CENTRE FOR
CYBER SECURITY
BELGIUM

UNDER THE AUTHORITY OF
THE PRIME MINISTER

L'ABC DU CCB

LA CYBERSÉCURITÉ EXPLIQUÉE EN 42 RÉPONSES

.be

POUR QUI ?
Pour les journalistes et les personnes intéressées par la cybersécurité.

QUOI ?
Ce document décrit au moyen de quelques phrases 42 notions très courantes dans le monde de la cybersécurité et les illustre si possible au moyen de chiffres récents.

EST-CE RÉCENT ?
Ce guide a été finalisé le 15 mars 2020.

QUI EST L'AUTEUR?
Cet ABC a été rédigé par Andries Bomans et Katrien Eggers, responsables de la communication du Centre pour la Cybersécurité Belgique avec l'aide de nombreux collègues.

À PROPOS DU CENTRE POUR LA CYBERSÉCURITÉ BELGIQUE
Le Centre pour la Cybersécurité Belgique (CCB) est le centre national dédié à la cybersécurité en Belgique. Le CCB a pour mission de superviser, coordonner et veiller à la mise en œuvre de la stratégie belge en matière de cybersécurité. C'est en optimalisant l'échange d'informations que la population, les entreprises les autorités et les secteurs vitaux pourront se protéger de manière adéquate.
www.ccb.belgium.be

À PROPOS DE CERT.BE
La Computer Emergency Response Team fédérale, ou CERT.be, est le service opérationnel du Centre pour la Cybersécurité Belgique (CCB). CERT.be est chargé de détecter, d'observer et d'analyser les problèmes de sécurité en ligne ainsi que d'informer les différents groupes cibles en permanence à ce sujet.
www.cert.be

Personnes de contact pour la presse
Andries Bomans : 0471 66 00 06, andries.bomans@ccb.belgium.be
Katrien Eggers : 0485 765 336, katrien.eggers@cert.be

TABLE DES MATIÈRES

1. LA 5G

La 5G est 100 à 200 fois plus rapide que la 4G.

Si aujourd'hui la plupart des internautes sont connectés au **réseau 4G**, à l'avenir nous passerons au **réseau 5G** qui est beaucoup plus rapide. Le secteur médical, l'industrie des voitures autonomes et toutes les autres applications technologiques qui nécessitent une connexion en temps réel attendent avec impatience l'arrivée de la 5G, car elle représente un bond en avant en termes de possibilités de progrès.

Cependant, comme souvent en matière de progrès technologique, il y a peut-être aussi un revers à la médaille. En effet, le fournisseur d'un réseau 5G jouira d'un pouvoir particulièrement important et la 5G pourra aussi être utilisée à des fins moins nobles, comme l'**espionnage**. Le CCB assure le suivi technique de ce dossier. D'autres partenaires se penchent quant à eux sur les conséquences économiques et géopolitiques du déploiement du réseau 5G.

2. ADVANCED PERSISTENT THREAT (APT)

« Advanced Persistent Threats », ou APT, est un nom qui regroupe les cyberattaques avancées et ciblées. Une APT se caractérise par sa faculté à se dissimuler longtemps et sans être vue dans un réseau, avant de réellement passer à l'action. C'est précisément parce que les ATP sont si sophistiquées que l'on suppose qu'elles sont le fait de nations et non de particuliers. Les APT sont souvent utilisées à des fins d'**espionnage** politique, économique ou industriel ou encore pour des **cyberattaques**.
CERT.be observe de près les Advanced Persistent Threats via l'Early Warning System, afin que les services visés soient rapidement informés et puissent renforcer leur sécurité. (Voir également A : attribution d'une cyberattaque ; E : Early Warning System)

3. ANTIVIRUS

78 % des Belges ont un antivirus (Safeonweb DGI, 2019)

Un antivirus rend un ordinateur moins perméable aux virus et le protège donc mieux contre les cyberattaques. L'utilisation d'un scanner antivirus est l'une des cinq règles de base de la cybersécurité.

Nos conseils :

- Même si aucun logiciel antivirus ne peut garantir une protection à 100 %, il est indispensable d'en installer un.

- Malheureusement, de nouveaux virus sont développés chaque jour. Il est donc nécessaire d'installer à tout moment les mises à jour les plus récentes de votre antivirus.

https://www.safeonweb.be/fr/scannez-votre-ordinateur

4. ATTAQUE ZERO DAY

Une attaque zero day est une **cyberattaque** qui profite des **vulnérabilités** des logiciels qui sont encore **inconnues** du développeur. Dès que les vulnérabilités en question sont révélées, les développeurs de logiciels s'attellent en effet à trouver une solution, ou « **patch** », pour supprimer les vulnérabilités. Le délai entre le moment où la vulnérabilité est révélée et le moment où le « patch » est développé s'appelle « zero day ». Les patchs sont transmis aux utilisateurs finaux via les mises à jour. D'où l'importance des **mises à jour**.

Les attaques zero day sont dangereuses parce qu'elles ont lieu au moment où la protection n'est pas encore possible. Il ressort d'études montrent que très peu d'attaques zero day sont couronnées de succès. La plupart des cyberattaques profitent de vulnérabilités connues sur des appareils dont le logiciel n'a pas été mis à jour à temps. Par exemple, WannaCry a profité des vulnérabilités connues pour lesquelles les mises à jour de sécurité étaient disponibles mais n'étaient pas toujours appliquées. (Voir également M : Mises à jour)

5. ATTRIBUTION D'UNE CYBERATTAQUE

L'attribution d'une cyberattaque consiste en l'identification de son auteur, une tâche qui s'avère très complexe. La détection de traces en ligne par le biais d'**enquêtes légales** représente un travail délicat de longue haleine. Les auteurs sont **difficiles à tracer**. Certains États se livrent parfois à des attaques envers d'autres États pour des raisons géopolitiques, dans le but d'obtenir des informations stratégiques au moyen de l'espionnage, de l'influence de l'opinion publique ou des processus démocratiques, voire du sabotage de services essentiels. Il n'est pas aisé de prouver avec certitude qu'un État est à la source d'une attaque envers un autre État ; une telle attribution est par ailleurs **sensible d'un point de vue diplomatique**. Le CCB n'a pas pour mission d'attribuer une cyberattaque ; c'est aux services compétents qu'il revient de se prononcer à l'issue d'une enquête judiciaire. (Voir également A : Advanced Persistent Threat)

6. BACK-UP

22 % des Belges ne réalisent jamais de back-up (Safeonweb DGI, 2019)

Un back-up est une **copie de sauvegarde** des données importantes pour une personne. Cette sauvegarde vous permet de récupérer vos données si un virus infecte votre ordinateur ou si un « virus de rançon » (ransomware) bloque vos données et demande de l'argent en échange pour le débloquer. La création de copies de sauvegarde est l'une des cinq **règles de base** de la cybersécurité que le Centre pour la Cybersécurité Belgique propose sur Safeonweb.be.

Nos conseils :

- Sauvegardez régulièrement les fichiers importants.
- Vous pouvez opter pour une sauvegarde **sur le *cloud*** ou **sur un disque dur externe**.
- Assurez-vous qu'il y a suffisamment de « distance » entre vos fichiers et la sauvegarde. Veillez au moins à déconnecter votre sauvegarde de votre ordinateur. La sauvegarde sur le ***Cloud*** constitue un bon choix car elle crée une distance.

https://www.safeonweb.be/fr/pensez-aux-sauvegardes
(Voir également R : Ransomware)

7. BASELINE SECURITY GUIDELINES

Les **Baseline Security Guidelines** (BSG) fournissent aux administrations publiques des **lignes directrices** de base en vue de l'implémentation ou de l'évaluation d'un **plan de sécurisation de l'information**, venant ainsi en aide aux responsables du traitement, aux conseillers en sécurisation, aux contrôleurs des données et aux responsables informatiques.

C'est le Centre pour la Cybersecurité Belgique en concertation avec des experts issus de différents SPF et des consultants externes qui a développé ce BSG, en tenant compte des normes en vigueur comme ISO 27001 et ISO 27002. (Voir également I : ISO 27002)

https://www.ccb.belgium.be/fr/government

8. BOTNET ERADICATION PROJECT

Le projet **Botnet Eradication** a pour but d'éliminer les botnets en Belgique. L'objectif est d'informer les utilisateurs infectés (tant les particuliers que les entreprises) qu'ils ont été touchés par un virus et qu'ils sont un des maillons d'un botnet. Outre ces informations, les

utilisateurs seraient également informés des moyens à leur disposition pour désinfecter leur système. (Voir également A : Attaque DDOS)

9. CRYPTOJACKING

En 2017, le nombre de signalements de coinminers auprès des utilisateurs finaux a grimpé de 8 500 pour cent.

Les cryptomonnaies sont des monnaies virtuelles, la plus connue étant le Bitcoin. Pour obtenir un Bitcoin ou une autre variante de cryptomonnaie, un ordinateur doit effectuer de nombreux calculs qui requièrent une quantité d'énergie (CPU) importante. Pour effectuer ces calculs, un ordinateur ou un smartphone est récompensé en Bitcoins. Ce processus est connu sous le nom de **cryptomining**, ou minage de cryptomonnaies.

Aujourd'hui, les criminels essaient d'accéder à des appareils pour pouvoir les utiliser pour collecter des **cryptomonnaies**, et ce à l'insu du propriétaire. Ce phénomène s'appelle le **cryptojacking**.

https://www.safeonweb.be/fr/mon-appareil-est-utilise-des-fins-de-cryptojacking

10. CYBERGUIDE

150 mesures de cybersécurité regroupées au sein d'un guide unique.

Le Cyberguide du CCB est un **guide de référence** en ligne qui a pour but d'aider **les organisations et les entreprises** à améliorer leur **stratégie en matière de cybersécurité. Quatre catégories** vous donnent un aperçu des mesures de cybersécurité basiques et plus avancées. Chaque mesure est assortie d'une description, d'informations pratiques et de liens utiles vers des sites Internet et des outils. Ce sont au total plus de 150 mesures de cybersécurité qui sont à votre disposition. Ce guide est un outil essentiel pour les organisations et les entreprises qui souhaitent mettre place une stratégie de **cybersécurité**.

Lire le guide complet

11. CYBER SÉCURITÉ

Le Centre pour le Cybersécurité Belgique est responsable de la politique générale de cybersécurité. Le CCB supervise, coordonne et contrôle l'application de la stratégie belge de cybersécurité. L'échange optimal d'informations permet aux entreprises, au gouvernement, aux fournisseurs de services essentiels et à la population de se protéger de manière appropriée. Le CCB a pour mission de veiller à ce que l'internet dans notre pays reste sûr et que l'internaute soit suffisamment informé pour être en sécurité en ligne.

12. CYBERSECURITY ACT

Le 10 décembre 2018, les institutions européennes sont parvenues à un accord politique concernant sur la cybersécurité, le « Cybersecurity Act ».

Le **Cybersecurity Act** délimite un **cadre** pour les **certificats européens de cybersécurité** pour les produits, les procédés et les services qui sera en vigueur à l'échelle de l'UE. Cette **loi** sur la cybersécurité renforce notamment le mandat et les ressources de l'Agence européenne de cybersécurité (**ENISA**). La loi prévoit également un cadre européen pour la **certification en matière de cybersécurité**, afin d'améliorer la sécurité des services et technologies en ligne. Il s'agit d'un développement novateur dans le sens où c'est la première fois qu'un marché intérieur se dote d'une législation qui s'attaque au défi d'améliorer par le biais de certificats la sécurité des produits connectés, des appareils de l'IoT et des infrastructures critiques.

Les nouvelles règles sont indispensables si l'on entend assurer la sécurisation de la technologie des appareils connectés ou l'**Internet of Things**. L'objectif est d'inciter les entreprises à investir dans la cybersécurité par le biais de la certification et de pouvoir l'utiliser comme un avantage concurrentiel. (Voir également E : ENISA)

13. CYBER SECURITY COALITION

Depuis 2015, la **Cyber Security Coalition** rassemble sous la bannière d'une seule organisation des représentants du secteur public, du secteur privé et du monde académique. Cette approche est unique en Belgique et garantit l'échange d'expériences et de bonnes pratiques concernant la sensibilisation, le respect de la vie privée, la NIS, le Cloud, l'Enterprise Security Architecture, la Crypto et la certification.

En qualité de directeur du Centre pour la Cybersécurité Belgique, Miguel De Bruycker a rejoint le conseil d'administration de la Cyber Security Coalition Belgium le 7 décembre 2015. La Cyber Security Coalition est un partenaire prioritaire du Centre pour la Cybersécurité Belgique et un lien important avec le secteur privé.

https://www.cybersecuritycoalition.be/

14. DIGITAL SINGLE MARKET (DSM)

Le **marché unique numérique** (DSM en anglais) concrétise la stratégie globale de la Commission européenne en matière de politique et d'investissement dans le monde numérique. La stratégie du DSM a été lancée en 2015 et mise à jour en 2017 ; elle est applicable à de nombreux sous-domaines, allant du commerce électronique au droit d'auteur, en passant par le géoblocage et la cybersécurité. Nous pensons à l'abolition des frais d'itinérance au sein de l'UE, à la législation relative au RGPD (GDPR), à la législation sur les droits d'auteur, à la directive NIS ou au cyber act.

De manière globale, la stratégie du DSM repose sur trois piliers : l'amélioration de l'accès aux biens et services numériques, la création de conditions justes et d'un terrain de jeu équitable pour mettre en place des réseaux numériques et des services innovants, ainsi que l'optimisation du potentiel de croissance de l'économie numérique.

15. DISTRIBUTED DENIAL OF SERVICE (DDOS)

Une attaque Denial of Service Distributed Denial ou **attaque DDoS** est une cyberattaque lors de laquelle le trafic sur des ordinateurs, des réseaux informatiques ou des serveurs est très intense, ce qui les perturbe.

Pour effectuer une attaque DDoS, les cybercriminels utilisent un **botnet**. Il s'agit d'un vaste réseau d'ordinateurs ou d'appareils connectés (les « **bots** ») qui sont contaminés par des malware. Un cyberpirate est en mesure de diriger ces ordinateurs pour exécuter une tâche déterminée à partir d'un point central (l'**hébergeur du bot**). Les internautes ne sont pas conscients que leurs appareils peuvent faire partie d'un botnet.

Notre conseil pour ne pas devenir un bot :

- Effectuez toujours les mises à jour
- Utilisez toujours un antivirus
- Remplacez les mots de passe par défaut des appareils connectés (comme les caméras)

(Voir également B : Botnet Eradication Project)

16. EUROPEAN CYBERSECURITY MONTH (ECSM)

Le European Cybersecurity Month ou Mois européen de la cybersécurité (ECSM) est la campagne annuelle de l'Union européenne visant à sensibiliser les internautes et les organisations à l'importance de la cybersécurité. Pendant un mois, l'ENISA, la Commission européenne et plus de 200 partenaires à travers l'Europe mènent une campagne autour de la cybersécurité.

La Belgique participe à l'ECSM, chaque année en octobre. (Voir également E : ENISA)

www.cybersecuritymonth.eu

17. EARLY WARNING SYSTEM (EWS)

Un **Early Warning System** (système d'alerte rapide, EWS) est déployé au sein de CERT.be afin d'informer rapidement les fournisseurs belges de services essentiels à propos des cybermenaces, des vulnérabilités et des incidents. L'EWS est alimenté grâce à des informations provenant de sociétés spécialisées et de partenaires de CERT.be, comme des CSIRTS étrangers. **Ces sources d'information ou feeds sont partagés sur la plateforme centrale que l'EWS partage avec les services de renseignements et de sécurité ainsi que les fournisseurs de services essentiels.** Grâce à ce dispositif, les avertissements en cas de menace sont transmis de manière rapide et uniforme et les mesures adéquates peuvent être prises. (Voir également O : Opérateur de services essentiels; A : ATP)

18. EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA)

L'ENISA est l'Agence européenne chargée de la cybersécurité. Il s'agit d'une agence de l'Union européenne, créée en 2004, ayant son siège à Athènes. L'Agence a pour mission de contribuer à sécuriser des réseaux d'information et des données. Elle joue un rôle capital pour les citoyens, les consommateurs, les entreprises et les organisations publiques dans toute l'Union européenne.

Le Centre pour la Cybersécurité Belgique travaille en étroite collaboration avec l'ENISA dans le cadre de l'exercice de cybercrise biennal (Cyber Europe), du Mois européen de la cybersécurité, etc... (Voir également E : European Cybersecurity Month)

19. FEDERAL COMPUTER CRIME UNIT (FCCU)

La Federal Computer Crime Unit (FCCU) est un service de la Police fédérale en charge de la criminalité informatique au niveau national. Sa mission est de protéger les citoyens contre toutes les formes de **cybercriminalité**, comme la pédophilie sur Internet, la fraude sur Internet et dans les télécoms, etc.

La FCCU est un partenaire important du Centre pour la Cybersecurité Belgique, même si ces deux organisations conservent leur pleine indépendance. On pense parfois à tort que le Centre pour la Cybersecurité Belgique est un service de la FCCU, ou inversement. La FCCU quant à elle est la cyberpolice qui accueille les victimes et recherche les auteurs.

https://www.police.be/5998/fr/a-propos/directions-centrales/federal-computer-crime-unit

20. FRAUDE AU CEO

Si la fraude au CEO n'est pas un phénomène nouveau, CERT.be reçoit régulièrement des signalements à propos de ce type de fraude. La fraude au CEO est une forme d'**escroquerie** par laquelle les cybercriminels contactent une entreprise (par téléphone ou par e-mail) en lui demandant d'effectuer un paiement important sur leur compte bancaire. Les cybercriminels prennent l'identité du CEO, du CFO ou d'une personne de confiance et demandent à un collaborateur du service financier ou de la comptabilité d'effectuer un **paiement urgent**.

Nos conseils :

- Les entreprises peuvent se prémunir contre les fraudes au CEO en informant correctement leurs collaborateurs et en les mettant en garde contre ce type de pratiques.
- Il est indispensable de mettre en place des procédures de paiement sans faille.

Pour en savoir plus, veuillez consulter notre brochure

21. FRAUDE VOIP

Le Voice over Internet Protocol, en abrégé Voice sur IP ou VoIP, n'est rien de plus qu'un appel téléphonique par Internet. Le VoIP est un nom collectif pour désigner les technologies permettant de téléphoner via les

réseaux IP. Les applications VoIP connues sont Skype, WhatsApp, Viber, Line et ChatON.

Cependant, une application VoIP peut être piratée. Il est alors possible d'écouter des conversations ou d'utiliser le compte pour téléphoner.

Nos conseils :

- Effectuez les mises à jour de tous les systèmes.
- Utilisez un pare-feu et un programme antivirus.
- Modifiez immédiatement les données de connexion par défaut.

22. GENERAL DATA PROTECTION REGULATION (GDPR) - OU RGPD

La **General Data Protection Regulation** (GDPR, ou Règlement général sur la protection des données – RGPD), porte sur la gestion et la sécurisation des données à caractère personnel des citoyens européens. Depuis le 25 mai 2018, les organisations sont tenues de préciser les **données à caractère personnel** qu'elles collectent et la manière dont elles utilisent, traitent et sécurisent ces données. Le GDPR contraint les organisations à prendre au sérieux la cybersécurité ; toute fuite de données doit être déclarée et peut aussi être pénalisée s'il s'avère que l'organisation n'a pas suffisamment sécurisé les données.

23. HTTPS

Le protocole **HTTP** est un protocole HyperText Transfer Protocol utilisé pour échanger des informations entre le navigateur et le serveur. Le **protocole HTTPS** fonctionne de la même façon, mais contient une sécurisation supplémentaire (HyperText Transfer Protocol Secure). Les données sont cryptées lors du transfert. Vous reconnaîtrez une adresse HTTPS au **cadenas vert** et à la mention « secure ». Nous considérons que les sites Internet qui utilisent uniquement le protocole HTTP ne sont pas sûrs. Par ailleurs, le protocole HTTPS n'est en rien un gage de site Internet sûr. Les cybercriminels dignes de ce nom peuvent tout à fait utiliser un protocole HTTPS sur leur site Internet falsifié. Veillez donc à toujours rester vigilant.

24. INDICE DE SANTÉ DIGITALE (ISD)

ISD 2019 = 70 %

L'**Indice de santé digitale** est un **indicateur des connaissances et du comportement** des Belges en matière de **cybersécurité**. L'ISD a été établi par le Centre pour la Cybersecurité Belgique, sur la base de la campagne annuelle de sensibilisation.

L'ISD mesure cinq aspects importants de la cybersécurité : l'utilisation correcte des mots de passe, la reconnaissance du phishing, la création de copies de sauvegarde et la réalisation de mises à jour et de scanners antivirus. Dans l'ISD, nous posons trois questions sur chacun de ces aspects, questions qui portent sur les connaissances et le comportement. Sur la base des réponses, le participant peut évaluer ses connaissances et son comportement et les comparer avec les réponses des autres participants. En outre, le participant reçoit des conseils sur mesure.

Les données ont été collectées jusqu'au 15 novembre 2019. À cette date, l'on a procédé au calcul de l'ISN pour 2019 : le score moyen était alors de 70 %. L'ISD sera également calculé pour les années 2020 et 2021.

Faites le test

25. INGÉNIERIE SOCIALE

L'ingénierie sociale est une technique de piratage des systèmes informatiques qui utilise les réactions psychologiques de l'homme.
L'ingénierie sociale n'est pas une attaque de la technologie proprement dite, mais de l'homme. Un agresseur joue sur des sentiments humains comme la peur, la curiosité, la compassion, l'euphorie...

L'ingénierie sociale est utilisée dans plusieurs cyberattaques, comme la fraude au CEO, l'arnaque par sextortion, le Microsoft scam et le phishing (Voir également F : Fraude au CEO ; M : Microsoft scam ; S : Sextortion scam; P : Phishing).

26. INTERNET OF THINGS (IOT)

D'ici 2020, 20 milliards d'appareils seront connectés à Internet dans le monde. En 2018, ce nombre était de 11 milliards. (Gartner, 2018)

De plus en plus d'appareils domestiques sont déclinés en une version **connectée à Internet** pour diverses raisons : si les caméras de surveillance sont les plus connues, les réfrigérateurs, les machines à café, les radiateurs et les panneaux solaires ne sont pas en reste. Et cela donne des gadgets amusants : vous pouvez chauffer votre maison ou encore suivre la production d'énergie solaire à distance. Mais cette avancée technologique n'est pas sans dangers. Certains de ces appareils ne sont pas suffisamment protégés contre les intrusions indésirables. Les cybercriminels peuvent en effet très aisément prendre le contrôle de certains appareils et, par exemple, regarder des images de votre caméra. En outre, les appareils en question peuvent être contaminés par un virus et faire partie intégrante d'un botnet, à l'insu du propriétaire.
Nos conseils :

- Remplacez les mots de passe par défaut par de nouveaux mots de passe forts
- Utilisez un réseau Wi-Fi sécurisé
- Effectuez les mises à jour (les fabricants améliorent leurs appareils et sont censés les mettre à jour)
- Utilisez un antivirus
- Désactivez les appareils que vous n'utilisez pas

(Voir également D : DDOS)

27. ISO 27001

La norme ISO 27001 est une norme internationale et une possibilité de certification qui spécifie formellement un ensemble d'activités de gestion des risques liés à l'information (généralement désignés « risques pour la sécurité de l'information ») pour un système de gestion de la sécurité de l'information (ou Information Security Management System - ISMS). L'ISMS est un cadre de gestion faîtière qui permet à l'organisation d'identifier, d'analyser et d'appréhender ses risques liés à l'information.

La norme couvre tous les types d'organisations (les entreprises commerciales, les organismes publics, les organisations sans but lucratif, des microentreprises aux grandes multinationales, etc.) et tous les secteurs ou marchés (la vente au détail, les banques, la défense, les soins de santé, l'enseignement et les autorités).

28. LOI NIS

Le 6 juillet 2016, les institutions européennes ont adopté une directive (n°2016/1148) concernant les mesures destinées à assurer un niveau commun élevé de **sécurité des réseaux et des systèmes d'information (NIS)** dans l'Union. Le Centre pour la Cybersécurité Belgique est chargé de **l'élaboration, de l'approbation et de l'implémentation effective** de la directive européenne NIS en Belgique.

Cette nouvelle loi, également appelée « loi NIS », prévoit d'**identifier des services essentiels** dans notre pays et leurs fournisseurs qui dépendent de la NIS et vise à garantir que ces fournisseurs prennent des mesures de sécurité suffisantes. En outre, la loi prévoit que ces fournisseurs de services essentiels signalent aux autorités nationales chargées de la cybersécurité tout incident majeur, comme une cyberattaque.
La loi NIS a été publiée au Moniteur belge le 3 mai 2019. Les opérateurs de services essentiels doivent être désignés au plus tard six mois après, soit le 3 novembre 2019. (Voir également O : Opérateur de services essentiels)

29. MICROSOFT SCAM

Chaque jour, au moins trois à quatre Belges sont victimes d'escrocs se présentant comme des techniciens de Microsoft ou Apple.

Une personne se faisant passer pour un employé de Microsoft ou d'Apple contacte la victime par téléphone. La personne en question

s'exprime en général dans un français ou un anglais bancal. L'escroc fait croire à la victime qu'il y a un **problème de sécurité** avec son ordinateur et lui propose de le sécuriser. Ensuite, il demande à la victime d'effectuer des actions précises : démarrer l'ordinateur, surfer sur un certain site Internet ou télécharger une application. Les criminels auront ainsi accès à l'ordinateur.

Nos conseils :

- Méfiez-vous toujours des appels téléphoniques d'entreprises qui vous demandent d'exécuter des actions sur l'ordinateur.
- Ne laissez pas un inconnu accéder à votre ordinateur à distance.
- N'effectuez pas de paiement, même de quelques euros, si un inconnu a accès à votre ordinateur.

https://www.safeonweb.be/fr/je-suis-contacte-par-un-inconnu-pour-un-probleme-de-pc

30. MISE À JOUR

8 % des Belges n'effectuent jamais de mise à jour (Safeonweb DGI, 2019)

Tout programme informatique contient des vulnérabilités. Une fois détectées, elles sont résolues dans des mises à jour de sécurisation. Par conséquent, les mises à jour régulières assurent une meilleure protection d'un appareil. Les personnes qui n'effectuent pas de mise à jour ou qui attendent trop longtemps avant d'y procéder augmentent le risque d'être prises pour cible par des cybercriminels.

Nos conseils :

- Lorsque vous recevez un message vous invitant à effectuer une mise à jour, faites-la le soir avant d'éteindre de votre appareil.
- La plupart des programmes peuvent être configurés pour exécuter automatiquement les mises à jour. Les mises à jour seront alors effectuées lors du redémarrage de votre ordinateur, sans intervention de votre part.
- Éteignez votre ordinateur au moins tous les deux jours.

En savoir plus sur https://www.safeonweb.be/fr/procedez-regulierement-des-mises-jour

31. MONARC

Afin d'assouplir la **gestion des risques** au sein des services publics, le Centre pour la Cybersecurité Belgique (CCB) met l'outil **MONARC** à disposition.

MONARC (Méthode Optimisée d'aNAlyse des Risques CASES) a pour objectif de permettre aux **organismes publics** (et aux entreprises) de **gérer** les **risques** auxquels ils sont confrontés. MONARC est à la fois une méthode et un instrument. C'est un outil facile d'utilisation qui offre un support maximal à l'utilisateur grâce à des base de données, des valeurs standard et un partage d'informations.

https://www.monarc.lu/

32. MOT DE PASSE

15 % des Belges utilisent le même mot de passe pour tous leurs comptes (Safeonweb DGI, 2019)

Les mots de passe les plus fréquemment utilisés sont : 123456, Azerty, admin, mot de passe... Si ces mots de passe sont faciles à retenir, ils aussi faciles à craquer, c'est-à-dire en moins d'une seconde. Utiliser des mots de passe forts est l'un des cinq conseils de base de Safeonweb.be.

Nos conseils :

- Utiliser des mots de passe sûrs
- Utilisez différents mots de passe pour tous vos comptes importants.
- Comme il est impossible de retenir une dizaine de mots de passe sûrs, vous pouvez utiliser un gestionnaire de mots de passe comme Lastpass, LogMeOnce, Myki, 1Password, Dashlane, etc.
- Utilisez la 2FA (Voir également T : Two factor Authentication)

En savoir plus sur
https://www.safeonweb.be/fr/utilisez-des-mots-de-passe-surs

33. NOTPETYA

NotPetya a fait sept victimes belges.

Le 27 juin 2017, CERT.be a été informé que des systèmes informatiques critiques avaient été supprimés dans plusieurs entreprises à travers le monde. En cause : une nouvelle variante de ransomware appelée NotPetya. C'est une mise à jour automatique d'un programme comptable légitime « MEDoc » qui était à l'origine de la propagation du virus NotPetya. Plusieurs entreprises internationales comptant une succursale en Ukraine utilisent le programme MEDoc et ont ainsi été infectées. Ensuite, NotPetya s'est répandu via le réseau interne à des succursales en dehors de l'Ukraine, y compris en Belgique.

Les conséquences de NotPetya sont restées limitées pour les entreprises belges. (Voir également R : Ransomware)

34. OPÉRATEUR DE SERVICES ESSENTIELS

Un **opérateur de services essentiels (OSE)** est une entité publique ou privée au sens de la loi sur les réseaux et les systèmes d'information, également appelée **loi NIS**. Un OSE est actif en Belgique dans l'un des six secteurs suivants : **énergie (électricité, gaz, pétrole**

spécifiquement), transports (air, rail, route, transport fluvial), soins de santé, eau potable, fournisseurs de services numériques et finances. Au sein de ces secteurs, un OSE fournit un service essentiel à l'organisation d'activités sociétales et/ou économiques critiques, ce service est tributaire des réseaux et des systèmes d'information et tout incident aurait un effet de distorsion non négligeable. Une entité qui remplit toutes ces conditions n'accède au rang d'OSE que lorsque les autorités la désignent officiellement comme telle. En regroupant toutes ces entreprises essentielles sous une définition et une loi, les autorités belges et européennes entendent améliorer globalement le niveau de sécurité. (Voir également N: loi NIS)

35. PHISHING

Le phishing est une escroquerie via de faux mails, sites Internet ou messages. Les cybercriminels tentent d'abuser de leurs victimes en abordant des sujets qui leur parlent ou en se faisant passer pour une personne de confiance. Par ailleurs, ils essaient bien souvent de jouer sur la peur. Reconnaître et signaler rapidement le phishing est l'un des cinq conseils de base de la cybersécurité de Safeonweb.be.

Nos conseils :

- Le mail est-il inattendu ? Si vous recevez sans raison un mail d'un expéditeur à qui vous n'avez rien acheté ou avec qui vous n'avez plus de contact depuis longtemps, etc. n'hésitez pas à vérifier.
- Le mail est-il urgent? Gardez la tête froide. Avez-vous réellement reçu une première mise en demeure ? Connaissez vous réellement cet ami en détresse?
- Où le lien sur lequel vous devez cliquer mène-t-il ? Placez votre souris sur le lien. Le nom du domaine, le mot avant « . be », « .com », « .eu », « .org », etc. et le premier « / », est-il réellement le nom de l'organisation ?
- Envoyez les messages suspects à suspect@safeonweb.be puis supprimez-les. (Voir également : suspect@safeonweb.be)

https://www.safeonweb.be/fr/apprenez-reconnaitre-les-e-mails-frauduleux

36. RANSOMWARE

Un ransomware ou virus à rançon est un virus installé sur un appareil sans l'autorisation du propriétaire. Le virus à rançon prend votre ordinateur et vos fichiers en otage et vous demande une rançon.

Nos conseils :

- Allez voir sur www.nomoreransom.org si la clé est disponible pour ce ransomware.
- Ne payez pas : vous n'aurez aucune garantie de réellement récupérer vos données de manière sécurisée. De plus, le risque que le virus n'ait pas été entièrement supprimé ou qu'il cache un moyen dérobé d'infecter à nouveau votre appareil à l'avenir reste réel.
- Évitez d'être victime d'un ransomware en procédant régulièrement aux mises à jour des appareils et en utilisant un antivirus. Effectuez régulièrement des sauvegardes, afin de pouvoir récupérer vos données en cas de perte. (Voir également B : Sauvegardes; U : Mises à jour; V : Scanner de virus)

https://www.safeonweb.be/fr/au-secours-mon-appareil-est-pris-en-otage
https://cert.be/sites/default/files/ransomware_2019_fr.pdf

37. RESPONSIBLE DISCLOSURE

Le 15 décembre 2018, le Centre pour la Cybersécurité Belgique a publié directives que les entreprises doivent suivre pour garantir une « coordinated vulnerability disclosure ».

La « Responsible disclosure », « Coordinated Vulnerability Disclosure » ou « stratégie de publicité coordonnée » est un accord entre une organisation et des tiers. Cet accord autorise, dans les limites fixées, les **pirates informatiques éthiques** à pénétrer dans les systèmes de l'organisation afin d'en tester la sécurité. De nos jours, la majorité des formes de piratage informatique éthique sont en effet interdites et les pirates, même s'ils ont de bonnes intentions, s'exposent à des poursuites pénales.

Une coordinated vulnerabilty disclosure reprend toutes les conditions auxquelles les deux parties s'engagent. Par exemple, l'organisme doit définir les systèmes qui peuvent être filtrés et la manière dont les pirates doivent signaler les vulnérabilités. Les pirates quant à eux s'engagent à ne pas divulguer les vulnérabilités au grand public, à ne pas installer de virus ou à ne pas voler de données.

38. SEXTORSION SCAM

Le sextortion scam ou arnaque par sextorsion est une forme d'**extorsion** dans laquelle les escrocs menacent de diffuser des **images à caractère sexuel** de la victime si elle ne leur verse pas **de l'argent**.

L'escroc affirme par exemple avoir trouvé sur Internet un mot de passe lui permettant d'accéder à des images vidéos d'actes sexuels de la victime. Ensuite, il demande de payer une certaine somme. Il est peu probable que l'escroc possède de telles images. La sextortion est **punissable** parce qu'il s'agit à la fois d'extorsion et d'escroquerie.

Nos conseils :

- Ne cédez pas aux demandes d'argent.
- Supprimez le mail.
- Si vous avez quand même payé, déposez plainte auprès de la police.

https://www.safeonweb.be/fr/je-suis-victime-dune-arnaque-par-sextorsion

39. SPOOFING

Le spoofing ou usurpation consiste en la falsification de caractéristiques dans le but d'adopter temporairement une fausse identité.
Le spoofing d'un site Internet consiste en l'imitation d'un site Internet existant et connu dans le but de critiquer l'organisation du site Internet original. En réalité, ce sont des utilisateurs finaux qui se cachent derrière ce site, par exemple à des fins frauduleuses (phishing).

40. SUSPECT@SAFEONWEB.BE

En 2020 nous sommes parvenus à faire bloquer plus que 4000 faux sites Internet.

En 2019, la population belge a transféré 1.700.000 e-mails à suspect@safeonweb.be. Les e-mails transférés sont automatiquement scannés par notre logiciel baptisé BeFish. Dans un premier temps, les e-mails sont identifiés à l'aide d'adresses URL. Ensuite, la technologie antivirus détecte les liens suspects dans ces e-mails, qui sont transmis à un partenaire externe qui fait bloquer les sites Internet de phishing via une collaboration avec quatre navigateurs : Google Chrome, Mozilla Firefox, Safari et Internet Explorer. (Voir également P : Phishing)

41. TWO FACTOR AUTHENTICATION

32 % des Belges n'ont jamais essayé le 2FA (Safeonweb DGI, 2019)

La Two Factor Authentication ou double authentification est un moyen sûr de vous connecter à un compte. La vérification en deux étapes utilise deux facteurs : en général un élément que vous connaissez (par exemple, un mot de passe) et un élément que vous possédez (par exemple, un téléphone portable) ou un élément biométrique (par exemple une empreinte digitale). Lors de la première étape, connectez-vous à votre compte à l'aide de votre mot de passe (Facebook, Twitter, Google, Microsoft, etc.). Lors de la deuxième étape, ce compte envoie un code à votre téléphone portable que vous introduisez pour accéder à votre compte. Il existe encore d'autres moyens d'authentification en deux étapes comme Google Authenticator App. Nous recommandons d'utiliser la vérification en deux étapes lorsqu'elle est disponible. C'est un moyen **simple et sûr** de vous connecter.

42. WANNACRY

Quelque 300 000 appareils infectés dans 150 pays. Avec ses **18 entreprises contaminées**, la Belgique n'a subi que des conséquences relativement limitées, en comparaison avec d'autres pays.

En mai 2017, le monde a été secoué par l'apparition du ransomware WannaCry. Des systèmes ont été infectés aux quatre coins du globe avec une rapidité sans précédent. La vitesse à laquelle le virus s'est propagé s'explique notamment par le fait que les assaillants ont exploité une vulnérabilité affectant les systèmes IT qui avait déjà été détectée par la NSA et qui était tombée dans les mains du groupe de hackers « Shadow Brokers **»** . Peu après la publication de cette vulnérabilité, WannaCry a surgi sur le devant de la scène, avec les conséquences que l'on connaît. (Voir également R : Ransomware)

https://www.safeonweb.be/fr/au-secours-mon-appareil-est-pris-en-otage

CERT.be
Federal Cyber Emergency Team
Rue de la Loi, 16
1000 Bruxelles
info@certbe

Centre pour la Cybersécurité Belgique
Rue de la Loi, 16
1000 Bruxelles
info@ccb.belgium.be

Editeur responsable
Centre pour la Cybersécurité Belgique
M. De Bruycker, Directeur
Rue de la Loi, 16
1000 Bruxelles

Dépot légal
D/2020/14828/005

Date, 15/03/2020