CENTRE FOR
CYBER SECURITY
BELGIUM

UNDER THE AUTHORITY OF
THE PRIME MINISTER

HET ABC VAN HET CCB

CYBERVEILIGHEIDSJARGON IN 42 ANTWOORDEN

.be

VOOR WIE IS DIT ABC BEDOELD?
Voor journalisten en geïnteresseerden in cyberveiligheid.

WAT KAN JE HIER VINDEN?
42 principes die een antwoord geven op alles wat je over cyberveiligheid in België wil weten.

HOE ACTUEEL IS DIT?
Deze gids is afgewerkt op 15 maart 2020.

WIE IS DE AUTEUR?
Dit ABC is opgemaakt onder de redactie van Andries Bomans en Katrien Eggers, communicatieverantwoordelijken van Centrum voor Cybersecurity België met de hulp van vele collega's.

OVER HET CENTRUM VOOR CYBERSECURITY BELGIË
Het Centrum voor Cybersecurity België (CCB) is de nationale autoriteit voor cyberveiligheid in België. Het CCB superviseert, coördineert en waakt over de toepassing van de Belgische cyberveiligheidsstrategie. Door optimale informatie-uitwisseling kunnen bedrijven, de overheid, aanbieders van essentiële diensten en de bevolking zich gepast beschermen.
www.ccb.belgium.be

OVER CERT.BE
Het federale Computer Emergency Response Team, kortweg CERT.be, is de operationele dienst van het Centrum voor Cybersecurity België (CCB). CERT.be heeft als opdracht het online opsporen, observeren en analyseren van veiligheidsproblemen en de verschillende doelgroepen hierover informeren.
www.cert.be

Contactpersonen voor de pers
Andries Bomans: 0471 66 00 06, andries.bomans@ccb.belgium.be
Katrien Eggers: 0485 765 336, katrien.eggers@cert.be

CONTENTS

1. 5G

5G is 100 tot 200 keer sneller dan 4G

Vandaag zijn de meeste internetgebruikers verbonden met het 4G netwerk, maar in de toekomst stappen we over naar het veel snellere 5G netwerk. De medische wereld, zelfrijdende auto's en alle andere technologische toepassingen die nood hebben aan real-time connectie wachten met ongeduld op de komst van 5G omdat het een grote sprong voorwaarts betekent in de mogelijkheden van hun vooruitgang.

Deze technomogische vooruitgang biedt nieuwe mogelijkheden maar moet ook voldoende beveiligd worden. Het CCB volgt dit dossier vanuit technisch oogpunt op. Andere partners onderzoeken de economische en geopolitieke consequenties van de uitrol van het 5G netwerk.

2. AANBIEDER VAN ESSENTIËLE DIENSTEN

Een **aanbieder van essentiële diensten (AED)** is een publieke of private entiteit zoals gedefinieerd in de wet op Netwerk en Informatiesystemen, kortweg de **NIS-wet**. Een AED is actief in België in één van de volgende 6 sectoren: **energie** (elektriciteit, gas, olie), **vervoer** (lucht, spoor, weg, watertransport), **gezondheidszorg, drinkwater, digitale dienstverleners en financiën**. Binnen deze sectoren moet een entiteit aan drie criteria voldoen om een AED te zijn: ze moet een dienst aanbieden die van essentieel belang is voor kritieke maatschappelijke en/of economische activiteiten, die dienst is afhankelijk van netwerk- en informatiesystemen en een incident op deze systemen zou een aanzienlijk verstorend effect hebben. Een entiteit die aan al deze voorwaarden voldoet is pas een AED wanneer ze door de overheid officieel is aangewezen. Door al deze essentiële bedrijven te groeperen onder een definitie en een wet, willen de Belgische en Europese overheden een groter algemeen veiligheidsniveau creëren. (Lees ook N: NIS-wet)

3. ADVANCED PERSISTENT THREAT (APT)

Advanced Persistent Threats, of **APT's**, is een verzamelnaam voor geavanceerde en doelgerichte cyberaanvallen. Een kenmerk van een APT is dat het zich gedurende lange tijd ongemerkt in een netwerk kan ophouden voordat het daadwerkelijk tot actie over gaat. Net omdat APT's zo geavanceerd te werk gaan, gaat men ervan uit dat ze het werk zijn van naties en niet van particulieren. APT's worden veelal ingezet voor politieke, economische of industriële **spionage** of **cyberaanvallen**. Advanced Persistent Threats worden nauw opgevolgd door CERT.be via het Early Warning System zodat diensten die geviseerd worden, snel

ingelicht zijn en de beveiliging kunnen opvoeren. (lees ook A: Attributie van een cyberaanval; E: Early Warning System)

4. ATTRIBUTIE VAN EEN CYBERAANVAL

Attributie van een cyberaanval is het **aanwijzen** van de **dader**. Het vinden van online sporen via **forensisch onderzoek** is een delicaat werk van lange adem. Sporen zijn **moeilijk traceerbaar**. Staten voeren wel eens aanvallen uit op andere staten vanuit geopolitieke motieven met de bedoeling het verwerven van strategische informatie via spionage, beïnvloeding van de publieke opinie of democratische processen of zelfs sabotage van essentiële diensten. De attributie van een aanval op een staat door een andere staat is moeilijk met absolute zekerheid aan te tonen en ligt bovendien **diplomatiek gevoelig**. Het attribueren van een cyberaanval hoort niet tot de opdracht van het CCB, maar gebeurt naar aanleiding van een gerechtelijk onderzoek of door de bevoegde diensten. (Lees ook A: Advanced Persistent Threat)

5. BACK-UP

22 % van de Belgen maakt nooit een back-up (Safeonweb DGI, 2019)

Een back-up is een **reservekopie** van gegevens die belangrijk zijn voor een persoon. Met een back-up kan men **gegevens terugzetten** als men een virus heeft of als een ransomware of gijzelvirus de toegang tot gegevens blokkeert en er geld voor vraagt. Back-ups maken is 1 van de 5 **basisregels** voor cyberveiligheid die het Centrum Voor Cybersecurity België via Safenweb.be voorstelt.

Ons advies:

- Maak regelmatig een back-up van de bestanden die belangrijk zijn;
- Je kan kiezen voor een back-up **in de cloud** of op een **externe harde schijf**;
- Zorg dat er voldoende afstand is tussen je bestanden en de back-up. Koppel je back-up minstens los van je computer. Een back-up in de **cloud** is een goede keuze omdat die voor afstand zorgt. (Lees ook R: Ransomware)

https://www.safeonweb.be/nl/maak-back-ups

6. BASELINE SECURITY GUIDELINES

De **Baseline Security Guidelines** (BSG) geeft minimale **richtlijnen** voor de implementatie of evaluatie van een **informatiebeveiligingsplan** voor **overheidsdiensten**.

Deze BSG is ontwikkeld door het Centrum voor Cybersecurity Belgium in overleg met experts van verschillende overheidsdiensten en externe consultants en houdt rekening met bestaande normen zoals ISO 27001 en ISO 27002. (lees ook I: ISO 27002)

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

7. BOTNET ERADICATION PROJECT

Het **Botnet Eradication project** heeft als doel **botnets** in België te **verwijderen**. Het doel is om de geïnfecteerde gebruikers (zowel thuisgebruikers als bedrijven) op de hoogte te brengen van het feit dat zij geïnfecteerd zijn en deel uitmaken van een botnet. De gebruikers worden ook op de hoogte gebracht over mogelijke manieren om hun systeem te desinfecteren. (lees ook D: DDOS aanval)

8. CEO FRAUDE

CEO fraude is geen nieuw fenomeen maar CERT.be krijgt regelmatig meldingen van deze manier van oplichting. CEO fraude is een vorm van **oplichting** waarbij cybercriminelen een onderneming contacteren (telefonisch of per e-mail) met de vraag een belangrijke betaling uit te voeren naar hun bankrekening. De cybercriminelen nemen de identiteit aan van de CEO, CFO of een vertrouwde persoon en vragen een medewerker van de financiële dienst of boekhouding om een **dringende betaling** uit te voeren.

Ons advies:

- Bedrijven kunnen zich wapenen tegen CEO fraude door hun medewerkers goed te informeren en te waarschuwen voor deze manier van handelen;
- Waterdichte procedures voor betalingen zijn een must.

Lees meer in onze brochure

9. CRYPTOJACKING

Het aantal waarnemingen van **coinminers** bij eindgebruikers is in 2017 met 8500 procent toegenomen. Cryptomunten zijn virtuele munten, de bekendste is de Bitcoin. Om een Bitcoin of een andere cryptomunt te verkrijgen, moet een computer veel berekeningen uitvoeren die een grote hoeveelheid energie (CPU) vereisen. Voor deze berekeningen wordt een computer of smartphone beloond met Bitcoins. Dit proces wordt **cryptomining** genoemd.

Tegenwoordig proberen criminelen toegang te krijgen tot toestellen om het dan zonder medeweten van de eigenaar te kunnen gebruiken om **cryptomunten** te verzamelen. Dit fenomeen heet **cryptojacking**.

https://www.safeonweb.be/nl/mijn-toestel-wordt-gebruikt-voor-cryptojacking

10. CYBERGUIDE

150 cyberveiligheidsmaatregelen gebundeld in 1 gids

De CCB Cyberguide is een online **referentiegids** om **organisaties en ondernemingen** te helpen bij een betere **cyberveiligheidsstrategie**. Via **4 categorieën** bieden we een overzicht van basis- en meer geavanceerde cyberveiligheidsmaatregelen. Voor elke maatregel is er een beschrijving, praktische informatie en nuttige links naar websites en tools. Samen worden meer dan 150 cyberveiligheidsmaatregelen voorgesteld. Deze gids is een onmisbaar instrument voor organisaties en ondernemingen die werk willen maken van een beleid rond **cyberveiligheid**.

Lees de volledige gids

11. CYBERSECURITY ACT

Op 10 december 2018 hebben de Europese instellingen een politiek akkoord bereikt over de zogenaamde **Cybersecurity Act**.

De Cybersecurity Act heeft twee hoofddoelstellingen: de wet **versterkt het mandaat en de middelen** van het **Europees Agentschap voor Cybersecurity** (ENISA) en legt een kader vast voor Europese **cybersecurity-certificaten** voor producten, processen en diensten die in de EU worden ingevoerd. Het doel van dit kader is het verbeteren van de veiligheid van online diensten en technologieën.

De nieuwe regels zijn nodig om de technologie van geconnecteerde toestellen of ook wel **the Internet of Things** te beveiligen. Het is de bedoeling om via certificering bedrijven te motiveren om te investeren in cybersecurity en dit te kunnen gebruiken als concurrentievoordeel.
(Lees ook E: ENISA)

12. CYBER SECURITY COALITION

Sinds 2015 brengt de **Cyber Security Coalition** vertegenwoordigers van de overheidssector, de privésector en de academische wereld samen in één organisatie. Die benadering is uniek in België en zorgt ervoor dat ervaring en goede praktijken rond onder meer awareness, privacy, NIS, Cloud, Enterprise Security Architecture, Crypto en certification worden uitgewisseld.

De directeur van het Centrum Voor Cybersecurity België werd op 7 december 2015 lid van de raad van bestuur van de Cyber Security Coalition Belgium.

https://www.cybersecuritycoalition.be/

13. CYBERVEILIGHEID

Het Centrum Voor Cybersecurity België is verantwoordelijk voor het algemene **cyberveiligheid**sbeleid. Het CCB superviseert, coördineert en waakt over de toepassing van de Belgische cyberveiligheidsstrategie. Door optimale informatie-uitwisseling kunnen bedrijven, de overheid, aanbieders van essentiële diensten en de bevolking zich gepast beschermen. Het is de opdracht van het CCB om ervoor te zorgen dat het internet in ons land veilig blijft en dat de internetgebruiker voldoende geïnformeerd is om veilig online te zijn.

14. DIGITALE GEZONDHEIDSINDEX (DGI)

DGI 2019 = 70 %

De **Digitale Gezondheidsindex** is een **indicator** voor **de kennis en het gedrag** van de Belgen rond **cyberveiligheid**. De DGI is opgemaakt door het Centrum Voor Cybersecurity België, in functie van de jaarlijkse **awareness campagne**.

De DGI meet vijf belangrijke aspecten van cyberveiligheid: goed gebruik van wachtwoorden, phishing herkennen, back-ups maken, updates uitvoeren en virusscans gebruiken. De test verzamelde gegevens tot 15 november 2019. Op dat ogenblik werd de DGI voor 2019 berekend: de gemiddelde score was dan 71 %. De DGI zal ook voor 2020 en 2021 berekend worden.

Doe de test

15. DIGITAL SINGLE MARKET (DSM)

De **digitale eengemaakte markt** (Digital Single Market, of DSM) is de algemene strategie van de Europese Commissie rond beleid en investering in de digitale wereld. De DSM-strategie werd gelanceerd in 2015 en geüpdatet in 2017 en is van toepassing op vele sub-domeinen, gaande van e-commerce, auteursrecht, geoblocking tot cybersecurity. We denken aan: afschaffing van roamingkosten binnen de EU, de GDPR (AVG) wetgeving, de copyright wetgeving, de NIS-richtlijn of de cyber act.

De DSM-strategie is in het algemeen gebaseerd op drie pijlers: betere toegang tot digitale goederen en diensten, het creëren van de juiste voorwaarden en een gelijk speelveld om digitale netwerken en innovatieve diensten te realiseren en het maximaliseren van het groeipotentieel van de digitale economie.

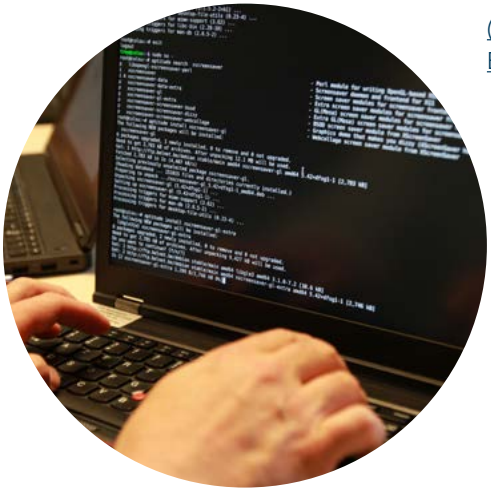
16. DISTRIBUTED DENIAL OF SERVICE (DDOS)

Een Distributed Denial of Service aanval, ook wel **DDoS-aanval**, is een cyberaanval waarbij ontzettend veel verkeer naar computers, computernetwerken of servers wordt verstuurd waardoor deze verstoord worden.

Om een DDoS aanval uit te voeren, wordt gebruik gemaakt van een **botnet**. Dit is een groot netwerk van computers of geconnecteerde toestellen (zogenaamde **bots**) die besmet zijn met malware. Vanuit een centraal punt (de **bot-herder**) kan een aanvaller deze computers aansturen om een bepaalde opdracht uit te voeren. Internetgebruikers zijn er zich niet van bewust dat hun toestellen deel kunnen uitmaken van een botnet.

Ons advies om geen bot te worden:

- Voer altijd updates uit;
- Gebruik altijd een virusscan;
- Vervang default wachtwoorden van geconnecteerde toestellen (bv. camera's).



(Lees ook B: Botnet Eradication Project)

17. EARLY WARNING SYSTEM (EWS)

Binnen CERT.be wordt een **Early Warning Systeem (EWS)** uitgerold om de Belgische aanbieders van essentiële diensten snel te informeren over cyberdreigingen, kwetsbaarheden en incidenten. Het EWS wordt gevoed met informatie van gespecialiseerde firma's en van de partners van CERT.be, zoals bijvoorbeeld buitenlandse CSIRTS. Deze informatiebronnen of feeds worden via het centrale EWS platform gedeeld **met inlichtingen- en veiligheidsdiensten en aanbieders van essentiële diensten.** Waarschuwingen bij dreigingen worden zo op een snelle en uniforme manier uitgestuurd, waardoor er gepaste maatregelen kunnen genomen worden. (lees ook A: Aanbieders van essentiële diensten; A: APT's)

18. EUROPEAN CYBERSECURITY MONTH (ECSM)

De European Cybersecurity Month of de Europese maand van de cyberbeveiliging (ECSM) is de jaarlijkse campagne van de Europese Unie waarmee internetgebruikers en organisaties bewust worden gemaakt van het belang van cyberbeveiliging. ENISA, de Europese Commissie en meer dan 200 partners uit heel Europa voeren een maand lang **campagne rond cyberveiligheid**.

Ook België neemt jaarlijks deel aan de ECSM in oktober. (Lees ook E: ENISA)
www.cybersecuritymonth.eu

19. EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA)

ENISA is het Europees Agentschap voor Cybersecurity. Het is een agentschap van de Europese Unie, opgericht in 2004 en heeft haar hoofdkantoor in Athene. Het agentschap heeft tot taak informatienetwerken en gegevens te helpen beveiligen. Dit is van belang voor de burgers, consumenten, bedrijven en overheidsorganisaties in de gehele Europese Unie.

Het Centrum Voor Cybersecurity België werkt nauw samen met ENISA in het kader van de 2-jaarlijkse cybercrisis oefening (Cyber Europe), bij de jaarlijkse European Cybersecurity Month, enz… De directeur van het Centrum voor Cybersecurity België maakt deel uit van de management board van ENISA. (lees ook E: European Cybersecurity Month)

20. FEDERAL COMPUTER CRIME UNIT (FCCU)

De Federal Computer Crime Unit (FCCU) is een **politiedienst** van de **Federale Politie** die belast is met ICT-criminaliteit op nationaal niveau. Hun opdracht is de burgers te beschermen tegen alle vormen **cybercriminaliteit**, bv. pedofilie op het internet, internet- en telecomfraude…

Het FCCU is een belangrijke partner van het Centrum Voor Cybersecurity België, maar beiden werken volledig onafhankelijk. Er wordt onterecht soms gedacht dat het Centrum Voor Cybersecurity België een dienst is van het FCCU of omgekeerd. Het FCCU is de cyberpolitie die slachtoffers opvangt, en op zoek gaat naar de daders.

https://www.politie.be/5998/nl/over-ons/centrale-directies/federal-computer-crime-unit

21. GENERAL DATA PROTECTION REGULATION (GDPR) – OF AVG

De **General Data Protection Regulation** (GDPR, of ook **Algemene Verordening Gegevensbescherming – AVG**) gaat over het beheer en de beveiliging van persoonlijke gegevens van Europese burgers. Sinds 25 mei 2018 moeten organisaties aantonen welke **persoonsgegevens** ze verzamelen en hoe ze deze gegevens gebruiken, verwerken en beveiligen. De GDPR dwingt organisaties om cyberveiligheid serieus te nemen, datalekken moeten gerapporteerd worden en kunnen ook bestraft worden als blijkt dat de organisatie de data onvoldoende beveiligde.

22. HTTPS

Het **HTTP**-protocol staat voor **HyperText Transfer Protocol** en wordt gebruikt om informatie uit te wisselen tussen browser en server. Het **HTTPS-protocol** doet hetzelfde, maar er wordt extra beveiliging toegevoegd (HyperText Transfer Protocol Secure). Aan de hand van versleuteling worden de data geëncrypteerd. Een HTTPS-adres herken je door **het groene slotje** en de vermelding 'secure'. Websites die enkel het HTTP-protocol gebruiken, beschouwen we als onveilig. Anderzijds is het HTTPS-protocol geen garantie op een veilige website. Cybercriminelen die hun werk goed doen, kunnen hun vervalste website net zo goed van een HTTPS-protocol voorzien. Het blijft dus altijd opletten geblazen.

23. INTERNET OF THINGS (IOT)

Alle Vlamingen beschikken over minstens één smart toestel (Imec, 2019)

Steeds meer toestellen kunnen om allerlei redenen aan het **internet** worden **aangesloten**: beveiligingscamera's zijn de meest bekende, maar ook koelkasten, koffiezetapparaten, verwarmingstoestellen en zonnepanelen worden steeds vaker met het internet verbonden. Dit levert leuke gadgets op: je kan je huis van op afstand verwarmen, je kan de productie van zonne-energie van op afstand opvolgen, enz… maar er zijn ook gevaren. Niet al deze toestellen zijn voldoende beveiligd tegen ongewenste indringers. Bij sommige toestellen is het voor cybercriminelen zeer eenvoudig om de controle over te nemen en bv. mee te kijken naar camerabeelden. De toestellen kunnen ook besmet worden met een virus en deel gaan uitmaken van een botnet, zonder dat de eigenaar zich van enig kwaad bewust is.

Ons advies:

- Default wachtwoorden vervangen door nieuwe sterke wachtwoorden;
- Beveiligde wifi gebruiken;
- Updates uitvoeren (fabrikanten verbeteren hun toestellen en daarvoor zijn updates bedoeld);
- Een virusscan gebruiken;
- Toestellen uitschakelen als ze niet in gebruik zijn.

(Lees ook D: DDOS).

24. ISO 27001

ISO 27001 is een internationale norm en certificatie die formeel voor een Information Security Management System (ISMS) een reeks activiteiten over het beheer van informatierisico's specifieert. Het ISMS is een overkoepelend managementkader waarmee de organisatie haar informatierisico's identificeert, analyseert en aanpakt.

ISO 27001 is geschikt voor alle soorten organisaties (commerciële bedrijven, overheidsinstellingen, non-profitorganisaties), en alle sectoren of markten (bijv. retail, banken, defensie, gezondheidszorg, onderwijs en overheid). (lees ook B: Baseline Security Guidelines)

25. MICROSOFT SCAM

Dagelijks worden minstens 3 à 4 Belgen het slachtoffer van oplichters die zich voordoen als technici van Microsoft of Apple.

Het slachtoffer wordt opgebeld via de vaste lijn door iemand die zich voordoet als **medewerker van Microsoft of Apple**. Vaak spreekt de persoon gebrekkig Nederlands of enkel Engels. Deze oplichter laat het slachtoffer geloven dat er een **veiligheidsprobleem** is met de computer en stelt voor om de computer te beveiligen. Daarna vraagt hij om bepaalde handelingen te doen: de computer opstarten, naar een bepaalde website surfen of een applicatie downloaden. Op die manier krijgen de criminelen toegang tot de computer.

Ons advies:

- Wantrouw altijd telefoonoproepen van bedrijven die vragen om een aantal acties uit te voeren op de computer;
- Laat je computer niet overnemen door iemand die je niet kent;
- Voer geen betalingen uit, ook niet van enkele euro's, terwijl een onbekende de computer heeft overgenomen.

https://www.safeonweb.be/nl/ik-word-opgebeld-door-een-onbekende-voor-een-pc-probleem

26. MONARC

Om **risicomanagement** in de overheidsdiensten te versoepelen, biedt het Centrum voor Cybersecurity Belgium (CCB) de tool **MONARC** aan.

MONARC (Méthode Optimisée d'aNAlyse des Risques CASES) heeft tot doel **overheidsinstellingen** (en ondernemingen) in staat te stellen de **risico's** waarmee zij geconfronteerd worden te **beheersen**. MONARC is tegelijkertijd een methode en een instrument. Het is gebruiksvriendelijk en biedt de gebruiker maximale ondersteuning door middel van kennisbanken, standaardwaarden en het delen van informatie.

https://www.monarc.lu/

27. NIS-WET

Op 6 juli 2016 keurden de Europese instellingen de richtlijn (nr. 2016/1148) goed over de maatregelen om een hoog gemeenschappelijk niveau van **Netwerk- en Informatieveiligheid (NIS)** in de EU te verzekeren. Het Centrum Voor Cybersecurity België was verantwoordelijk voor de **uitwerking, goedkeuring en effectieve uitvoering** van de Europese NIS-richtlijn in België.

Deze nieuwe wet, kortweg ook 'NIS-wet' genoemd, voorziet het **identificeren van de essentiële diensten** in ons land.

De NIS-wet is op 3 mei 2019 gepubliceerd in het Belgisch Staatsblad. De aanbieders van essentiële diensten moeten 6 maanden later aangeduid zijn, dus tegen 3 november 2019. (lees ook A: Aanbieder van essentiële diensten)

28. NOTPETYA

NotPetya maakte 7 Belgische slachtoffers.

Op 27 juni 2017 kreeg CERT.be informatie dat kritieke informaticasystemen uitgeschakeld zijn bij bedrijven in verschillende landen. De oorzaak was een nieuwe variant van **ransomware** die de naam **NotPetya** kreeg. Een automatische update van een legitiem boekhoudingsprogramma MEDoc lag aan de basis van de verspreiding van het NotPetya virus. Meerdere internationale bedrijven met een vestiging in Oekraïne gebruikten MEDoc en raakten op die manier geïnfecteerd waarna NotPetya zich via het intern netwerk verspreidde naar vestigingen ook buiten Oekraïne, waaronder België.

NotPetya maakte indruk maar de gevolgen voor de Belgische organisaties en ondernemingen bleven beperkt. (lees ook R: Ransomware)

29. PHISHING

Phishing is **online oplichting** door **valse e-mails, websites of berichten**. Cybercriminelen proberen misbruik te maken van iets waar het slachtoffer in gelooft of van iemand die hij kent en vertrouwt. Ze proberen ook vaak in te spelen op angst. Phishing snel herkennen en melden is één van de 5 basistips voor cyberveiligheid van Safeonweb.be.

Ons advies:

- Komt het bericht onverwacht? Krijg je zonder reden een bericht van deze afzender: je kocht niets, had lang geen contact, enz. Controleer zeker verder.
- Is het bericht dringend? Hou je hoofd koel: kreeg je echt een eerste aanmaning tot betaling? Ken je die 'vriend in nood'.
- Naar waar leidt de link waar je moet op klikken? Zweef met je muis over de link. Is de domeinnaam, het woord voor.be,.com,.eu,.org, … en voor de allereerste slash "/", ook echt de naam van de organisatie?
- Stuur verdachte berichten door naar verdacht@safeonweb.be en verwijder ze daarna. (lees ook V: verdacht@safeonweb.be)

https://www.safeonweb.be/nl/leer-valse-mails-herkennen

30. RANSOMWARE

Ransomware is een **virus** dat wordt geïnstalleerd op een toestel zonder dat de eigenaar daarvoor toestemming gaf. Het **gijzelvirus** houdt het toestel en de bestanden gegijzeld (**geëncypteerd**) en vraagt **losgeld**.

Ons advies:

- Voorkom dat je slachtoffer wordt van ransomware door toestellen steeds up to date te houden en een virusscan te gebruiken. Maak op regelmatige basis back-ups zodat je bij verlies je gegevens kan terug plaatsen;
- Betaal niet: je hebt geen enkele garantie dat je effectief op een veilige manier je gegevens terugkrijgt. Bovendien bestaat het risico dat het virus niet helemaal verdwenen is of dat er achterpoortjes worden ingebouwd om je in de toekomst opnieuw te besmetten;
- Bekijk op www.nomoreransom.org of de ontcijfersleutel voor deze ransomware beschikbaar is.

(lees ook B: Back-ups; U: Updates; V: Virusscan)
https://www.safeonweb.be/nl/help-mijn-toestel-gegijzeld
https://cert.be/sites/default/files/ransomware_2019_nl.pdf

31. RESPONSIBLE DISCLOSURE

Op 15/12/2018 publiceerde het CCB richtlijnen voor ondernemingen voor een coordinated vulnerability disclosure.

Responsible disclosure, Coordinated Vulnerability Disclosure of gecoördineerd bekendmakingsbeleid is een afspraak tussen een organisatie en derden. Het geeft **ethische hackers** binnen afgebakende grenzen de toestemming om de systemen van de organisatie binnen te dringen om de veiligheid ervan te testen. Vandaag zijn de meeste vormen van ethisch hacken immers verboden en lopen hackers, ook met goede bedoelingen, het risico op strafrechtelijke vervolging.

Een coordinated vulnerabilty disclosure bevat alle voorwaarden waar beide partijen zich toe verbinden. De organisatie legt bv. vast welke systemen geïnfiltreerd mogen worden en op welke manier hackers kwetsbaarheden moeten melden. De hacker van zijn/haar kant verbindt zich ertoe om de kwetsbaarheden niet openbaar te maken, om geen virussen te installeren of gegevens te stelen.

32. SEXTORTION SCAM

Sextortion scam is een vorm van **afpersing** waarbij de afpersers dreigen om **seksueel getinte beelden** van het slachtoffer te verspreiden als die niet met **geld** over de brug komt.

De afperser stelt bijvoorbeeld dat hij op het internet een paswoord vond waarmee hij toegang kreeg tot camerabeelden van seksuele handelingen van het slachtoffer. Hierna vraagt de afperser een som te betalen. Het is onwaarschijnlijk dat de afperser werkelijk dergelijke beelden bezit.

Ons advies:

- Ga niet in op de vraag om een som geld te betalen;
- Verwijder het bericht;
- Dien een klacht in bij de politie, als je wel betaalde.

https://www.safeonweb.be/nl/ik-word-afgeperst-sextortion

33. SOCIAL ENGINEERING

Social engineering is een **techniek** waarbij een hacker een aanval doet op computersystemen door in te spelen op de **psychologische reacties** van de mens. Social engineering is geen aanval op de technologie zelf maar op de mens. Een aanvaller speelt in op menselijke gevoelens zoals angst, nieuwsgierigheid, medelijden, euforie…

Social engineering wordt bij verschillende cyberaanvallen gebruikt zoals CEO fraude, sextortion scam, Microsoft scam en phishing (lees ook C: CEO fraude; M: Microsoft scam; S: Sextortion scam; P: Phishing).

34. SPOOFING

E-mail spoofing is het verzenden van e-mails waarbij het e-mail adres van de afzender vervalst wordt. Dat wil zeggen dat de eigenlijke afzender bijvoorbeeld je eigen e-mailadres kopieert en gebruikt om je om de tuin te leiden.

Deze techniek wordt vaak gebruikt voor spam, phishing en de sextortion scam. De auteur doet dit om zijn eigen identiteit te verbergen, om je te misleiden of om je te doen geloven dat je mailbox werd gehackt. (lees ook P: Phishing; S: Sextortion scam)

35. TWO FACTOR AUTHENTICATION

32 % van de Belgen heeft nog nooit 2FA uitgeprobeerd (Safeonweb DGI, 2019)

Two Factor Authentication of ook wel **verificatie in twee stappen** is een veilige manier om je aan te melden op een account. Verificatie in twee stappen maakt gebruik van **2 factoren:** bijvoorbeeld van iets dat je weet (bv. een wachtwoord) en iets dat je hebt (bv. een gsm) of iets dat je bent (bv. vingerafdruk). In de eerste stap log je met je wachtwoord in bij je account (Facebook, Twitter, Google, Microsoft…). In de tweede stap stuurt die account bv. een code naar je gsm die je invult om toegang te krijgen tot je account. Er bestaan ook andere manieren voor verificatie in 2 stappen zoals bv. via Google Authenticator App of ITSME. Wij raden aan om verificatie in 2 stappen te gebruiken als ze beschikbaar is. Het is een **eenvoudige en veilige** manier om je aan te melden.

36. UPDATE

8 % van de Belgen voert nooit updates uit (Safeonweb DGI, 2019)

Elke computerprogramma bevat **kwetsbaarheden**. Zodra deze ontdekt worden, worden die in beveiligingsupdates opgelost. Met **regelmatige updates** blijft een toestel dus **beter beschermd**. Wie geen updates doet of daar te lang mee wacht, verhoogt het risico dat cybercriminelen hen te slim af zijn.

Ons advies:

- Wanneer je een melding krijgt om een update uit te voeren, doe je dit het best die avond nog, voor je je toestel afsluit;
- De meeste programma's kan je instellen om automatisch updates uit te voeren. De updates worden dan uitgevoerd bij het heropstarten van je computer zonder dat je daarvoor iets moet doen;
- Zet ten minste om de paar dagen de computer eens uit.

Meer info op https://www.safeonweb.be/nl/doe-regelmatig-updates

37. VERDACHT@SAFEONWEB.BE

In 2019 konden wij meer dan 4000 valse websites laten blokkeren.

In 2019 stuurde de Belgische bevolking 1.700.000 e-mails door naar **verdacht@safeonweb.be**. De doorgestuurde e-mails worden automatisch gescand. In een eerste fase worden de berichten met URL's geïdentificeerd. Daarna detecteert de anti-virustechnologie verdachte links in deze e-mails, die worden doorgestuurd naar een externe partner. Deze laat de **phishing websites blokkeren** via een samenwerking met 4 browsers: Google Chrome, Mozilla Firefox, Safari en Internet Explorer. (lees ook P: Phishing)

38. VIRUSSCAN

78 % van de Belgen heeft een virusscanner (Safeonweb DGI, 2019)

Een **virusscanner** zorgt ervoor dat een computer niet vatbaar is voor **virussen** en dus beter **beschermd** is voor cyberaanvallen. Een virusscan gebruiken is 1 van de 5 basis regels voor cyberveiligheid.

Ons advies:

- Ook al biedt geen enkele virusscanner 100 % bescherming, toch blijft het cruciaal om er een te installeren;
- Jammer genoeg worden elke dag nieuwe virussen ontwikkeld. Daarom is het noodzakelijk om altijd de meest recente updates van een virusscanner te installeren.

https://www.safeonweb.be/nl/scan-je-computer

39. VOIP FRAUDE

Voice over Internet Protocol, kortweg Voice over IP of VoIP, is niet meer dan 'telefoneren via het internet'. VoIP is een verzamelnaam voor technologieën om te telefoneren via IP-netwerken. Bekende applicaties voor VoIP zijn Skype, WhatsApp, Viber, Line en ChatON.

Een VoIP applicatie kan echter gehackt worden. Het is dan mogelijk om gesprekken af te luisteren of om de account te gebruiken om te telefoneren.

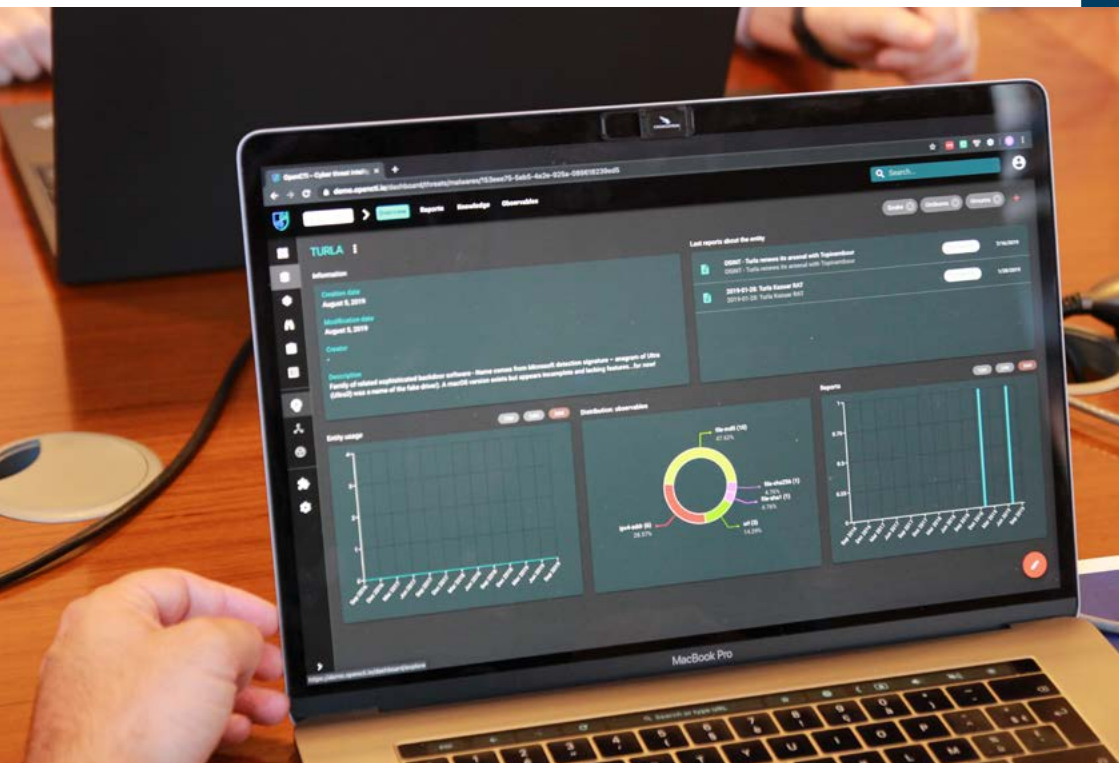
Ons advies:

- Hou alle systemen steeds up to date;
- Gebruik een firewall in combinatie met een antivirusprogramma;
- Verander onmiddellijk de standaard logingegevens.

40. WACHTWOORD

15 % van de Belgen gebruikt voor elke account hetzelfde wachtwoord (Safeonweb DGI, 2019)

De **meest gebruikte wachtwoorden** zijn: 123456, Azerty, admin, password... Deze wachtwoorden zijn gemakkelijk te onthouden, maar ook gemakkelijk te kraken, nl. in minder dan 1 seconde. Sterke wachtwoorden gebruiken, is één van de 5 basistips van Safeonweb.be.



Ons advies:

- Gebruik sterke wachtwoorden;
- Gebruik verschillende wachtwoorden voor al je belangrijke accounts;
- Omdat het een onbegonnen zaak is om een 10-tal sterke wachtwoorden te onthouden, kan je een wachtwoordkluis gebruiken zoals Keepass, Lastpass, LogMeOnce, Myki, 1Password, Dashlane, enz.;
- Maak gebruik van 2FA. (lees ook T: Two factor Authentication)

Meer info op
https://www.safeonweb.be/nl/gebruik-sterke-wachtwoorden

41. WANNACRY

300.000 toestellen geïnfecteerd in 150 landen. Met 18 geïnfecteerde bedrijven bleven de gevolgen voor België in vergelijking tot andere landen eerder beperkt.

In mei 2017 werd de wereld opgeschrikt door de uitbraak van de **ransomware** WannaCry. De snelheid waarmee systemen wereldwijd werden geïnfecteerd, was van een nog niet eerder vastgestelde grootte. De snelheid waarmee het virus zich verspreidde was deels te verklaren door het feit dat de aanvallers gebruik maakten van een zwakheid in IT-systemen die eerder door het National Security Agency (NSA) was ontdekt en die in handen kwam van de hackergroepering Shadow Brokers. Kort nadat zij deze zwakheid publiceerden, verscheen WannaCry op het toneel met de gekende gevolgen. (Lees ook R: Ransomware)

https://www.safeonweb.be/nl/help-mijn-toestel-gegijzeld

42. ZERO DAY AANVAL

Een zero day aanval is een **cyberaanval** die misbruik maakt van **kwetsbaarheden** in software die op dat ogenblik nog **onbekend** zijn voor de softwareontwikkelaar. Van zodra de kwetsbaarheden bekend zijn, werken de softwareontwikkelaars immers aan een oplossing, of **patch** om de kwetsbaarheid te herstellen. De periode tussen het tijdstip dat de kwetsbaarheid bekend is en de patch ontwikkeld is, heet zero day. Patches worden doorgevoerd naar de eindgebruikers via updates. Vandaar het belang van **updates**.

Zero day aanvallen zijn gevaarlijk omdat ze uitgevoerd worden op

het ogenblik dat er nog geen bescherming mogelijk is. Onderzoeken tonen aan dat er heel weinig geslaagde zero day aanvallen zijn. De meeste cyberaanvallen maken gebruik van gekende kwetsbaarheden op toestellen waarvan de software niet tijdig geüpdatet is. Bij bijvoorbeeld WannaCry werden bekende kwetsbaarheden gebruikt, waarvoor de beveiligingsupdates beschikbaar waren maar in niet altijd toegepast werden. (Lees ook U: Updates)

CERT.be
Federal Cyber Emergency Team
Wetstraat 16
1000 Brussel
info@certbe

Centrum voor Cybersecurity België
Wetstraat 16
1000 Brussel
info@ccb.belgium.be

Disclaimer

Deze gids en de bijbehorende documenten zijn opgesteld door het Centrum voor Cybersecurity België (CCB), een federale overheidsdienst opgericht bij koninklijk besluit van 10 oktober 2014 en onder het gezag van de eerste minister.

Het Centrum voor Cybersecurity België wijst alle aansprakelijkheid voor de inhoud van deze gids af.
De verstrekte informatie:

- is uitsluitend van algemene aard en heeft niet tot doel alle specifieke gevallen te behandelen;
- is niet noodzakelijk op alle punten volledig, nauwkeurig of up-to-date.

Verantwoordelijke uitgever
Centrum voor Cybersecurity België
M. De Bruycker, Directeur
Wetstraat, 16
1000 Brussel

Wettelijk depot
D/2020/14828/004

Datum, 15/03/2020