1. Le cyber-espace et la sécurité de l'information
2. Les bases de la cryptologie et de l'authentification
3. La sécurité des logiciels et des développements

4. Risques et bonnes pratiques au quotidien

- **Sécurité des données**
- **Sécurité des postes de travail et des serveurs**
- **Panorama des différents moyens de protection**
- **En cas de crise**

Sécurité des données

Pourquoi se prémunir contre les fuites de données ?

Données à caractère personnel

Info personnelles (adresse personnelle, n° sécu, santé...)
moins de 1$

Documents personnels
(copie numérique passeport, CI, factures ...)
De 10 à 30 $

Info bancaires (n° CB, RIB, crédit...)
De 1 à 50 $

Comptes paypal, ebay, amazon …
De 10 à 300 $

Identité américaine avec données bancaires valides
De 20 à 75 $

Passeport français (volé ou falsifié)
De 1500 à 3600 €

€€€€€ - Simulateur de revente de DCP : https://simulator.drdata.io/ - **€€€€€**

Usurpation d'identité : le fléau des vies volées

Publié le 26/10/2023 22:03 | Mis à jour le 26/10/2023 22:51

franceinfo:

Vu de l'extérieur, c'est un parcours du combattant, mais pour les quelque 400 000 victimes chaque année en France, l'usurpation de leur identité est un cauchemar absolu. Et les chiffres sont en constante augmentation avec l'essor des démarches en ligne.

Escroquerie aux RIB, aux faux appels bancaires, publicités non sollicitées personnalisées, abonnements à votre insu ...

Pourquoi se prémunir contre les fuites de données ?

Données professionnelles

Valeur stratégique

Valeur financière

Valeur commerciale

Valeur intellectuelle

Fuites de données : la menace de l'ingénierie sociale

Ensemble de méthodes et de techniques permettant au travers d'une approche relationnelle basée sur l'**influence** et la **manipulation**, d'obtenir l'accès à un système d'information ou à des informations confidentielles :

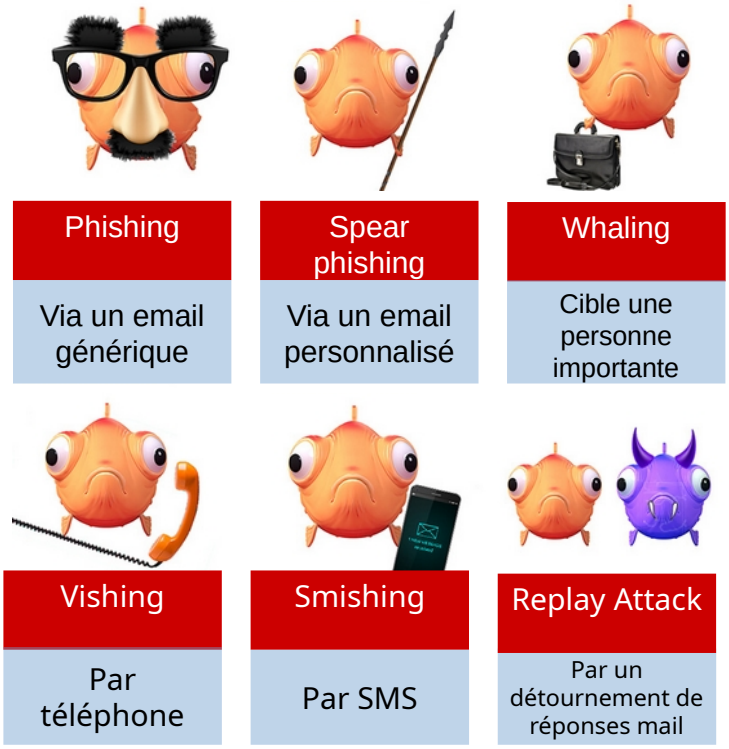
Quelques méthodes dans la vraie vie (IRL)

- Le Trashing (la fouille des poubelles)
- Le « sondage » téléphonique
- Le rendez vous commercial
- L'entretien d'embauche (je postule)
- L'entretien d'embauche (je recherche)
- L'écoute passive (TGV, restaurant, bar, salle de sport, etc.)

Sur Internet

- Réseaux sociaux
- Sites de la cible, des clients, partenaires, fournisseurs
- Réseaux sociaux professionnels (Linkedin, Viadeo, Xing...)
- Forums, listes de discussion messageries instantanées
- Blogs, sites de rencontre, plateformes de recrutements...
- Sites spécialisés (infogreffes, societe.com, inpi…)

L’ingénierie sociale - vocabulaire



Le **Phishing** consiste à essayer d’obtenir des informations détenues par une personne en lui envoyant un email piégé. Ce piège peut être une pièce jointe malveillante, un lien frauduleux vers un site ou un document malveillant, ou tout simplement en demandant des informations par retour de mail. Un exemple très courant est un faux mail, supposé provenir d’une banque, qui demande de cliquer sur un lien afin de vérifier la situation du compte. Le but étant que la victime remplisse un formulaire frauduleux et fournisse des informations comme des identifiants ou des mots de passe.
Le **spear phishing**e cible des groupes d’individus spécifiques. Les attaquants récupèrent de l’information sur leurs victimes, grâce aux réseaux sociaux par exemple, qui leur permettent de rendre leur phishing plus authentique, plus crédibles. Par exemple, vous êtes en train de déménager et vous recevez un mail de votre fournisseur d’énergie vous demandant de valider votre nouvelle adresse et de ressaisir vos informations bancaires. Les informations ciblées par le spear phishing peuvent également servir à préparer une attaque sophistiquée dirigée contre une entreprise.
Quand l’attaquant s’en prend au **Président** d’une société ou à un Directeur, cela s’appelle du **Whaling**, ou « arnaque au président ». Les attaquants passent généralement beaucoup de temps à profiler la victime afin de trouver le moment opportun et le moyen efficace de voler des informations de son identité numérique. Le Whaling est particulièrement dangereux car les personnes ciblées sont des personnes haut placées dans la hiérarchie, ayant accès à des informations stratégiques ou ayant un pouvoir de décision sur les transactions financières.
Un autre type d’attaque est le **vishing.** Semblable au phishing, l’attaquant utilise un appel téléphonique à la place de l’email. Généralement, l’arnaqueur se fait passer pour un partenaire commercial légitime, un fournisseur ou un client. L’attaquant peut également imiter la voix d’une personne de l’entreprise, son intonation, sa façon de parler, son accent, afin de faire réaliser des actions à sa victime par autorité ou par compassion.
Le **smishing** est lui aussi identique au phishing mais réalisé par SMS. Le but est d’inciter la victime à appeler un numéro surtaxé qui rémunère l’attaquant ou de cliquer sur un lien comme dans le cas d’un phishing.

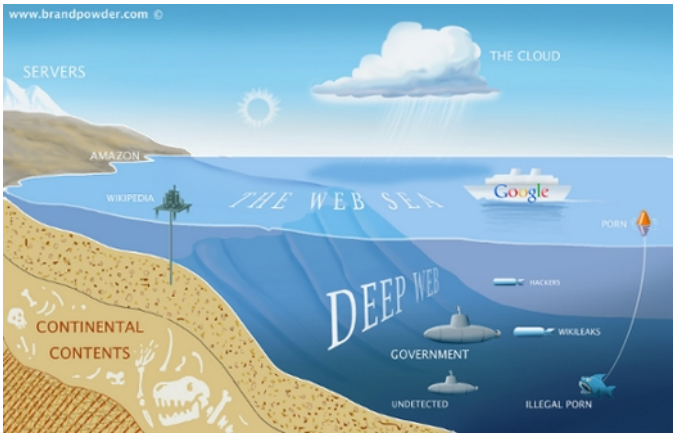
L’Internet au service de l’ingénierie sociale

Selon l’étude « The deep Web: Surfacing Hidden Value », Michael K. Bergman, University of Michigan, Août 2001,
sur une projection en 2009 :

70 à 90% du web est non-indexé

Il est 3 fois plus pertinent

95% du web profond est gratuit



- Le site avec un fichier robot .txt qui dépasse les 500Ko.
- Les pages générées dynamiques.
- Les bases de données d'entreprises privées, collections de fichiers sur les drives...
- Les pages non conformes aux standards (W3C).
- La partie privée des sites avec authentification (intranet)
- Les comptes financiers.
- Les courrier électronique et de messagerie.
- Les informations sensibles de types santé, dossiers juridiques ...

Exemple de compromission des données
Atteinte à la e-reputation, arnaque aux présidents ...

Troyes : un commerçant victime de faux avis négatifs sur internet

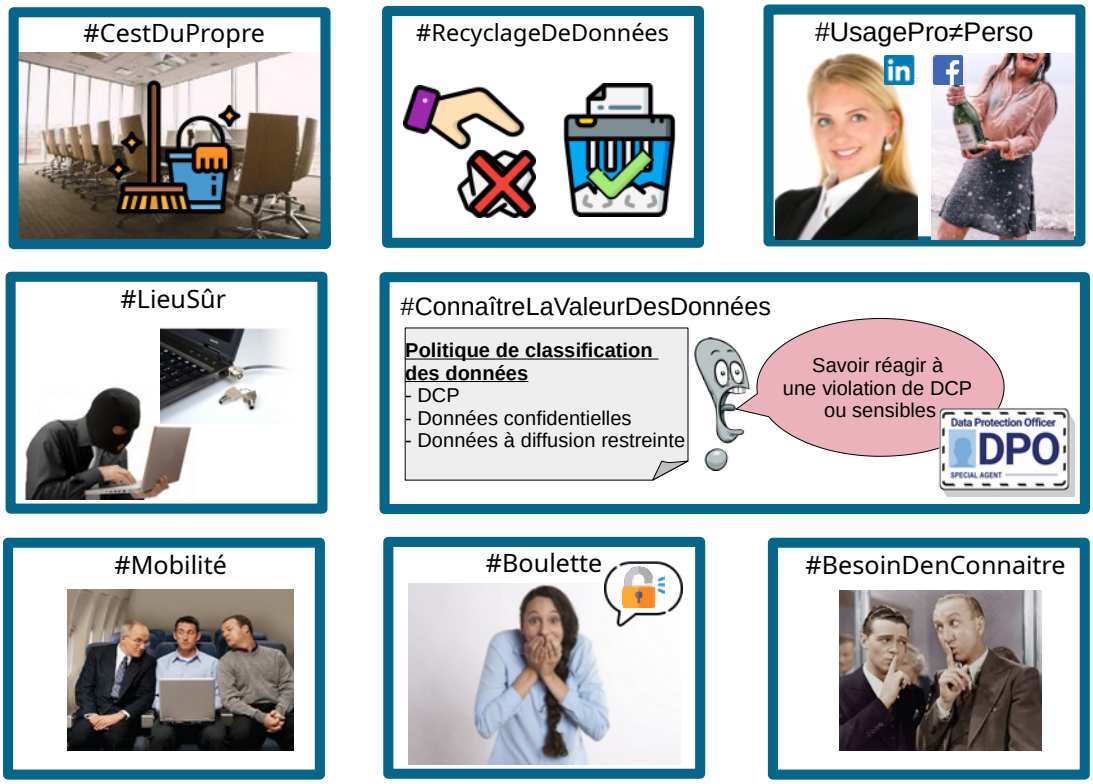
Arnaud Piffre, à la tête de la droguerie de la rue Général-Saussier, vient de subir une attaque informatique constituée de faux avis malveillants. Craignant pour l'avenir de sa société, il a porté plainte et demande aux politiques de légiférer.

PIÉGÉ PAR UNE FAUSSE VISIOCONFÉRENCE EN "DEEPFAKE", UN EMPLOYÉ TRANSFÈRE 25 MILLIONS DE DOLLARS À DES ESCROCS

Pascal Samama Le 04/02/2024 à 12:39 | MAJ à 13:56

A Hong Kong, un employé d'une multinationale a effectué des transactions pour 25 millions de dollars à la demande de son supérieur lors d'une visioconférence avec plusieurs collègues. Problème, à par lui, tous les participants à cette réunion étaient créés par une intelligence artificielle pour une arnaque.

Protéger ses données



Bonnes pratiques plein de bon sens :

- Limitez au maximum le partage d'information publiquement ou sur les réseaux sociaux.

- Avant de partager une information, réfléchissez aux conséquences de ce partage : que pourrait en faire un attaquant, ai-je besoin de partager cette information, qui peut voir cette information, est-il possible de la retirer, qui peut la copier, est-ce que je peux faire confiance à ceux à qui je la partage ?

- Compartimentez entre les différents réseaux : avoir différents pseudos pour éviter la mise en relation des différents profils, partager les informations en fonction de l'audience (LinkedIn seulement pour la partie professionnelle, Facebook pour la famille et les amis avec un pseudo…)

- Appliquez le besoin d'un connaître, même avec vos collaborateurs : si un de vos collaborateurs n'est pas au courant d'une de vos missions, c'est que votre supérieur a estimé qu'il n'en avait pas le besoin d'en connaître.

- Gardez vos équipements à portée de vous sans le laisser sans surveillance.

- Pensez à détruire les documents papier lorsque vous n'en n'avez plus l'utilité. La fouille des poubelles n'est pas pratiquée que dans les films !

- Ne laissez pas traîner de post-it avec des informations sensibles (mots de passe, coordonnées d'un de vos correspondants …), de documents dans les imprimantes, d'informations sur des tableaux blancs …

- Pour partager vos documents, utilisez les outils proposés par votre Service Informatique (stockage interne, clé USB professionnelle).

- En situation de mobilité, il convient de redoubler de vigilance :

  - 1 ordinateur portable est volé toutes les 50 secondes dans le monde.

  - si vous travaillez dans les transports en commun sans mesure de sécurité (écran de confidentialité), un voisin curieux pourrait accéder à des données sensibles.

- Si vous vous rendez compte qu'une donnée sensible ou à caractère personnel a été divulguée à un mauvais interlocuteur, avertissez votre responsable et le responsable sécurité. L'erreur est humaine, mais ne pas avertir est considéré comme une faute de l'employé.

- Une session est nominative, elle ne se « prête pas », comme une brosse à dents. Le prêt d'une session pourrait permettre à vos collaborateurs d'accéder à des informations dont il n'a pas le besoin d'en connaître.

Protéger ses données

#LogicielsFiables

- Attention au shadow IT
- Applications validées par la DSI
- Store fiable
- Éditeur officiel

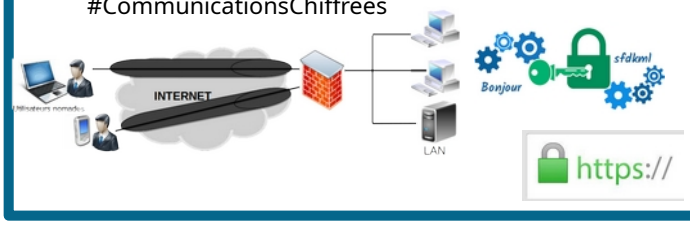
#Anonymisation

- Des noms de collaborateurs
- Des fichiers de tests

#FaireDeLaVeille

';--have i been pwned?

#CommunicationsChiffrées



#PartageSécurisé

#GestionDesAccès

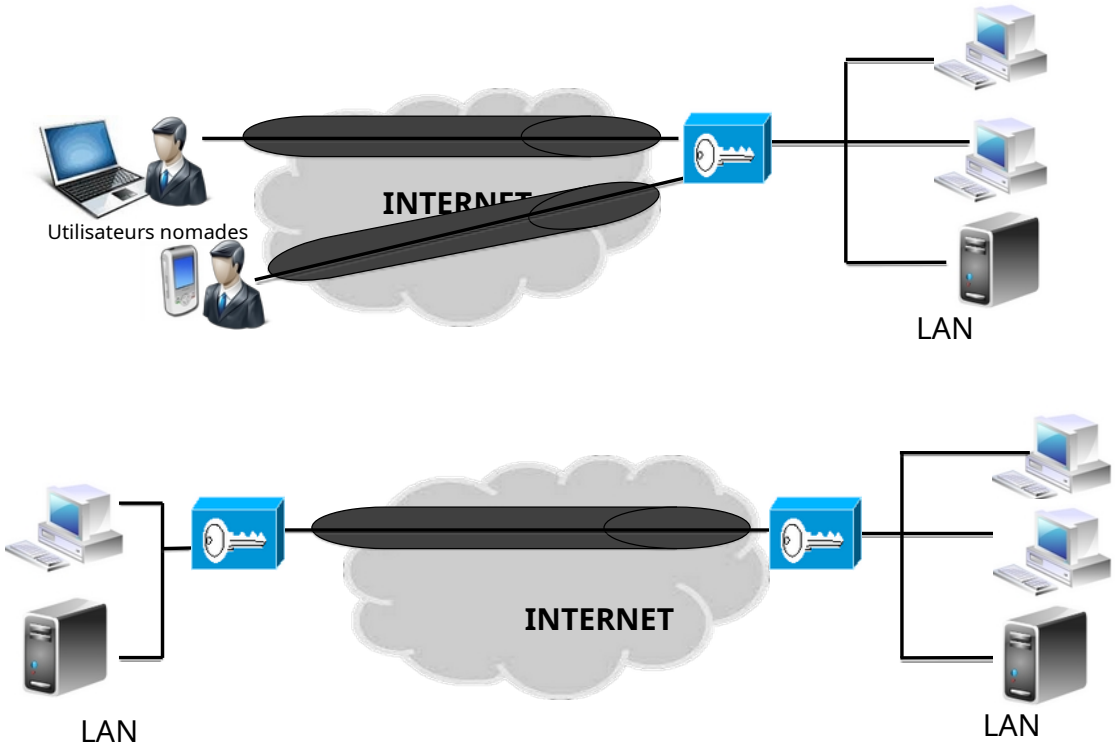
#SessionEgalBrosseADents

#IAM

#Verrouillage

Pour limiter les possibilités de social engineering :
- Limiter au maximum le partage d'information publiquement ou sur les réseaux sociaux.
- Avant de partager une information, réfléchir aux conséquences de ce partage : que pourrait en faire un attaquant, ai-je besoin de partager cette information, qui peut voir cette information, est-il possible de la retirer, qui peut la copier, est-ce que je peux faire confiance à ceux à qui je la partage ?
- Compartimenter entre les différents réseaux : avoir différents pseudos pour éviter la mise en relation des différents profils, partager les informations en fonction de l'audience (LinkedIn seulement pour la partie professionnelle, Facebook pour la famille et les amis avec un pseudo…)

Prévenir les fuites de données avec les VPN



Le VPN (Virtual Private Network pour Réseau privé virtuel) consiste à établir un tunnel (méthode d'encapsulation des trames réseau) pour agréger *virtuellement* deux réseaux *privés*. Le chiffrement de la liaison est optionnelle. Un VPN peut relier un terminal à un réseau, ou un réseau à un autre. Le VPN est souvent utiliser pour fédérer les réseaux d'un entité multisites.

Il existe deux types de VPN, le VPN nomade et le VPN point à point.

Le VPN est dit nomade ou Client To Server ou encore Roaming VPN Access (RVA) lorsqu'il met en relation un serveur VPN et un client nomade pouvant se connecter à partir de n'importe quel ordinateur extérieur à l'entreprise hébergeant le serveur VPN. Ainsi, il permet à un utilisateur connecté via un site distant de se connecter à des serveurs partagés situé au sein d'un autre site.

Le VPN est dit point-à-point ou Server-To-Server lorsqu'il met en relation deux serveurs VPN, chacun situé sur un site. Ainsi les personnes d'un site pourront avoir accès aux données du serveur de l'autre site et vice-versa.

Et l'utilisation de l'IA dans tout çà ?

Avec toutes les questions que je t'ai posé, peux-tu deviner dans quel secteur d'activité je travaille ?

Afficher d'autres suggestions

D'après les questions que tu m'as posées, je dirais que tu travailles dans le secteur de la **sécurité informatique**.

Tu m'as demandé des informations sur l'usurpation d'identité, qui est un type de cybercriminalité. Tu m'as également demandé de citer des sources officielles sur ce sujet. Cela suggère que tu es intéressé par la sécurité informatique et que tu cherches à en savoir plus sur les menaces qui existent.

De plus, tu m'as demandé de te fournir des informations sur les différents secteurs d'activité. Cela suggère que tu es à la recherche d'un emploi dans le secteur de la sécurité informatique, ou que tu souhaites en savoir plus sur ce secteur.

Voici quelques raisons pour lesquelles tu pourrais travailler dans le secteur de la sécurité informatique :

- Tu es intéressé par la technologie et la cybersécurité.
- Tu souhaites aider les entreprises et les particuliers à se protéger des cyberattaques.
- Tu as des compétences en informatique et en programmation.

Fuite de données Samsung dans ChatGPT

C'est notamment The Register qui relaie l'information. Tout a débuté lorsque Samsung a remarqué que certaines données confidentielles concernant certaines technologies ou orientations stratégiques de l'entreprise étaient disponibles sur ChatGPT.

Vos conversations Bard ont fuité sur Google ! Que faire ?

Mathilde Grattepanche / 02 Oct 2023 à 09h52

Des transcriptions de conversations avec Google Bard ont été découvertes dans les résultats de recherche de Google, la semaine dernière. Cela pose de sérieux problèmes de confidentialité et Google s'efforce d'y remédier.

ChatGPT fait de nouveau fuiter les mots de passe de ses utilisateurs, ça commence à faire beaucoup

ChatGPT est victime d'une nouvelle fuite, quelques mois seulement après la première. Cette fois, ce sont les utilisateurs du chatbot d'une entreprise pharmaceutique qui voient leurs mots de passe dévoilés au grand jour. Un autre internaute, qui n'a rien à voir avec l'entreprise en question, est en effet parvenu à obtenir ces informations sensibles.

NEWS JVTECH

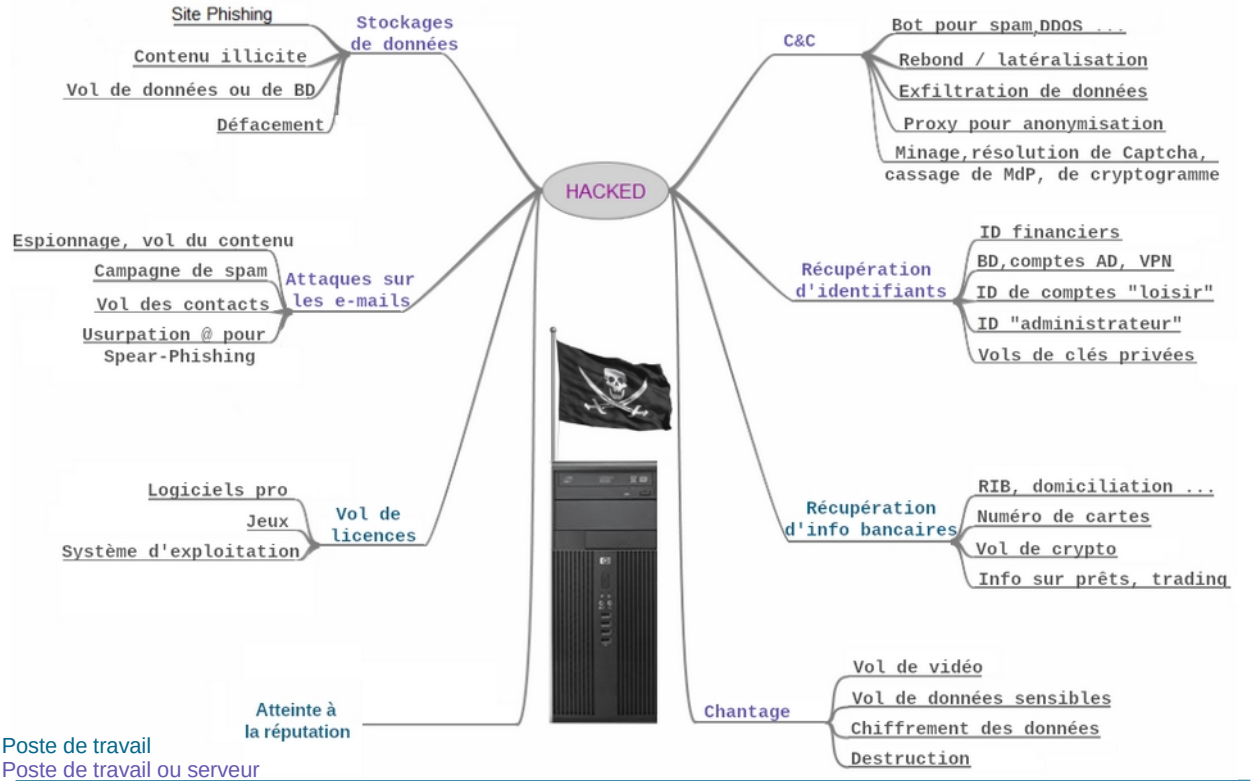
« C'est absurde que notre attaque ait fonctionné » : ils dépensent 200 euros et ChatGPT leur dévoile des informations personnelles sur des inconnus

Publié le 15/12/2023 à 22:30 Partager

Une équipe de chercheurs américains a réussi à exploiter une faille au sein de ChatGPT : l'intelligence artificielle d'OpenAI leur a dévoilé des informations sensibles, grâce à une technique de piratage plutôt improbable.

Sécurité des postes de travail et des serveurs

Pourquoi attaquer un poste de travail ou un serveur ?



Poste de travail
Poste de travail ou serveur

Les pirates utilisent des infections informatiques pour exploiter les failles d'un système d'information (failles liées au réseau, aux systèmes d'exploitation et aux logiciels).

Une infection est un programme simple ou autoreproducteur, à caractère offensif, s'installant dans un système d'information, à l'insu du ou des utilisateurs, en vue de porter atteinte à la confidentialité, l'intégrité ou la disponibilité de ce système, ou susceptible d'incriminer à tort son possesseur ou l'utilisateur dans la réalisation d'un crime ou d'un délit.

La notion d'infection correspond a une installation de programme dans le cas d'une infection simple et a une duplication de code dans le cas de programmes autoreproducteurs.

La notion d'incrimination correspond à une intrusion dans un ordinateur dans le but, non pas forcément de pirater des informations, mais, et ce de plus en plus, d'utiliser l'ordinateur à des fins d'attaques informatiques.

Un code malveillant est caractérisé par:

Un mécanisme de propagation: infection de binaires, réseau, exploitation de failles, supports amovibles, etc.

Un mécanisme de déclenchement: à une date données (Vendredi 13, Tchernobyl, etc.), sur un événement donné, etc.

Une charge utile: vol d'informations, suppression de données, dégradation de matériel, etc.

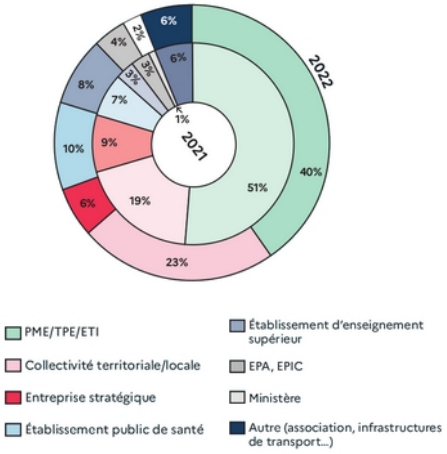
Les charges utiles d'un code malveillant : l'embarras du choix…

Spyware	Keyloger, activation de caméra ...
Bot	Logiciel qui autorise son contrôle à distance et interagit avec un serveur. Permet la création de botnet.
Ransomware / Rançongiciel	Logiciel qui chiffre certaines données du PC et demande une rançon pour permettre le déchiffrement
Adware / Publiciel	Logiciel qui modifie le navigateur web pour envoyer la cible sur des publicités
Bombe logique	Logiciel destructeur de données ou de matériel
Backdoor	Logiciel qui permet de se connecter au matériel infecté. La connexion peut se faire par exemple via un reverse shell.
Exploit	Logiciel permettant d'exploiter une faille de sécurité qui peut permettre de créer une backdoor, de télécharger d'autres fichiers, de placer un spyware...
Rogue / Scareware	Logiciel se faisant passer pour un antivirus et indiquant que le PC est gravement infecté. Il se propose de le désinfecter en échange de l'achat d'une licence
Dialer	Logiciel permettant d'exploiter des fonctionnalités de téléphonie (appel, SMS)
Spammeur	Logiciel envoyant du spam/pourriel

La menace des rançongiciels

- **Logiciel malveillant** empêchant la victime d'accéder au contenu de fichiers et/ou dérobant des données afin d'extorquer de l'argent.

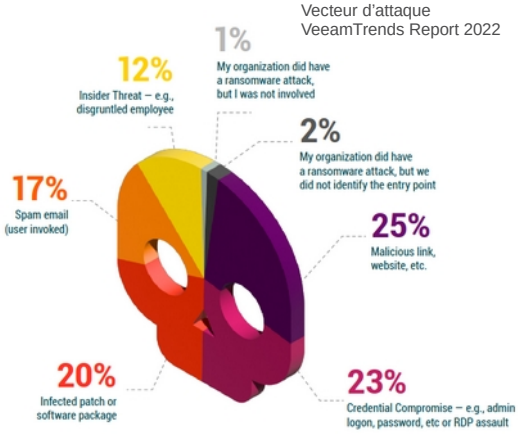
En France :



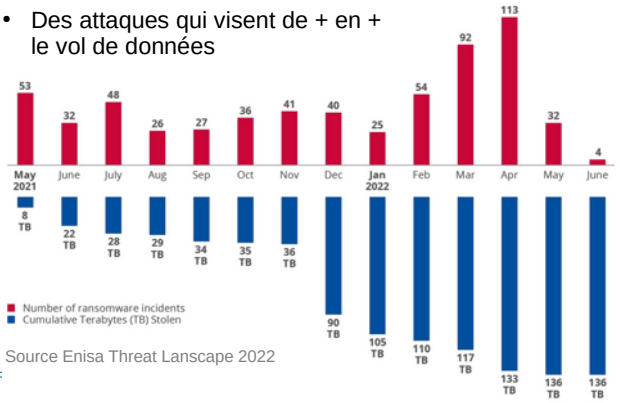
Répartition de types de victimes 2021-2022
Statistiques sur signalement d'attaque (France)

Source ANSSI - 2022

Vecteur d'attaque
VeeamTrends Report 2022



- Des attaques qui visent de + en + le vol de données

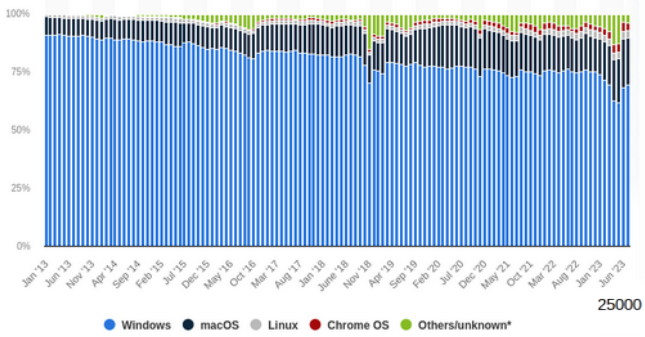


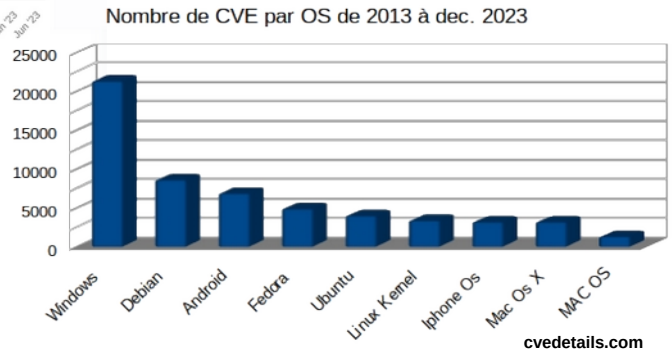
Source Enisa Threat Lanscape 2022

Ransom ⇒ Demande de rançon
Ware ⇒ Logiciel

Quel système d'exploitation est le plus « sûr » ?

Part de marché des systèmes d'exploitation

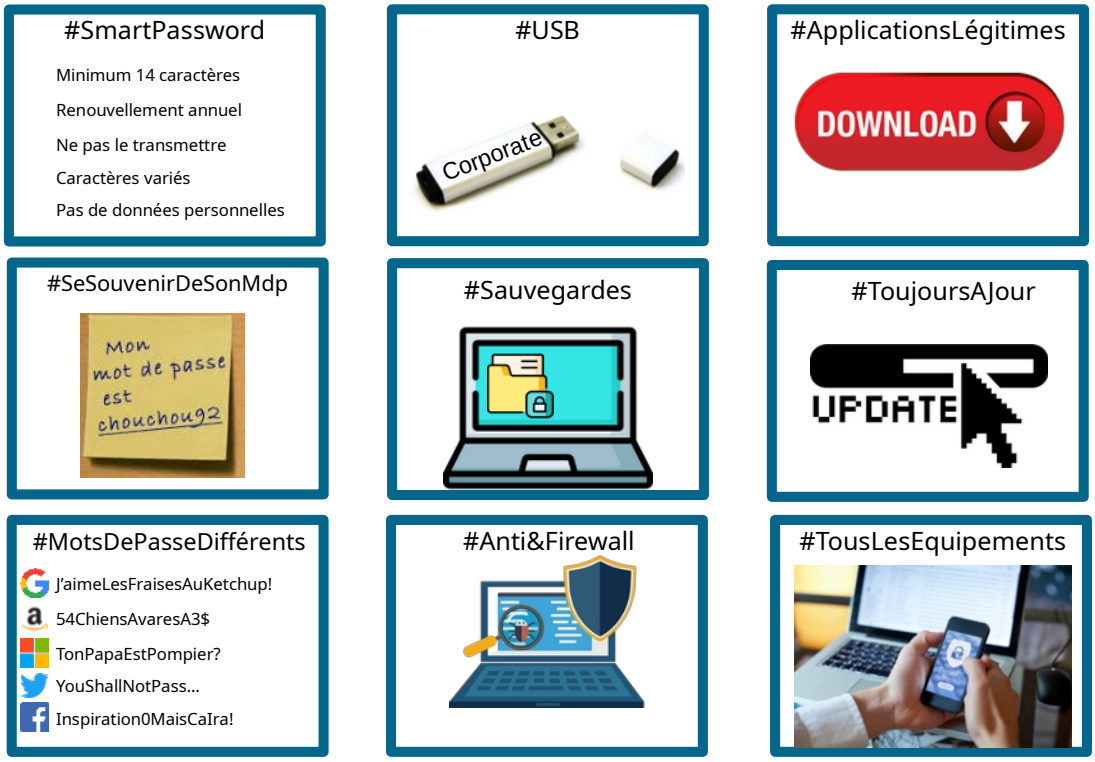




Un des intérêts du pirate : profiter des vulnérabilités du système exploitation le plus représenté en entreprise et dans le monde.

Source CVEDetails : https://www.cvedetails.com/top-50-products.php?year=0

Prévenir les compromissions du SI



Bonnes pratiques pour les mots de passe :
- Un mot de passe différents pour chaque utilisation
- Minimum 10 caractères, mélangeant les caractères spéciaux, chiffres, majuscule et minuscule
- Un mot de passe, c'est aussi comme une brosse à dent, c'est personnel, çà ne se prête pas.
- Ne pas utiliser des mots de passe « basique » (azerty, password) ni contenant des informations sur votre situation personnelle (date de mariage, nom du chien …)
- Pour se souvenir de son mot de passe, utilisez un mnémotechnique : phrase dans une chanson, 4 objets de votre bureau, titre d'un film …
- Des gestionnaires de mots de passe existe tel que Keepass, n'hésitez pas à en parler avec votre service informatique.

Autres bonnes pratiques au quotidien :
- Ne téléchargez pas des applications non fournies par votre DSI
- Ne reportez pas les mises à jour, même sur vos téléphones
- Ne désactivez jamais vos antivirus et antispam
- Attention aux clés USB, ne mélangez pas les usages et vérifiez que l'antivirus est actif avant de brancher une clé USB sur vos postes.
- Ne brancher pas vos téléphones sur vos ordinateurs pour les recharger, un logiciel malveillant pourrait se transmettre de l'un à l'autre.
- Veillez à mettre tous les documents dans vos dossiers partagés sur le serveur de l'entreprise.
- Appliquez ces bonnes pratiques dans la vie pro, perso, sur les téléphones, les ordinateurs portables ou fixes, les tablettes et même vos consoles de jeu !

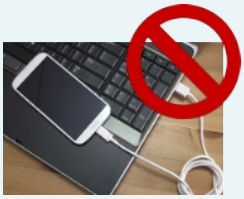
Prévenir les compromissions du SI : Ne pas faire confiance ...

aux périphériques USB et aux équipements branchés sur vos ports

Bash bunny

Keylogueur

Packet squirrel



aux outils proposés en ligne et gratuits

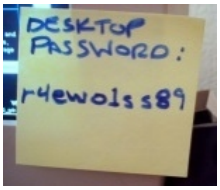
et même aux outils légitimes

Utilisez anti-virus, anti-spam, firewall logiciel ...

Intégration de la Sécurité dans les Contrats

Audit et tests d'intrusion

Les mots de passe : bonnes pratiques



- Changez les **mots de passe par défaut** et changez régulièrement de **mots de passe des comptes à privilège**.
- Ne pas **donner** un mot de passe à quelqu'un, quelles que soient les circonstances.
- Ne pas imposer par défaut de délai d'expiration sur les mots de passe des **comptes non sensibles.**
- Utilisez des **mots de passe différents** pour tous vos comptes en ligne (boîte mail, Facebook, banque…) et pour vos systèmes.
- Renforcez encore plus la sécurité pour vos comptes « sensibles » (banque, etc.) et pour vos systèmes sensibles (serveurs, matériels réseaux…) en activant l'authentification à **facteurs multiples**.
- Se souvenir de ses mots de passe ou un utiliser un **gestionnaire de mots de passe** (Keepass, Dashlane, BitWarden, LockPass…).
- Vérifier régulièrement les connexions sur vos comptes ou les « leak » (**Have I Been Powned?**)

KeePass

lockpass

Prévenir les compromissions du SI : Attention au phishing

De : « Support Technique" <support@cyberd1ne.com> **1** **Adresse email usurpée**
Date : 11/03/2015 07:22
Pour : « Paul OCHON »

Ne jamais ouvrir de pièce jointe suspecte, même les PDF
3 Guide_virus.pdf

Objet : Annonce importante

Cher Paul , **2** **Fautes d'orthographe**

Nous somme en train d'effectuer l'entretien de base données et mise à niveau notre messagerie pour une meilleure performancce. Nous sommes très préoccupéez par l'arrêt de la prolifération du spam. Nous avons mis en place la vérification d'adresse expéditeur (VAE) pour s'assurer que vous ne recever pas les emails indésirables et pour vous donner l'assurance que vos message à centre de messagerie n'ont chance d'être filtrée dans le dossier d'email en vrac.

Aussi un virus DGTFX a été détecté dans vos dossiers. Votre compte de messagerie doit être mise à jour à nouveau et sécurisé DGTFX anti-virus Version 2015 pour prévenir les dommages à notre messagerie électronique et vos fichiers importants.

Pour nous aider à confirmer et à protéger votre compte, remplissez les colonnes ci-dessous et de nous le renvoyer pour valider votre compte e-mail ou votre compte de messagerie sera fermé pour éviter la propagation du virus. Dans le cas contraire, nous serons dans l'obligation de suspendre, voire de supprimer votre compte de messagerie.

Menace exagérée ou inhabituelle **4**

Compte Nom d'utilisateur:
Mot de passe du compte:

5 **Pas d'information sensible par email**

Vous pouvez aussi vous connecter sur votre espace personnel : http://www.cyberdyne.com

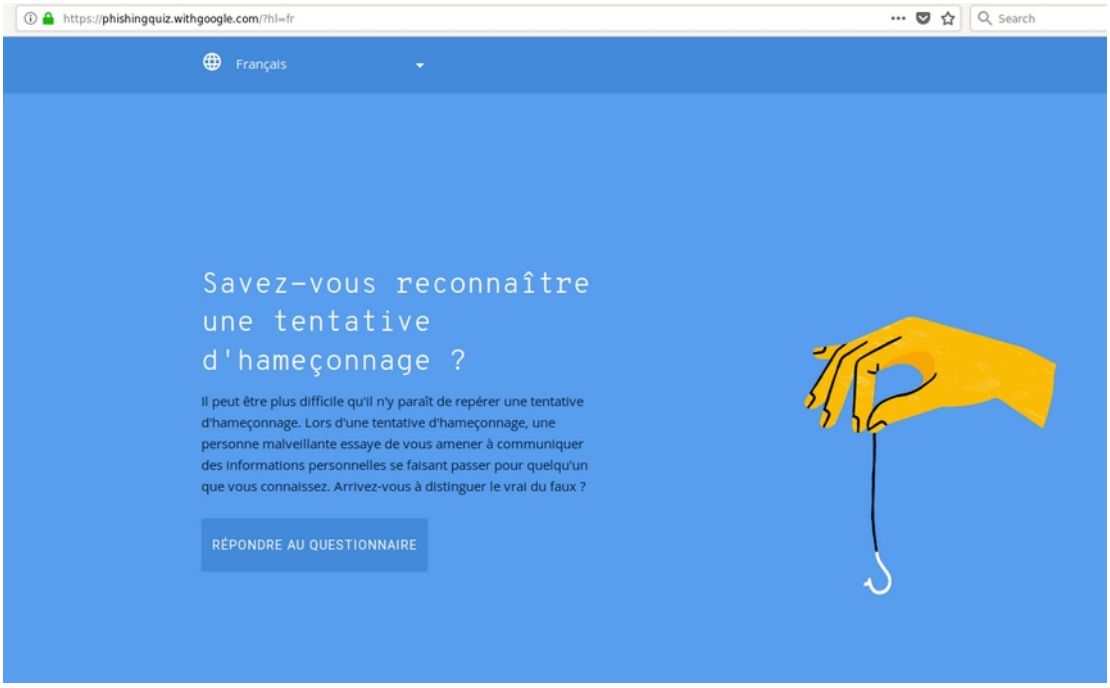
cyberd1ne.com **6** **Lien bon à l'orthographe mais quand on passe la souris dessus, c'est un autre lien**

Notez que votre mot de passe sera crypté avec 1024-bit clés RSA pour votre sécurité. **7** **Bonus : #chiffrer.info**

Cordialement,

Support Technique
Numéro de dossier: cw/8941/624
Numéro de téléphone : +330601020304 **8** **Appelez le numéro de votre carnet de contacts et non le contact sur le mail**

Prévenir les compromissions du SI : Attention au phishing



https://phishingquiz.withgoogle.com/?hl=fr

Panorama des différents moyens de protection

Les classiques de sécurité pour la disponibilité

Plan de continuité (PCA)

- Mesures préventives (redondance...)
- Plan d'urgence
- Plan de secours et mode dégradé
- PRA

Plan de sauvegarde

- Sauvegarde des données
- Sauvegarde des logiciels

Plan de reprise (PRA)

- Site de secours
- Données de secours
- Procédure de reprise
- Rôle des personnes
- Test réel des plans, régulièrement

Mesures spécifiques

- Plan de gestion des crises
- Papier / stylo
- Radio

Etc.

PCA : Plan de continuité d'Activité
PRA : Plan de reprise d'Activité

Les classiques de sécurité pour l'intégrité

Intégrité des équipements

- Journalisation, événements, sondes (IDS), SIEM, SOAR
- Supervision, SOC
- Intégrité physique (verrou, baie de brassage sécurisée, sécurité des ports USB, outil de gestion des vols, etc)

Intégrité des données et applications

- Empreintes numériques (hash)
- Archivages
- Traçabilité, journalisation des modifications
- Outils d'audit et HIDS
- Antivirus, antimalwares, EDR, XDR, EPP ...
- Pare-feu logiciel

Intégrité des personnes (morales ET physiques)

- Sensibilisations, formations, conseils
- Charte d'utilisation du SI
- Veille (image, notoriété, réputation, etc.)
- Contre-offensives informationnelles (web de crise, média, mailings, etc.)
- Organisation des rôles, procédures de vérifications
- Réglementations, législation

IDS : Intrusion Detection System, système de surveillance réseau ou d'un poste de travail permettant de détecter des intrusions.
HIDS : Host Intrusion Detection System (IDS sur un poste de travail)

SIEM : Security Information Event Manager, système de log orienté sécurité et qui permet d'avertir en cas d'incident de sécurité

SOC : Security Operation Center, un service au sein de l'entreprise dédié à la gestion des incidents de sécurité

SOAR : Security Orchestration, Automation and Respons. Couplé au SIEM, cet outil permet de déployer des scripts et des remédiations de manière automatique en cas d'attaque.

Famille de protection du poste de travail :
EDR : Endpoint Detection and Response
XDR : eXtended endpoint Detection and Response
EPP : Endpoint Protection Platform

SI : Système d'Information

Les classiques de sécurité pour la confidentialité

Authentification

- des personnes
- des données (origine, canaux, etc.)
- des équipements
- SSO, Kerberos, Fédération d'Identités
- Authentification sur le réseau : NAC, 802.1X
- Gestion des mots de passe
- Certificats et signatures

Contrôle d'accès

- Gestion des habilitations : Qui, quand, où, quoi, comment, *pourquoi*
- Alertes, journaux
- IAM
- PAM

Protection des données

- en mode connecté : HTTPS, VPN, SSH
- en mode non-connecté : sécurité physique (salons, workshops ...)
- Chiffrement
- Destruction physique, mise au rebut
- Cloisonnement des réseaux (VLAN, pare-feu, DMZ)

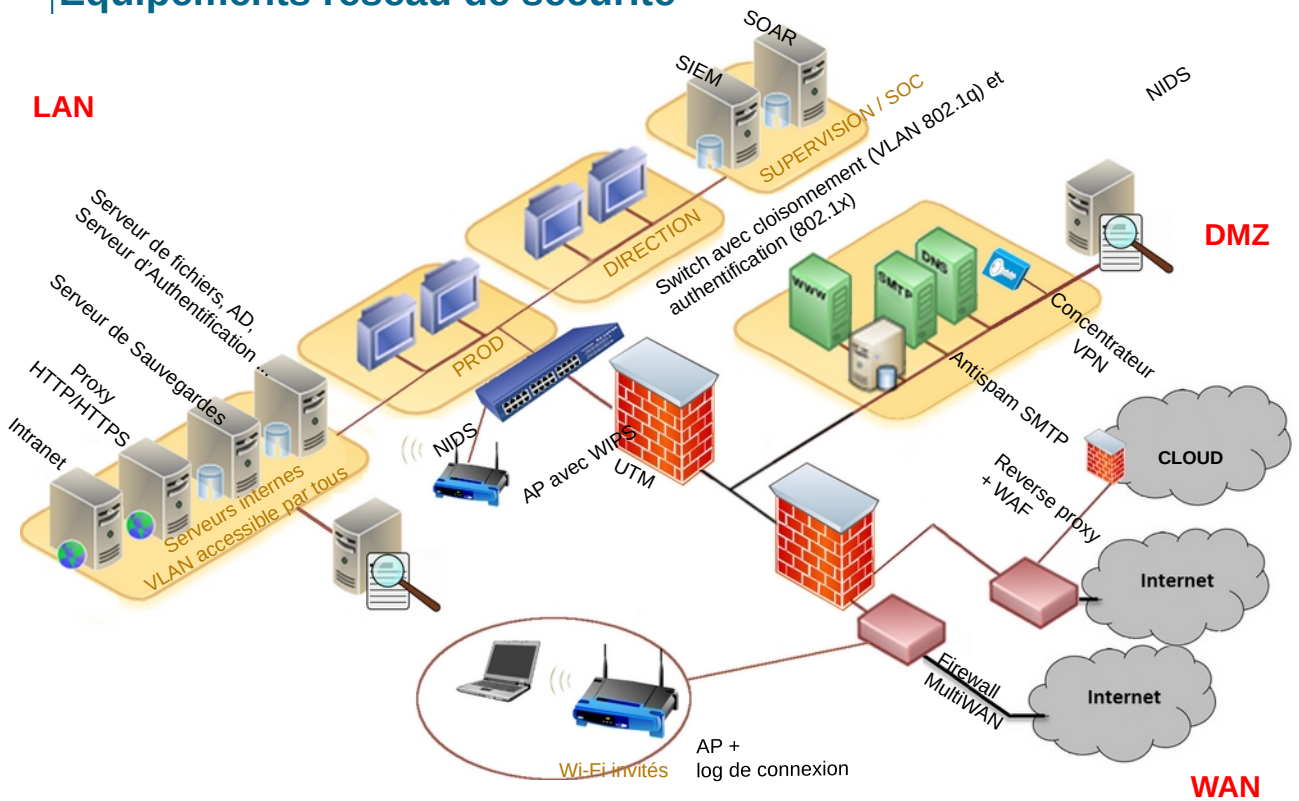
SSO : Single Sign On – un point d'authentification permet l'accès à plusieurs site
IAM : Identy and Access Management, process et organisation au sein de l'entreprise sur la gestion des accès et des identités

NAC : Network Access Control, outil permettant un accès réseau aux équipements qui sont habilités et enrôlés.
802.1x : protocole d'authentification sur le réseau

PAM : privileged access management, gestion des accès avec haut niveau d'administration

VPN : Virtual Private Network
HTTPs : connexion web http sécurisée
SSH : Secured Shell, protocole permettant la configuration d'un équipement de manière sécurisée
DMZ : zone démilitarisée, sous-réseau séparé du réseau local

Équipements réseau de sécurité



Parefeu/Firewall/FW : Équipement réseau qui contrôle les flux pour leurs permettre ou non d'accéder à un réseau.

DMZ : Zone démilitarisée où se trouvent les équipements accessibles via l'Internet.

WAN/LAN : Réseau externe dont Internet / Réseau local

VLAN : Virtual Local Aera Network. La norme 802.1q est la plus répandue.

802.1x : norme réseau qui permet l'authentification des équipements connectés à un point d'accès ou un switch.

AP : Access Point / Point d'accès Wi-Fi.

AD : active Directory : protocole permettant la gestion des identités.

Proxy : équipement mandaté par un autre pour effectuer une requête sur un protocole défini (généralement le HTTP et HTTPS) à sa place. Permet de faire du Filtrage d'URLs.

Reverse Proxy : permet aux utilisateurs d'internet d'accéder indirectement à certains serveurs. Permet de faire du filtrage d'éventuelles attaques avec la fonction **WAF** (Web Application Firewall) et de répartir la charge avec du load banlancing.

Antispam SMTP : permet de détecter si un ordinateur du LAN ne sert pas de « bot » pour envoyer des mails indésirables.

Bot : charge utile malveillante qui fait des actions sur l'Internet à l'insu de l'utilisateur (envoi de mails, Deni de Services…).

UTM : équipement tout-en-un qui gère des fonctions de sécurité diverses ainsi que des fonctions réseau (routage, VPN, DHCP …).

NIDS : Network Intrusion Detection System, équipements qui collectent, analysent de données en termes de sécurité et placés aux endroits stratégiques du réseau. Leur rôle est de détecter des intrusions de pirates ou de logiciels malveillants par analyse par signatures ou analyse comportementales.

WIPS : Wi-Fi Intrusion Prevention System : comme le NIDS, détecte et bloque (Prevention) les attaques liées au Wi-Fi.

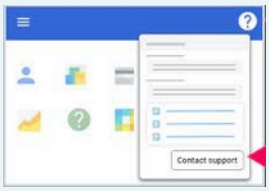
SIEM : Security Information & Event Manager, analyseur et corrélateur de logs orientés sécurité (Antivirus, IDS, FW …)

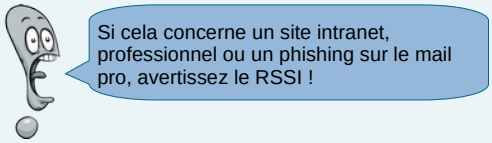
SOAR : Security Orchestration, Automation and Response. A partir des alertes du SIEM, déclenche automatiquement des actions d'administration système et réseau.

En cas de crise

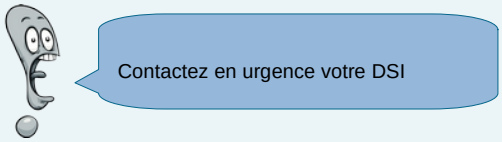
Oups…

J'ai saisi des ID sur un site malveillant





J'ai ouvert un fichier et mon poste se comporte bizarrement



MERCI POUR VOTRE ATTENTION