Veille Technologique

BTS SIO

Sommaire

Quelques définitions :

- Veille : (1er sens) Représente le fait de ne pas dormir, être actif 24h/24. (2ème sens) Le fait de surveiller, et d'agir en cas de changement.

- Veille Technologique : Consiste à surveiller, collecter, s'informer sur les évolutions technologiques pour les anticiper et éviter les risques possibles et rester en cohésion avec les changements.

- Environnement numérique : Un espace qui permet d'accéder à des ressources matérielles et logicielles et à des services numériques en ligne (WAN Public) ou locales (LAN Privé).

Thème choisis pour la Veille Technologique :

Les « cyberguerres » ou « cyberattaques » (Cybersécurité).

Voir quels sont les méthodes et les moyens utilisés pour effectuer des attaques informatiques et leurs objectifs finals. Déterminer les conséquences qui peut y avoir sur différentes échelles (mondiales, entreprises, etc.).

Comparaison d'outils de veille :

- Méthode **Pull** : Récolter les informations par nous-même en effectuant plusieurs recherches (très chronophage). Possibilité d'obtenir des informations que des algorithmes ne trouveront pas.

- Méthode **Push** : Recevoir des notifications concernant des recherches ayant des mots-clés qui peuvent nous intéresser. Plus rapide et plus efficace, mais on peut recevoir des recherches qui ne nous intéresseront pas. Donc à vérifier et trier régulièrement.

Outil	Méthode	Utilisation	Avantages	Inconvénients
Netvibes (Logiciel sur PC et Applications sur Smartphone) *[Gratuit/Payant]*	Push	Utilisation de flux RSS, Atom et iCal. Tableau de bord présentant différents onglets (widget, flux...). Choix d'applications ou des flux qui nous intéressent.	- Efficace et rapide. - Recherche automatique en fonction de nos critères. - Utilisable sur PC et Smartphones. - Veille à la fois sur des sites et des applications. - Gratuit et Payant.	- Certaines recherches ne seront sûrement pas intéressante. - Vérifier et trier les infos.
Pocket (Extension pour navigateur)	Pull	Principe de marques pages. Sauvegarder du contenu (articles, vidéo, etc.) depuis n'importe quelle page ou application.	- Organiser et de regrouper nos différentes recherches - Consulter à n'importe quel moment.	- Recherches à faire soi-même. - Reste chronophage.

[Gratuit/Payant]			- Rechercher à travers nos marques pages. - Gratuit.	- Plus accessible sur PC que sur Smartphones.
Feedly (Extension et Application) *[Gratuit]*	Push	Trouver des articles de grands sites (du plus populaire au moins populaire) en recherchant des mots-clés. Feedly va proposer tous les articles/sites traitant ces mots-clés. Possibilité de suivre les sites pour recevoir des notifications.	- Simple à utiliser. - Recherche à la fois manuelle et automatique - Recherche du plus visité/populaire, au moins visité. - Voir le rythme des publications des sites. Utilisable sur PC et Smartphones. - Gratuit.	- Limité sur la version gratuite -
Hootsuite (Logiciel) *[Payant]*	Push	Permet de récolter des recherches sur des réseaux sociaux (Twitter, LinkedIn, Facebook, etc.) grâce aux flux. Présente les recherches sur un tableau de bord avec des colonnes qui regroupe les recherches par réseau.	- Sépare les fils d'actualité, message envoyé, message reçu, réponse à des message, etc. - Gestion de différents réseaux en même temps.	- Utilisable seulement pour les réseaux sociaux. - Payant
Clusif (Forum/site) *[Gratuit/Payant]*	Pull	Site axé sur la Sécurité de L'information. Principe de publication traitant sur différents thèmes.	- Possibilité de filtrer en fonction de la date de publication. - Information axé sur la SI et Cybersécurité.	- Recherche à faire de façon manuelle.
Symbaloo (Site/Dashboard) *[Gratuit]*	Pull	Site sous forme de Dashboard (tableau de bord). Avoir accès à différentes applications personnalisable.	- Permet de faire des recherches rapide et organisé. - Possibilité de personnalisé les applications.	- Vérification autonome des nouveautés.
OneNote (Site/Application) *[Gratuit/Payant]*	Pull	Utilisé pour la prise de note. Possibilité de choisir différents pages de notes. Possibilité d'insérer différents fichiers (photo, lien…)	- Organiser les prises de notes. - Insérer différents types de fichiers - Accessible depuis l'ordinateur (site) ou par téléphone (application)	- Doit être rédigé manuellement - Mettre à jour au fur et a mesure soi-même

Etude sur la Veille

Définitions de termes :

Le préfixe « cyber » va regrouper plusieurs termes liés à l'informatique/le numériques tel que : Cybersécurité, Cybercafé, Cyberdéfense, Cybercriminalité, Cyberguerre, etc.

Cybersécurité :
Représente la protection des ressources, des données, des outils connectées ou installés. La cybersécurité regroupe l'ensemble des moyens utilisés (lois, dispositifs, gestion des risques, actions, etc..) pour assurer la défense d'un particulier (utilisateur lambda) ou d'une entreprise.

Cyberattaque :
Attaques/actions qui vise le cyberspace ou des infrastructure, systèmes, etc., ayant un but malveillant. Ces actions sont volontaires et offensives. Elles peuvent être faites par des personnes seules ou des groupes de pirate ou biens d'organisation (état). L'objectif de ces attaques est des créer des dommages ou des perturbations sur les informations et les systèmes afin de voler des données ou nuire leurs utilisations.

Cyberguerre :
La cyberguerre est en quelques sorte un regroupement de cyberattaques (attaque dans le cyberspace) mais sur un niveau géopolitique (confrontations entre états, entre grande ou petites entreprises, etc..). Ces attaques ont principalement des buts politiques à différentes échelles (entreprises, état, continentale, mondiale).

Pourquoi toutes ces attaques ?

Toutes ces attaques ont des buts différents dépendant de leurs échelles. Par exemple, une cyber-attaque peut être faite pour procurer une satisfaction personnelle aux attaquants en effectuant des DoS (déni de service, mettre des systèmes hors ligne), mais elle peut également avoir comme buts l'obtention de données personnels (nom, prénom, adresse, code de carte bancaire, etc..), la modification de données, l'espionnage, etc. Elle peut être orchestrées par des entreprises/organisations ou même des états, pour des buts politiques ou pour en soutirer de l'argent.
Les attaques peuvent également être interne, par exemple, lorsqu'un salarié divulgue ou supprime des données intentionnellement ou par mégarde.

Une cyberattaque peut entraîner une cybercrise, que ce soit au niveau IT (blocage du site), financier ou de réputation (les données utilisateurs risquent d'être exposées).

Qu'est-ce que la cybersécurité ?

La cybersécurité représente tous les moyens utilisés afin d'assurer la protection et l'intégrité des données. Cette notion devient de plus en plus récurrente grâce la transformation numérique des entreprises (utilisation d'outils informatiques, etc ...).

Dans une entreprise, les dirigeants sont responsables de l'intégrité et de la confidentialité des données qui circulent pour son activité. En tant qu'employeur, il s'agit également de protéger les salariés en ce qui concerne leurs informations personnelles.

Les entreprises peuvent internaliser les compétences dans le domaine de la cybersécurité grâce à une DSI (Direction des Systèmes d'Information). L'intervention d'un expert extérieur est également une bonne pratique (externalisation).

Différents types d'attaques

TYPE D'ATTAQUE	PRINCIPE
Déni de Service (DoS / DDoS)	Une attaque par déni de service submerge les ressources d'un système afin que ce dernier ne puisse pas répondre aux demandes de service.
TCP SYN Flood	Exploitation de l'espace tampon lors du Handshake d'initialisation de session TCP.
Teardrop	Modification des paquets IP perturbant le système ciblé qui tente de reconstruire le paquet. Le système s'embrouille et plante.
Smurf	Usurpation d'une adresse IP et saturer le trafic d'un réseau cible en utilisant des demandes ICMP.
Ping of Death	Ping des systèmes cible avec des paquets IP dont la taille est supérieure au maximum. Envoi d'un paquet fragmenté, la cible reçoit et réassemble le paquet (plantage).
Détournement de session (MitM)	Lors d'une session entre un client et un serveur, l'attaquant se fait passer pour le client et effectue les échanges avec le serveur.
Phishing	L'hameçonnage consiste à envoyer des e-mails qui semblent provenir de sources fiables dans le but d'obtenir des informations personnelles ou d'inciter les utilisateurs à faire quelque chose.

Exemples d'attaques

DATE (MM/AA)	LIEN	SUJET
12/19	https://www.hiscox.fr/sites/france/files/documents/CP_Les_10_cyberattaques_qui_ont_marque_l_annee_2019.pdf	Liste d'attaques 2019
12/19	https://cyberguerre.numerama.com/1921-la-cyberattaque-du-chu-de-rouen-reflete-une-annee-2019-delicate-pour-les-hopitaux-francais.html	Attaque du CHU de Rouen 2019
01/20	https://www.zdnet.com/article/wawa-card-breach-may-rank-as-one-of-the-biggest-of-all-times/	Coordonnées de clients mis en vente en ligne
03/20	https://www.zdnet.com/article/skimming-code-lurking-on-nutribullet-website-puts-customer-credit-card-data-at-risk/	Attaque de type Magecart
08/20	https://siecledigital.fr/2020/08/21/le-passage-au-teletravail-a-cause-une-augmentation-des-cyberattaques/	Augmentation des cyberattaques avec le télétravail
09/20	https://siecledigital.fr/2020/09/04/sfr-et-bouygues-telecom-victimes-dune-importante-cyberattaque/	Attaque d'SFR et Bouygues
09/20	https://siecledigital.fr/2020/09/18/twitter-renforce-la-securite-des-comptes-des-politiciens/	Renforcement de la sécurité des comptes Twitter des politiciens
10/20	https://www.zdnet.fr/actualites/la-coree-du-nord-a-tente-de-pirater-11-membres-du-conseil-de-securite-de-l-onu-39910579.htm	Cyberattaque de la Corée du Nord contre au moins 28 membres de l'ONU
12/20	https://www.zdnet.fr/actualites/2020-les-cyberattaques-qui-ont-marque-l-annee-39914023.htm	Liste d'attaques 2020
12/20	https://www.novethic.fr/actualite/economie/isr-rse/entre-les-vaccins-le-covid-19-et-le-teletravail-2020-a-ete-l-annee-des-cyberattaques-149341.html	90% des organisations françaises visées par des cyberattaques en 2020
12/20	https://www.oci.fr/cyberattaques-2020/	Liste d'attaques 2020
12/20	https://www.ouest-france.fr/societe/cyberattaque/tribune-un-bouclier-cyber-pour-l-europe-7088381	Cyber-bouclier pour protéger l'Europe
12/20	https://press.avast.com/third-party-browser-extensions-from-instagram-facebook-vimeo-and-others-infected-with-malware	+28 Extension Chrome et Edge malveillant.
02/21	https://siecledigital.fr/2021/02/10/floride-hacker-eau-potable/	Tentative d'empoisonnement d'un réseau d'eau potable
02/21	https://www.huffingtonpost.fr/entry/pourquoi-les-hopitaux-francais-sont-particulierement-vises-par-les-cyber-attaques_fr_602e4880c5b6cc8bbf397a59	Ciblage des hôpitaux
03/21	https://siecledigital.fr/2021/01/29/emotet-malware-demantelement/	Démantèlement du Malware Emotet
08/21	https://siecledigital.fr/2021/03/08/cybersecurite-les-etats-unis-mis-a-lepreuve-par-la-russie-et-la-chine/	Cyberguerre entre les Etats-Unis, la Russie et la Chine

Se protéger des attaques

Les entreprises sont les plus grandes cibles des attaques informatiques. Il est donc important d'avoir un service de cybersécurité en externalisant ou de façon interne en nommant un responsable qui préviendra, analysera les risques et proposera des plans d'actions. Les employés doivent également être formé sur les bons gestes à avoir pour limiter les risques.

Il est également important d'avoir d'une habitude de sauvegarde régulière des données (sur support physique et cloud) pour minimiser les dégâts causés par une cyberattaque.

L'utilisation de logiciel d'antivirus efficace et de confiance.

L'utilisation de mots de passe sécurisés (12 caractères minimum avec lettre majuscules, chiffres, caractères spéciaux) permet de bien protéger ces données. Il est impératif de changer les mots de passe au bout de quelque mois ou en cas de doutes de fuites.

Bilan

Les cyberattaques prennent une ampleur de plus en plus grande au fil du temps avec l'évolution constante des technologies. De plus en plus d'établissements sont ciblés par des attaques, et doivent y faire face en mettant en place de meilleure sécurité au sein de leurs infrastructures. Même si certaines vulnérabilités sont corrigées, d'autre peuvent apparaitre, et ainsi de suite. Le domaine de la cybersécurité sera toujours un domaine actif tant qu'il y des réseaux.

Source et Référencement

Pourquoi toutes ces attaques ?

https://www.sudouest.fr/economie/reseaux-sociaux/cyberattaques-qui-quoi-et-pourquoi-1355348.php (02/20)

https://www.undernews.fr/reseau-securite/comment-se-proteger-contre-les-cyberattaques%e2%80%89.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+undernews%2FoCmA+%28UnderNews%29 (05/21)

Qu'est-ce que la cybersécurité ?

https://www.cisco.com/c/fr_fr/products/security/what-is-cybersecurity.html (//)

https://www.sage.com/fr-fr/blog/glossaire/cybersecurite-definition-de-la-cybersecurite/ (11/20)

https://whatis.techtarget.com/fr/definition/cybersecurite (//)

Différents types d'attaques

https://blog.netwrix.fr/2018/07/04/les-10-types-de-cyberattaques-les-plus-courants/ (09/19)

https://www.cisco.com/c/fr_fr/products/security/common-cyberattacks.html (05/20)

https://www.logpoint.com/fr/blog/lutter-cyberattaques/ (11/20)

https://www.oodrive.com/fr/blog/securite/top-10-differents-types-cyberattaques/ (03/21)

Se protéger des attaques

https://business.lesechos.fr/entrepreneurs/efficacite-personnelle/0602317764287-se-proteger-des-cyberattaques-les-7-piliers-de-la-sagesse-333500.php (12/19)

https://www.undernews.fr/reseau-securite/comment-se-proteger-contre-les-cyberattaques%e2%80%89.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+undernews%2FoCmA+%28UnderNews%29 (05/21)

https://www.aviva.fr/assurance-professionnelle/mon-activite/cybersecurite/cyberattaque/ (08/20)