manquant d'expertise
 - De plus en plus virtualisés
 - Vulnérables aux failles humaines (ingénierie sociale)

Pourquoi est-ce si complexe ?

- . Globalement des SI complexes à construire et à gérer MAIS une simple faille peut leur être fatale :
 - Les pirates n'ont souvent besoin que de trouver une faille,
 - Les outils de hacking sont distribués gratuitement et sont de plus en plus puissants,
 - Les moteurs de recherche permettent de récupérer toujours plus d'informations,
 - Les bases d'exploits et les codes associés sont facilement récupérables (**léggalement**) sur Internet.

Pourquoi est-ce si complexe ?

- L'ingénierie sociale est plus simple qu'il n'y paraît
- Les utilisateurs finaux sont mal informés et généralement sous-estiment ce qui peut être fait
- Les administrateurs systèmes et réseaux ne sont pas toujours conscients des risques
- La sécurité coûte et demande un investissement constant
- La sécurité demande une synchronisation continue et importante de beaucoup (trop) d'acteurs

Les 5 risques majeurs selon l'ANSSI

- L'espionnage : des groupes organisés s'introduisent dans les systèmes les plus critiques
- Les attaques indirectes : exploitation des partenaires de confiances
- Les opérations de déstabilisation et d'influence
- Opérations clandestines sur la cryptomonnaie
- La fraude en ligne

Un monde de vulnérabilités (potentielles)



89

Exercice

- Par groupe, essayez de déterminer les risques de sécurité les plus importants pour vous :
 - Sur une machine,
 - Sur un réseau

90



La sécurité des systèmes

The image is a word cloud centered around the term "OPERATING SYSTEM". Other prominent words include "HARDWARE", "SOFTWARE", "PROGRAMS", "COMPUTER", and "SYSTEM". The words are in various sizes and colors (black, orange, red, grey) and are arranged in a circular, radiating pattern.

Les menaces sur les systèmes d'exploitation

- Le système d'exploitation permet
 - De gérer l'utilisation des ressources physiques d'une machine
 - De fournir une interface avec l'utilisateur
- C'est un système complexe :
 - Multiplicité des composants
 - Spécificité des programmes utilisés
 - Diversité des usages
- Des failles existent et sont régulièrement exploitées

Les types de menaces

- Les malwares : virus, vers, troyens, rootkits
- Les dénis de service (DoS) :
 - Surcharge du système (ou de son accès réseau) afin de l'empêcher de fonctionner normalement
 - Blocage ou plantage d'un service critique au fonctionnement du système
 - Blocage des accès aux données
- L'intrusion : accès illégitime à un système
 - Usurpation d'identité
 - Cassage de mot de passe
 - Utilisation de vulnérabilités
- L'utilisation en tant que « bot »

Botnets: nombre = puissance

Critical Password Warning— 2.8 Million Devices Used In New Hack Attack

According to the [Shadowserver Foundation](#), which describes itself as “a nonprofit security organization working altruistically behind the scenes to make the Internet more secure for everyone,” an ongoing brute force password attack has ramped up the volume to 11 and is now employing up to 2.8 million compromised devices every day to facilitate the attacks against Palo Alto Networks, Ivanti, and SonicWall network edge security devices such as VPNs and firewalls. A Shadowserver Foundation [X posting](#) confirmed that there had been a “large increase in web login brute-forcing attacks against edge devices seen last few weeks in our honeypots.”

Source : <https://www.forbes.com/sites/daveywinder/2025/02/10/critical-password-warning-28-million-devices-used-in-new-hack-attack/>

• Source : <https://www.cvedetails.com/top-50-products.php?year=2023>

Quelques chiffres (2023)

Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2023

Go to year: [2013](#) [2014](#) [2015](#) [2016](#) [2017](#) [2018](#) [2019](#) [2020](#) [2021](#) [2022](#) [2023](#) [All Time Leaders](#)

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Android	Google	OS	915
2	Windows Server 2022	Microsoft	OS	420
3	Windows Server 2019	Microsoft	OS	401
4	Windows Server 2016	Microsoft	OS	375
5	Windows 11 21h2	Microsoft	OS	373
6	Windows 10 1809	Microsoft	OS	362
7	Windows 10 21h2	Microsoft	OS	360
8	Windows 11 22h2	Microsoft	OS	359
9	Windows 10 22h2	Microsoft	OS	355
10	Windows Server 2012	Microsoft	OS	343
11	Windows 10 1607	Microsoft	OS	333
12	Windows Server 2008	Microsoft	OS	264
13	Linux Kernel	Linux	OS	247
14	Macos	Apple	OS	238
15	Windows 10 20h2	Microsoft	OS	229
16	Fedora	Fedoraproject	OS	228
17	Chrome	Google	Application	228

La sécurité des réseaux



96

96

Tout (ou presque) est connecté...

- Le monde numérique moderne dépend du (bon) fonctionnement des réseaux
- Les réseaux sont constitués de composants spécifiques susceptibles d'être attaqués
- Les composants interconnectés peuvent être pris pour cible
- Les attaques peuvent être réalisées à distance ou via un périphérique compromis (notion de pivot ou de relais)

Quelques menaces classiques sur les réseaux

- **Écoutes du réseau** pour capter les données non sécurisées
- Le déni de service (**DoS**) ou le déni de service distribué (**DDoS**)
Objectifs : paralyser le fonctionnement normal d'un service
- **Les intrusions**
Objectifs : pénétrer un réseau pour obtenir des accès illégitimes à des ressources internes
- Les attaques "**Man-in-the-Middle**"
Objectifs :
 - Bloquer l'accès à des services
 - Intercepter des données
 - Modifier des transactions
 - Rediriger l'utilisateur vers un site pirate

Le top 10 du “Bad Practice”

Through NSA and CISA Red and Blue team assessments, as well as through the activities of NSA and CISA Hunt and Incident Response teams, the agencies identified the following 10 most common network misconfigurations:

1. Default configurations of software and applications
2. Improper separation of user/administrator privilege
3. Insufficient internal network monitoring
4. Lack of network segmentation
5. Poor patch management
6. Bypass of system access controls
7. Weak or misconfigured multifactor authentication (MFA) methods
8. Insufficient access control lists (ACLs) on network shares and services
9. Poor credential hygiene
10. Unrestricted code execution

Études de cas : Le WiFi

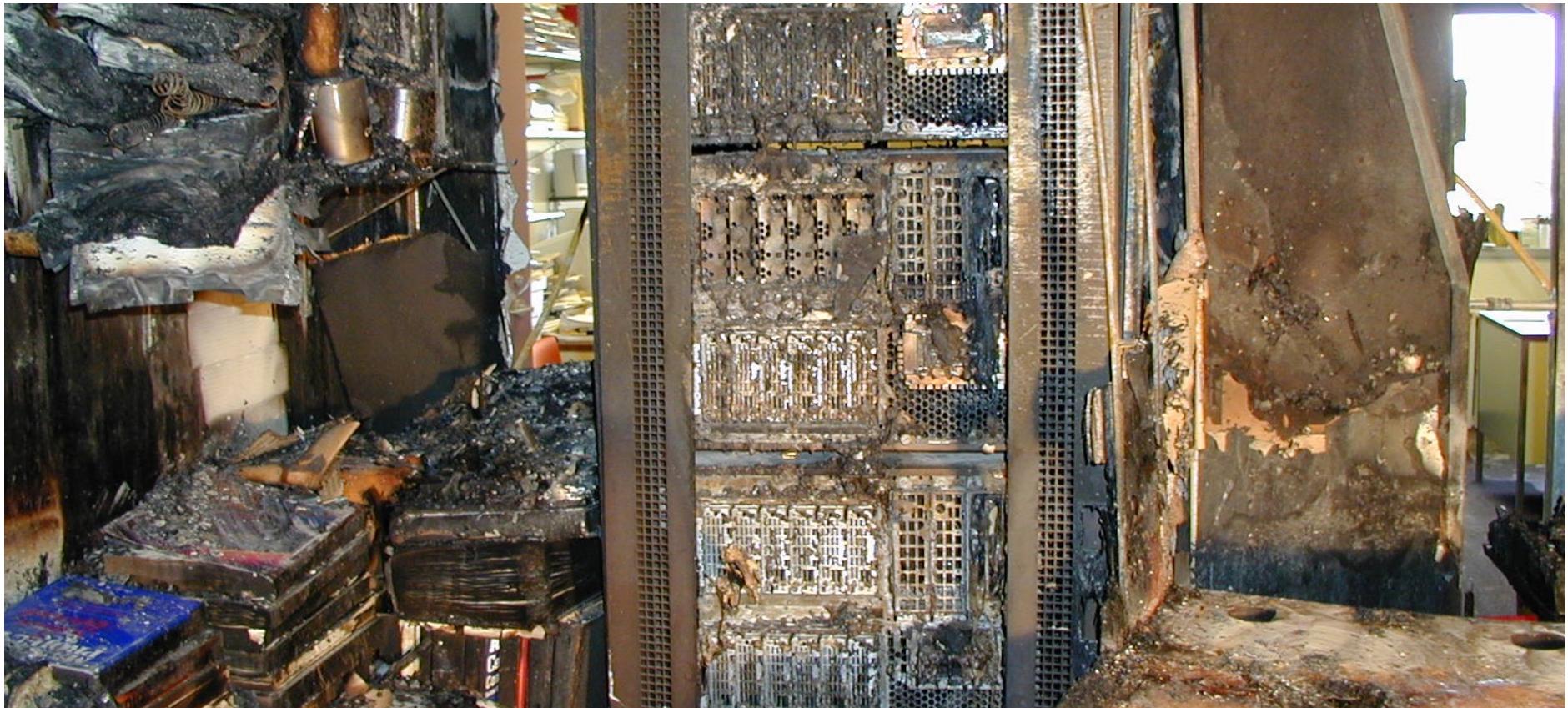
- Connexion à un réseau non sécurisé : type WiFi public
 - Écoute de trafic non chiffré
 - Mise en place d'un faux point de connexion
 - Exemple en vidéo
 - <https://www.youtube.com/watch?v=1OVTrXGHyU>

La sécurité physique



101

La sécurité incendie



102



La sécurité physique

- Protection incendie
 - Moyens techniques
 - Séparation des zones sensibles

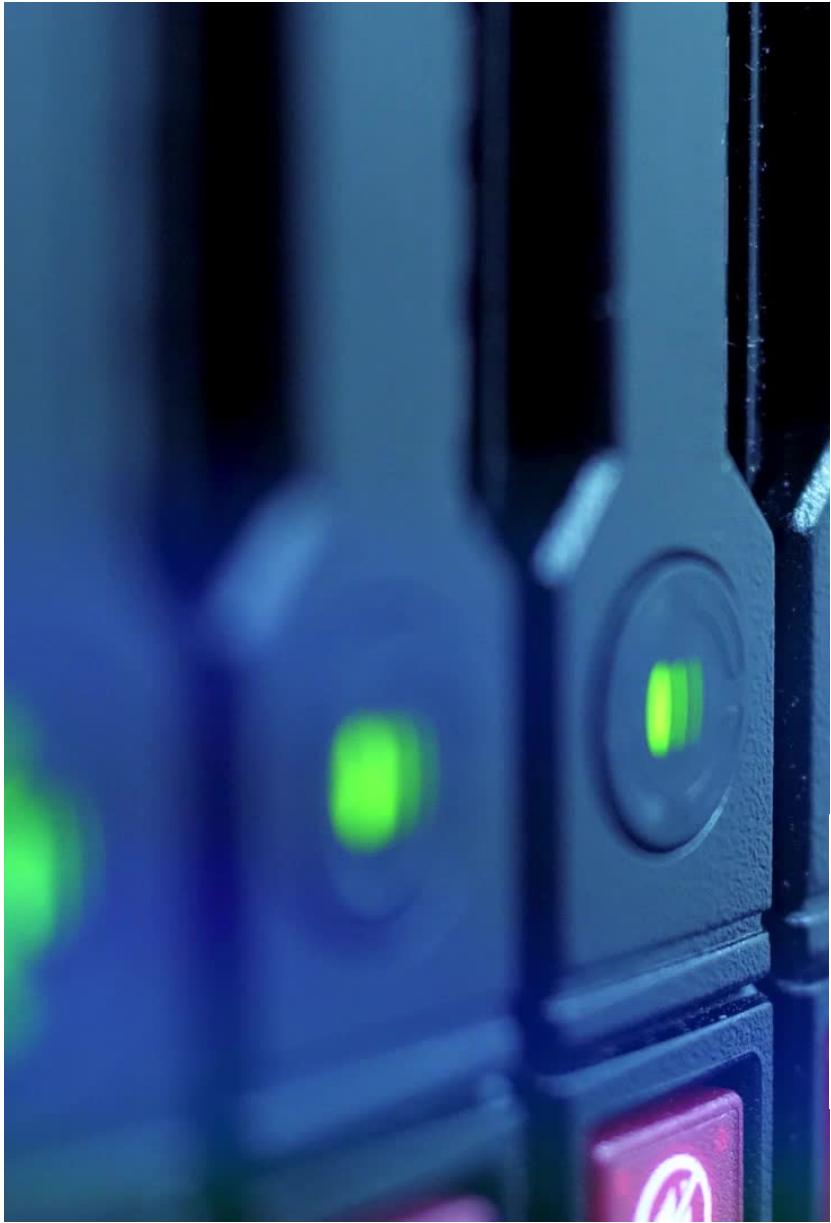


La sécurité électrique



104





La sécurité électrique

- Alimentation électrique
 - Onduleurs et groupes électrogènes
 - Arrêt automatique des serveurs
 - Redondance électrique



La sécurité du câblage



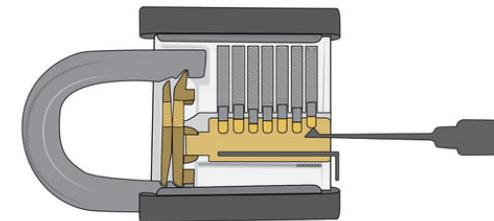
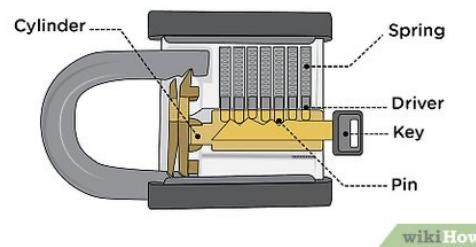
106



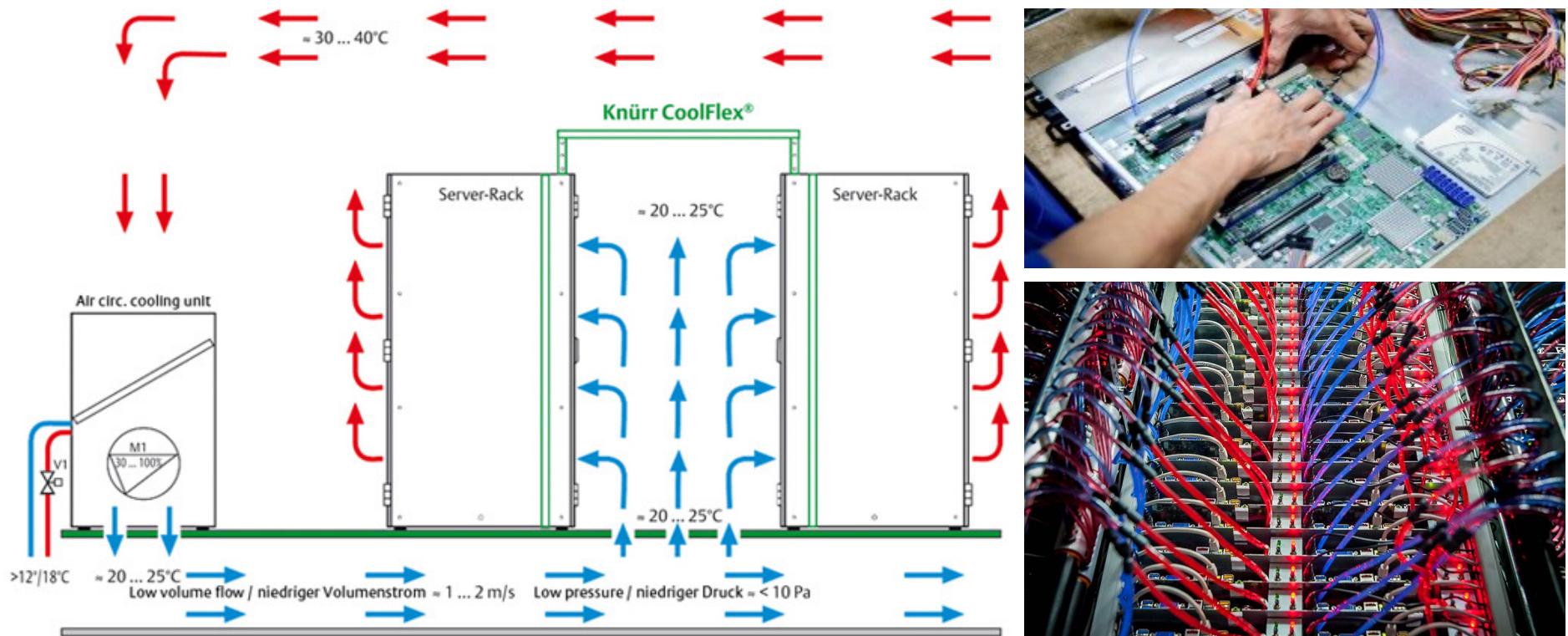
La sécurité des accès



- Accès aux bâtiments / locaux
 - Les accès par clés
 - Les accès par badge



La sécurité en température



La sécurité physique... un faux problème ?

Le récit d'une attaque "Red Team" sur le réseau électrique US

<https://www.youtube.com/watch?v=pL9q2IOZ1Fw&t=124s>

Les étapes classiques d'une attaque



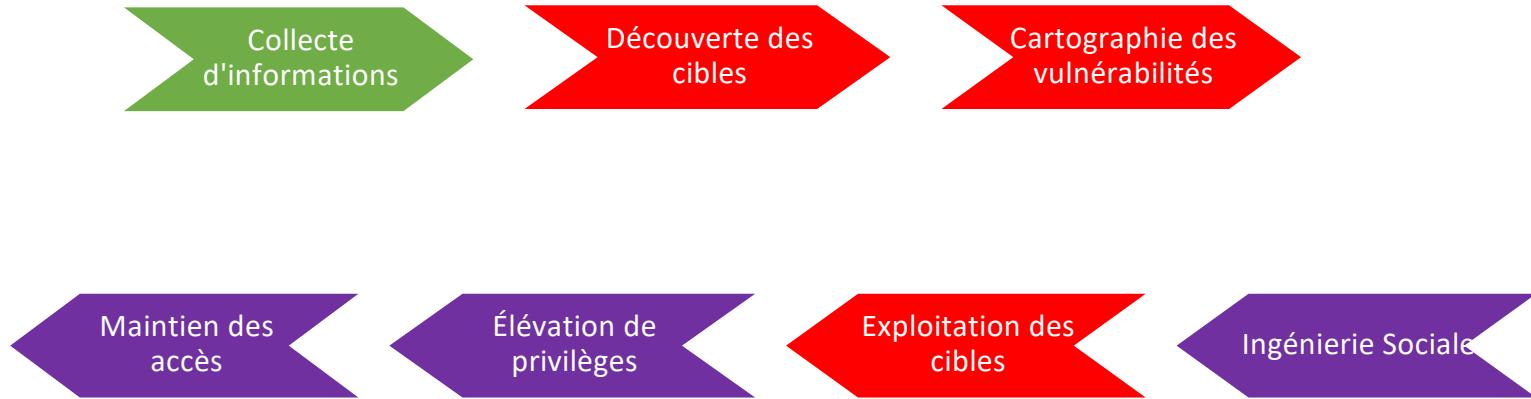
L'art de la guerre

Sun Tzu
(544–496 av. J.-C.)



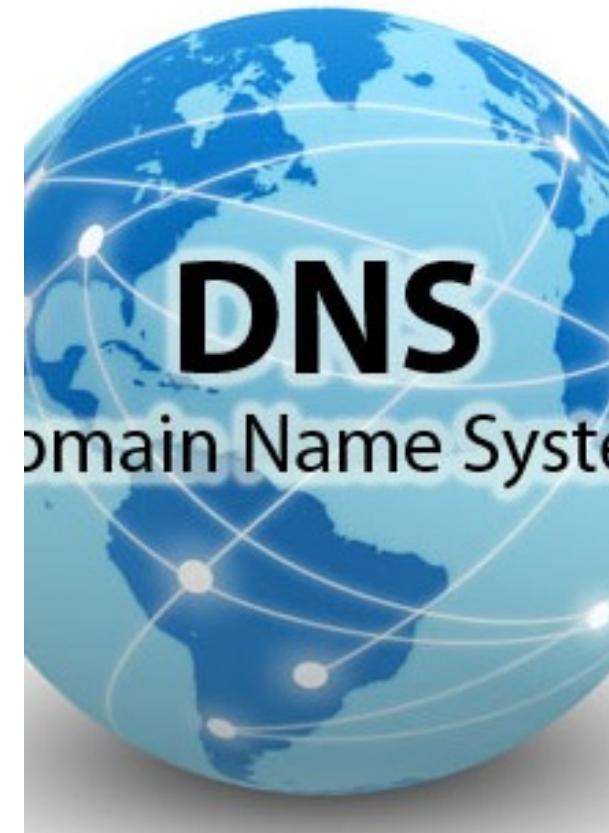
111





Collecte d'informations

- Utilisation de ressources Internet spécialisées :
- Serveurs DNS,
- Base de données Whois,
- Adresses courriels,
- Comptes utilisateurs,
- Routage réseau,...



113

Collecte d'informations

La collecte d'informations n'est pas forcément (très) technique :

Utilisation des ressources Internet « globales » :

Moteurs de recherche : Google, Yahoo, Bing,...

Utilisation de google dorks
(<https://www.stationx.net/google-dorks-cheat-sheet/>)

Utilisations de ressources Internet spécifiques :

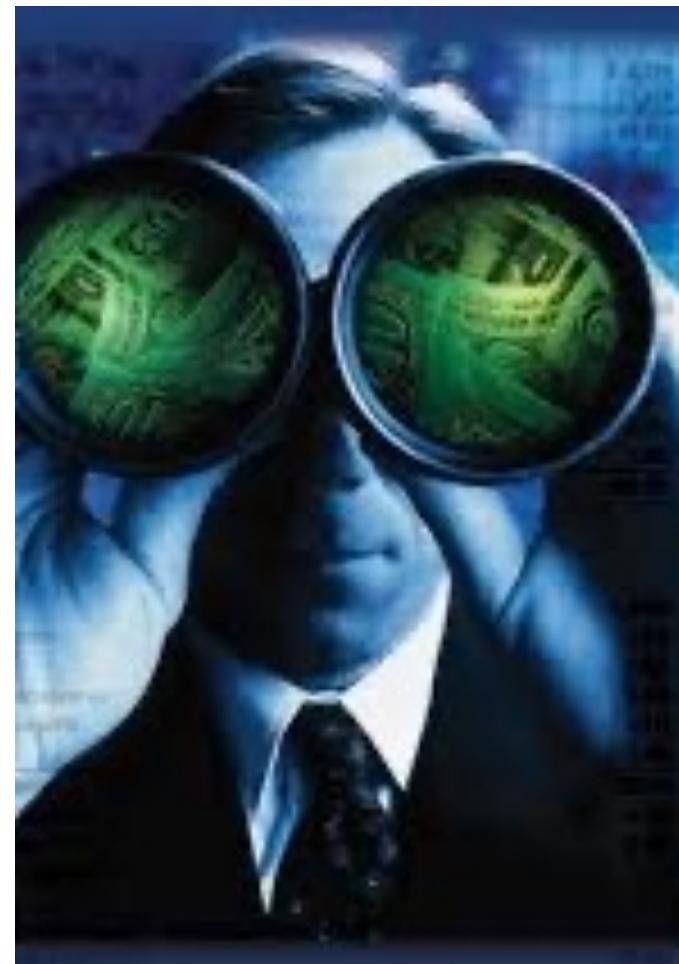
Forums,

Newsgroups,

Articles et sites Web,

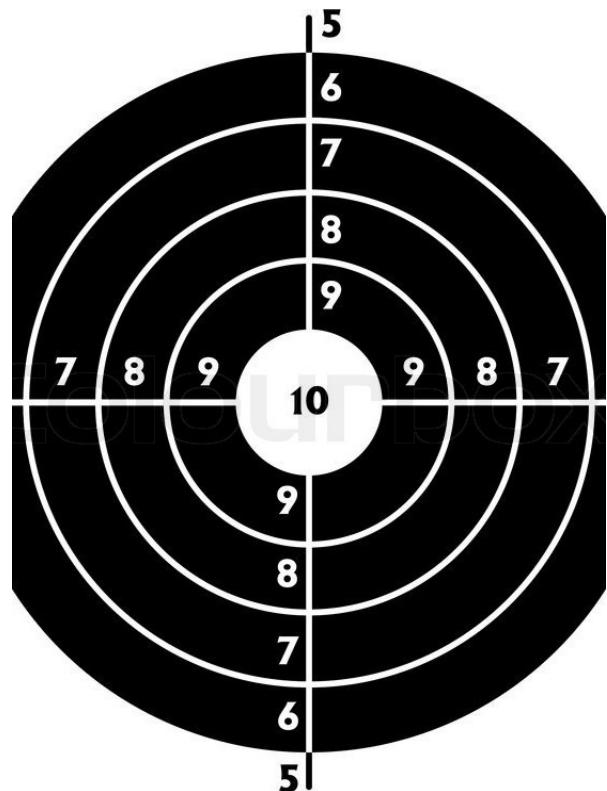
Blogs,

Réseaux sociaux...



114

Découverte des cibles



- L'objectif principal de cette phase est :
- D'identifier les cibles disponibles sur le réseau,
- D'identifier les systèmes d'exploitation utilisés,
- De déterminer les architectures réseaux,
- De déterminer le rôle des différentes cibles identifiées.

115



Cartographie des vulnérabilités

Avec les étapes précédentes, suffisamment d'informations devraient être disponibles pour passer à une étape (encore) plus active.

En utilisant les services découverts sur les différentes cibles, le hacker va maintenant essayer de trouver des vulnérabilités connues qui y sont associées



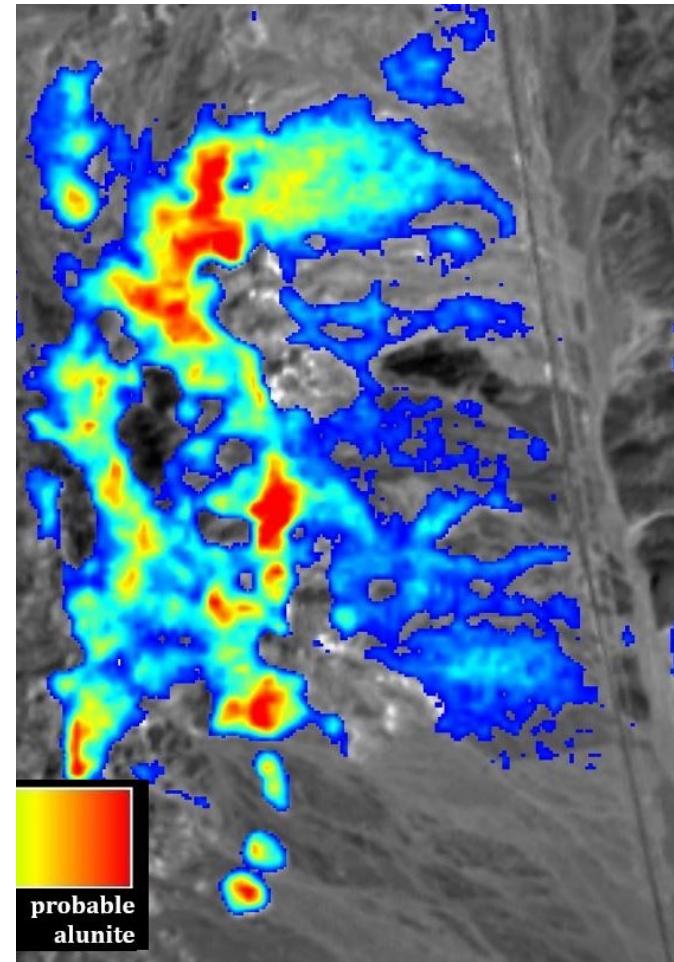
116

Cartographie des vulnérabilités

Des attaques spécifiques peuvent alors être réalisées :

Automatiquement à partir d'applications dédiées,

Manuellement en utilisant des outils dédiés à certains types de vulnérabilités ou spécifiquement créés ou adaptés par le hacker.



117

Ingénierie Sociale

- Dans certaines situations, cette étape est une phase clé dans le travail du hacker. L'ingénierie sociale utilise l'être humain comme un vecteur d'attaque.
- Différentes méthodes standards sont utilisées :
- Usurpation d'identité,
- Phishing,
- Attaques Man In The Middle,
- Faux sites,
- ...
- Ces méthodes sont généralement basées sur la psychologie humaine





Ne sous-estimez
jamais la puissance
de l'ingénierie
sociale !

Quand nos données nous échappent...

Nous pouvons également être des victimes indirectes :
<https://www.youtube.com/watch?v=yIG4kTJTZuY>

L'Exploitation des cibles

- Selon les résultats des phases précédentes différents objectifs peuvent, à ce stade, être définis :
 - Obtenir un accès non-privilégié,
 - Obtenir un accès privilégié,
 - Réaliser une attaque DOS sur un service,
 - Réaliser une attaque DOS sur la cible,
 - Réaliser une attaque DOS sur le réseau,
 - Etc.



121

L'Élévation des privilèges

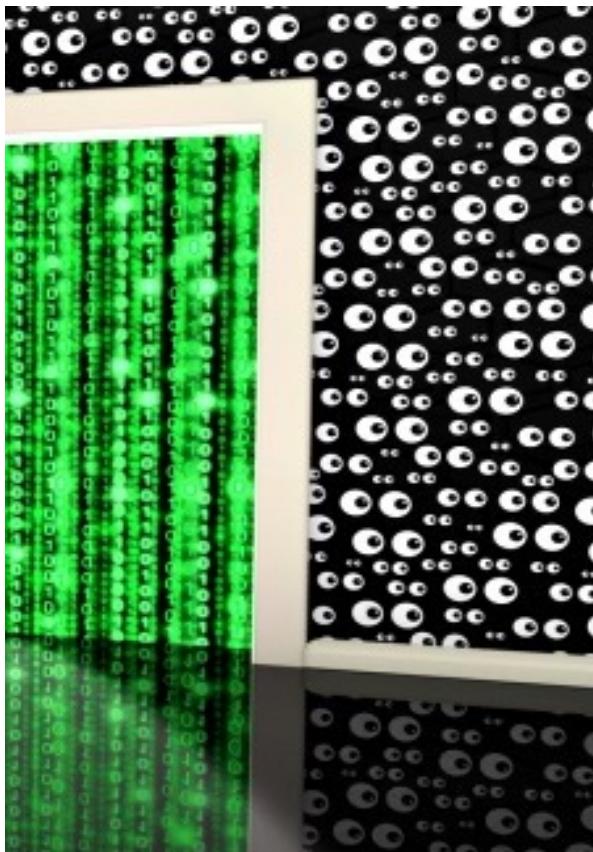
Si le hacker a pu obtenir un accès non privilégié à une cible, il peut essayer d'obtenir des droits supérieurs.

Selon le système d'exploitation, les services et programmes actifs, le niveau de correction, ... différents exploits et différentes approches peuvent alors être essayées.



122

Le Maintien des accès



- Dans certains cas, le hacker va essayer de maintenir un accès obtenu sur une cible.
- Différentes techniques peuvent être utilisées telles que :
 - Les Backdoors,
 - Les shells distants,
 - Les shells distants inversés,
 - Les méthodes de tunneling,
 - Les rootkits,
 - Etc.

123

Les préconisations



132



Les préconisations de l'ANSSI

- CHOISISSEZ AVEC SOIN VOS MOTS DE PASSE
 - Définissez des mots de passe composés d'au moins 14 caractères
 - mélangeant majuscules, minuscules, chiffres et caractères spéciaux
 - n'ayant aucun lien avec vous comme votre nom, date ou lieu de naissance
 - ne formant pas de mots figurant dans le dictionnaire

Source : <https://www.gouvernement.fr/risques/conseils-aux-usagers>

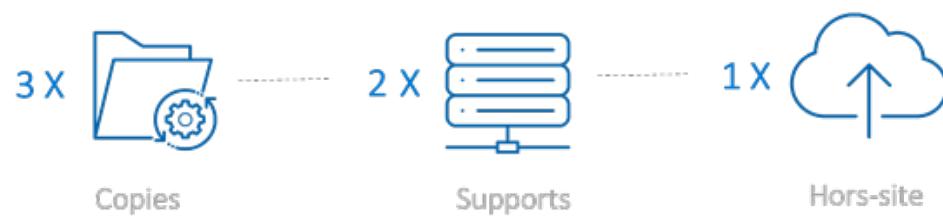
Les préconisations de l'ANSSI

- Utilisez un principe de moindres privilèges
 - Pour vos machines,
 - Pour vos applications
- Toute action doit être faite avec le moins de privilèges possibles
- Le compte Administrateur (ayant tous les droits) est
 - Le compte initial pour instaurer la politique de droits
 - Le compte de dernier recours (s'il est nécessaire).

Source : <https://www.gouvernement.fr/risques/conseils-aux-usagers>

Les préconisations de l'ANSSI

- ENTRETENEZ RÉGULIÈREMENT VOS APPAREILS NUMÉRIQUES
 - En mettant à jour régulièrement les logiciels de vos appareils numériques
 - Effectuer des sauvegardes régulières (quotidiennes ou hebdomadaires par exemple) permet de disposer de ses données après un dysfonctionnement ou une panne d'ordinateur



Source : <https://www.gouvernement.fr/risques/conseils-aux-usagers>

Les préconisations de l'ANSSI

- PRENEZ SOIN DE VOS INFORMATIONS PERSONNELLES ET DE VOTRE IDENTITÉ NUMÉRIQUE
 - Soyez vigilant vis-à-vis des formulaires que vous êtes amenés à remplir : ne transmettez que les informations strictement nécessaires et **pensez à décocher les cases qui autoriseraient le site à conserver ou à partager vos informations, par exemple avec des partenaires commerciaux**
 - Ne donnez accès qu'à un minimum d'informations personnelles sur les réseaux sociaux
 - Utilisez plusieurs adresses électroniques dédiées à vos différentes activités sur Internet : une adresse réservée aux activités dites sérieuses (banques, recherches d'emploi, activité professionnelle...) et une adresse destinée aux autres services en ligne (forums, jeux concours...)

Source : <https://www.gouvernement.fr/risques/conseils-aux-usagers>

Les préconisations de l'ANSSI

- PROTÉGEZ VOS DONNÉES PENDANT VOS DÉPLACEMENTS
 - Précautions à prendre avant de partir en mission
 - Utilisez le matériel dédié à la mission prêté par votre entreprise (ordinateur, clefs USB, téléphone) ;
 - Sauvegardez aussi vos données sur un support amovible pour les retrouver en cas de perte ;
 - Si vous comptez profiter des trajets pour travailler, emportez un filtre de protection écran pour votre ordinateur ;
 - Apposez un signe distinctif (comme une pastille de couleur) sur vos appareils pour vous assurer qu'il n'y a pas eu d'échange pendant le transport.

Les préconisations de l'ANSSI

- PROTÉGEZ VOS DONNÉES PENDANT VOS DÉPLACEMENTS
 - Pendant la mission
 - Gardez vos appareils, supports et fichiers avec vous, pendant votre voyage comme pendant votre séjour (ne les laissez pas dans un bureau ou un coffre d'hôtel) ;
 - Si vous êtes contraint de vous séparer de votre téléphone, retirez la carte SIM ;
 - En cas d'inspection ou de saisie de votre matériel par des autorités étrangères, informez votre organisation ;
 - N'utilisez pas les équipements que l'on vous offre si vous ne pouvez pas les faire vérifier par un service de sécurité de confiance ;
 - Évitez de connecter vos équipements à des postes qui ne sont pas de confiance. Par exemple, si vous avez besoin d'échanger des documents à l'occasion d'une présentation.

Source : <https://www.gouvernement.fr/risques/conseils-aux-usagers>

Les préconisations de l'ANSSI

- SÉCURISEZ VOTRE WI-FI
- Quelques recommandations générales :
 - Modifiez le nom d'utilisateur et le mot de passe par défaut (généralement « admin » et « 0000 ») de votre page de configuration accessible via votre navigateur Internet
 - Vérifiez que votre « box » dispose du protocole de chiffrement WPA2 (ou supérieur) et activez-le. Sinon, utilisez la version précédente WPA-AES (ne jamais utiliser le chiffrement WEP cassable en quelques minutes)
 - Modifiez la clé de connexion par défaut avec une clé (mot de passe) de plus de 20 caractères de types différents (cf. choisissez des mots de passe robustes)
 - Ne divulquez votre clé de connexion qu'à des tiers de confiance et changez-la régulièrement
 - Note personnelle : Si possible créez un réseau Guest en coupant les accès entre machines
 - Activez et configurez les fonctions pare-feu / routeur.
 - Désactivez le « wi-fi » de votre borne d'accès lorsqu'il n'est pas utilisé

Source : <https://www.gouvernement.fr/risques/conseils-aux-usagers>

Les préconisations de l'ANSSI

- SÉPAREZ VOS USAGES PERSONNELS DES USAGES PROFESSIONNELS
- Les usages et les mesures de sécurité sont différents sur les équipements de communication (ordinateur, ordiphone,...) personnels et professionnels.
- Dans ce contexte, il est recommandé de séparer vos usages personnels de vos usages professionnels :
 - Ne faites pas suivre vos messages électroniques professionnels sur des services de messagerie utilisés à des fins personnelles
 - Ne stockez pas de données professionnelles sur vos équipements communicants personnels

Source : <https://www.gouvernement.fr/risques/conseils-aux-usagers>

Les préconisations de l'ANSSI

- SOYEZ AUSSI PRUDENT AVEC VOTRE SMARTPHONE OU VOTRE TABLETTE QU'AVEC VOTRE ORDINATEUR
 - N'installez que les applications nécessaires et vérifiez à quelles données elles peuvent avoir accès avant de les télécharger (informations géographiques, contacts, appels téléphoniques...). Certaines applications demandent l'accès à des données qui ne sont pas nécessaires à leur fonctionnement : il faut éviter de les installer
 - En plus du code PIN qui protège votre carte téléphonique, utilisez un schéma ou un mot de passe pour sécuriser l'accès à votre terminal et configurez votre téléphone pour qu'il se verrouille automatiquement
 - Effectuez des sauvegardes régulières de vos contenus sur un support externe pour pouvoir les retrouver en cas de panne de votre ordinateur ou smartphone

Les préconisations de l'ANSSI

- SOYEZ PRUDENT LORSQUE VOUS OUVREZ VOS MESSAGES ÉLECTRONIQUES
- Lorsque vous recevez des courriels, prenez les précautions suivantes :
 - L'identité d'un expéditeur n'est en rien garantie : vérifiez la cohérence entre l'expéditeur présumé et le contenu du message
 - N'ouvrez pas les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que vous envoient habituellement vos contacts
 - Si un lien ou plusieurs figurent dans un courriel, vérifiez l'adresse du site en passant votre souris sur chaque lien avant de cliquer. L'adresse complète du site s'affichera alors dans la barre d'état en bas de la page ouverte. Si vous avez un doute sur l'adresse affichée, abstenez-vous de cliquer
 - Ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles (ex : code confidentiel et numéro de votre carte bancaire)
 - N'ouvrez pas et ne relayez pas de messages de types chaînes de lettre, appels à la solidarité, alertes virales, etc.

Source : <https://www.gouvernement.fr/risques/conseils-aux-usagers>

VOUS AVEZ UN DOUTE SUR LE MESSAGE QUE VOUS AVEZ REÇU ?

- ❖ **N'ayez pas peur !** Vous n'avez sans doute rien de compromettant à vous reprocher
- ❖ **N'ouvrez pas de liens ou de pièces jointes** sans être sûr de la fiabilité de son expéditeur
- ❖ **Vérifiez l'adresse de l'expéditeur** : contactez-le par un autre canal. Un organisme officiel aura presque systématiquement une adresse mail de type "ne-pas-repondre@ministere.gouv.fr"
- ❖ **Ne répondez à aucun mail suspect** ou à du **chantage** pour ne pas montrer à l'expéditeur que vous êtes réceptif au message
- ❖ Faites des **captures d'écran** et **signalez le mail** sur le site : www.signal-spam.fr
- ❖ Si l'escroquerie que vous souhaitez signaler vous est parvenue par SMS, **transférez-le** au numéro 33700
- ❖ **Supprimez le message**

Les préconisations de l'ANSSI

- SOYEZ VIGILANT PENDANT VOS ACHATS EN LIGNE
 - Avant d'effectuer un paiement en ligne, il est nécessaire de procéder à des vérifications sur le site :
 - Contrôlez la présence d'un cadenas dans la barre d'adresse ou en bas à droite de la fenêtre de votre navigateur (remarque : ce cadenas n'est pas visible sur tous les navigateurs) ;
 - Assurez-vous que la mention « https:// » apparait au début de l'adresse du site ;
 - Vérifiez l'exactitude de l'adresse du site Internet en prenant garde aux fautes d'orthographe par exemple.
 - Note personnelle : ce n'est pas parce que vous avez le « cadenas » que la connexion est **valide (c.f. Use case vu plus tard dans le cours)**

Source : <https://www.gouvernement.fr/risques/conseils-aux-usagers>

Les préconisations de l'ANSSI

- TÉLÉCHARGEZ LES PROGRAMMES, LOGICIELS SUR LES SITES OFFICIELS DES ÉDITEURS
 - Si vous téléchargez du contenu numérique sur des sites Internet dont la confiance n'est pas assurée, vous prenez le risque d'enregistrer sur votre ordinateur des programmes ne pouvant être mis à jour, qui le plus souvent contiennent des virus ou des chevaux de Troie.

Source : <https://www.gouvernement.fr/risques/conseils-aux-usagers>

Zoom : La sécurité de vos appareils mobiles

- Votre appareil mobile est devenu un outil indispensable pour votre vie de tous les jours : gestion des contacts, des mails, des opérations bancaires, des autorisations, des preuves de vaccination,...
- Quelques règles de base pour le protéger :
 - Mettez en place un code d'accès
 - Si disponible, activez les chiffrement des données
 - Appliquez les mises à jours
 - Faites des sauvegardes
 - Utilisez un antivirus
 - N'installez pas n'importe quoi
 - Contrôler les autorisations de vos applications
 - Ne vous connectez pas à des réseaux publics ou inconnus (sans protection)
 - Conserver le code IMEI de votre appareil (*#06# pour le récupérer)
 - Ne laissez pas votre appareil sans surveillance

146

La sécurité n'est jamais un absolu!
C'est juste une question de temps!

