INTRODUCTIE TOT CYBERSECURITY

SUMMARY GUIDE

CONTENT

1. Soorten aanvallen

Ransomware

Er zijn in principe 3 soorten ransomware.

1. Stelen van gegevens en die "niet publiceren" tegen betaling
   Hackers bemachtigen op de 1 of andere manier (hacking, phishing, …) gevoelige gegevens en dreigen met de publicatie ervan. Enkel door te betalen kan u een publicatie (en eventueel ook een GDPR-boete) vermijden.
2. Versleutelen van gegevens en de sleutel aanbieden tegen betaling
   Hackers dringen binnen in uw device (smartphone, tablet, pc, …), netwerk of omgeving (Cloud) en gaan daar gegevens versleutelen (=encryptie). Deze gegevens kunnen enkel hersteld worden door aankoop van de encryptiesleutel van de hackers of door ze terug te zetten d.m.v. een correcte en recente back-up.
3. Beide voorgaande gecombineerd
   Hackers gaan eerst gevoelige gegevens stelen (extractie) en dan versleutelen. Ze vragen dan 2x geld om a) de gegevens niet publiek te maken en b) voor de sleutel om de gegevens te herstellen. Dit wordt ook al eens "double extortion" genoemd.

Wat kan u doen?
Wees zeer voorzichtig met het openen van bijlages in uw email of met het klikken op linken in boodschappen. Neem daarnaast goede veiligheidskopijen van al uw gegevens en bewaar die op een veilige plaats. Naast beveiliging tegen ransomware zorgt dit trouwens ook voor de mogelijkheid tot herstel van deze gegevens bij verlies, defect of diefstal van het toestel waar de gegevens op staan. Back-up in de Cloud is een optie maar beveilig de toegang tot deze omgeving met een degelijk paswoord en MFA (Multi Factor Authenticatie – zie verder).

Phishing

Phishing is een techniek om u te ver-/misleiden om bepaalde gegevens te geven aan de hackers/oplichters. Meestal gaat het hier om uw login en paswoord maar eventueel ook om andere belangrijke en gevoelige gegevens zoals het nummer van uw bankrekening of bankkaart, pincodes, e-id gegevens en dergelijke. U krijgt een mail met een link die u naar een bepaalde website leidt (bv Office365) die vaak een perfecte kopij is van de echte website maar hier worden alle gegevens die u intypt zichtbaar voor de criminelen. Er kan bijvoorbeeld gevraagd worden om aan te loggen met login en paswoord. Na een eerste poging kan het zijn dat u wordt omgeleid naar de echte website waar u dan nogmaals probeert om in te loggen en ditmaal succesvol. U denkt dan misschien de eerste keer een fout te hebben getypt maar dat was dus niet het geval. De hacker is op dit moment in het bezit van uw login en paswoord van de desbetreffende website/dienst. Aangezien we als gebruiker vaak hetzelfde paswoord gebruiken voor verschillende sites hoeft de valse website in principe niet altijd een kopij te zijn van een bestaande.

Wat kan u doen?
Klik niet te snel op een link in een email of ander soort bericht. Kijk de link na door (op de pc) met de muis over de link te zweven zonder te klikken. De bestemming van de link (die soms enkel door <klik hier> of met een andere tekst wordt weergegeven) zal dan zichtbaar worden. Stel dan onomstotelijk vast dat de link correct is. Let zeker op met het openen van links op de smartphone. "Zweven" met je vinger boven de link heeft geen gevolg en vaak worden URL's na het klikken verborgen om schermruimte te recupereren.

Business Email Compromise (BEC)

BEC kan gebeuren vanuit 2 standpunten:

1. Er is geen hack gebeurd van een IT-omgeving, account of device. De oplichter zal proberen om u te benaderen vanuit een identiteit (klant, leverancier, leidinggevende, collega of andere bekende,…) die u normaal gezien vertrouwt om zo gevoelige gegevens te weten te komen of geld te bemachtigen.
2. Er is wel een hack gebeurd van een IT-omgeving of device van iemand in de communicatie. Dit wil dus zeggen dat de hackers/oplichters gewoon al uw communicatie (e-mails) kunnen volgen en zien wat er wordt geschreven. Op deze wijze kunnen zij eventueel kennisnemen van zeer gevoelige informatie. Ze kunnen zich ook uw schrijf- en communicatiestijl eigen maken (afkortingen, emoji's, …). Wanneer het hen uitkomt kunnen ze tussenbeide komen in een bestaande communicatie zonder argwaan te wekken. Dit zou dan bv kunnen zijn om een bepaalde factuur naar een andere rekening te laten betalen.

BEC-mails of berichten zijn meestal zeer eenvoudig in vorm en hebben meestal geen linken of bijlages in zich. Enkele technieken die hackers gebruiken:

- Spoofing van het domein: de mail komt blijkbaar van een afzender van een gekend domein (bv het domein van uw bedrijf/organisatie) maar wanneer u de header van het bericht zou bekijken of de mail beantwoordt zal u merken dat er plots een ander domein en/of adres tevoorschijn komt in het "Aan:" of "To:" veld.
- Spoofing van de display naam: de hacker/oplichter zal de naam gebruiken van iemand die u kent maar een ander emailadres of domein. Typisch is bv het aanmaken van een Gmail- of hotmailaccount met dezelfde naam en dan een smoes verzinnen waarom er niet gemaild is met het corporate emailadres (device verloren, gestolen of defect).
- Typo-squating: het domein wordt iets anders geschreven dan het origineel maar het menselijk brein zal vaak over deze afwijking heen lezen. Bijvoorbeeld vlaams-welzijnsverbond.be i.p.v. vlaamswelzijnsverbond.be (met een "-"-teken). Maar ook achtervoegsels kunnen belangrijk zijn. Wanneer het domein van de afzender <domein.net> is dan is dat duidelijk niet hetzelfde als <domein.be> maar ook hier kan de hacker/oplichter een goede plausibele uitleg voor verzinnen.

Wat kan u doen?
Probeer altijd op een onweerlegbare manier de afzender te bevestigen. Wanneer u antwoordt op een mail check dan ook even snel de bestemmeling in de To- of CC-balk. Let ook op kleine afwijkingen of fouten in de domeinnamen en op de correcte achtervoegsels.

Smishing

Smishing is eigenlijk phishing via SMS. De hacker/oplichter stuurt u een SMS met allicht een link waar u om de 1 of andere dringende reden moet op klikken. Bijvoorbeeld omdat er problemen zouden zijn met uw account van een service (Gmail, Hotmail, Apple-id, Itsme, Instagram, Facebook, …). De link die wordt meegegeven leidt dan normaal gezien naar een perfect nagemaakte website van die dienst waar u wordt gevraagd om in te loggen. Alles wat wordt ingetypt op die website is zichtbaar voor de hacker.

Wat kan u doen?
Wanneer u een bericht krijgt via SMS, Whatsapp, Messenger of gelijk welke weg met de melding dat er een probleem is met uw account van die dienst of website (dat u dan terug zou moeten instellen of confirmeren), ga dan naar de website of de app van die desbetreffende dienst en probeer daar in te loggen. Mocht er inderdaad iets mis zijn met uw account zal daar een melding worden gegeven.

Klik nooit op links in dergelijke boodschappen en zeker niet op de smartphone. Gebruik zelf opgeslagen of opgezochte links (let op voor advertenties van Google die ook door de hacker/oplichter kunnen zijn gekocht).

Whaling

'Whaling' is een 'Cybercrime'-fenomeen waarbij een oplichter zich voordoet als een (voor u) bekende persoon. Er wordt dan meestal gevraagd om even wat geld over te maken of een betaling te doen omdat hij/zij met een klein probleem zit (niet genoeg geld of tijdelijk niet aan de eigen rekening kunnen) met de belofte om dit zo snel mogelijk terug te betalen (niet dus...!). Er wordt vaak beweerd dat de eigen smartphone verloren, gestolen of defect is of gewoon dat de bekende een ander nummer heeft. Zeer snel zal er trouwens ook gezegd worden dat u het oude nummer mag verwijderen om dubbele communicaties te voorkomen. Vaak wordt er ook geen enkele naam genoemd. De oplichters gaan zeer deskundig rond bepaalde hindernissen in de communicatie heen en maken het zo geloofwaardig mogelijk.

Wat kan u doen?
Probeer altijd om de persoon die u contacteert aan de lijn te krijgen wanneer er geld of belangrijke informatie wordt gevraagd. Wanneer er smoesjes gegeven worden dat hij/zij er op dat moment dan toch niet is kan u ervan uitgaan dat het fake is.

Vishing

Vishing kan u bekijken als phishing via telefoon. Er wordt gebruik gemaakt van “Caller ID spoofing” waarbij de oplichter in staat is om gesprekken te voeren waarbij het bellende nummer schijnbaar van een legitieme bron komt (bv. van uw bank, het Covid Vaccinatie Center, …). Door de telecom serviceproviders (Telenet, Proximus, …) worden tegenwoordig bij hen bekende nummers van bedrijven ook vertaald naar de bedrijfsnaam. Dus ook wanneer u bv het nummer van uw bank niet hebt opgeslagen in uw telefoon zal er op het scherm verschijnen “Bank X” met de naam van de desbetreffende bank die wordt gespoofd door de oplichters.

Wat kan u doen?
Probeer zoveel mogelijk om zelf de nummers te vormen. Dan bent u zeker dat de partij aan de andere kant van de lijn wel degelijk de gewenste partij is. Vraag om zelf te kunnen terugbellen en controleer het opgegeven telefoonnummer via het internet of andere diensten. Specifieke vragen stellen kan helpen maar er zijn cases gekend waarbij de antwoorden rustig, professioneel (en dus geloofwaardig) werden gegeven door de oplichters.

“Man in the middle” aanval

Bij een “man in the middle” aanval zal de hacker zich proberen te nestelen tussen uw device en het internet. Dit gebeurt normaal gezien via de Wifi verbinding. Er zijn 2 soorten te onderkennen:

Gebruik van publieke Wifi verbindingen

Restaurants, hotels maar ook luchthavens en treinstations bieden vaak gratis Wifi aan maar bent u zeker dat u connecteert naar die Wifi en niet naar een Wifi die uitgezonden wordt door een hacker? Wanneer u op een locatie bent waar gratis (free) Wifi wordt aangeboden probeer dan altijd te verifiëren dat het wel degelijk een Wifi is van (bv) het etablissement, gelegenheid of organisatie waar u op dat moment bent. Mocht u toch connecteren via een Wifi uitgezonden door een hacker zal al uw internetverkeer door zijn computer gaan. De hacker kan op dat moment heel wat informatie capteren.

Nemen we even aan dat de publieke Wifi waarmee u geconnecteerd bent wel degelijk de correcte is, dan wil dit zeggen dat u nu op een netwerk aangesloten bent met nog heel wat andere toestellen van mensen die u niet kent. Ook dit kan potentiële gevaren met zich inhouden.

Wat kan u doen?
Probeer zo weinig mogelijk gebruik te maken van gratis/publieke Wifi. Wanneer u het toch doet wees dan absoluut zeker dat het de correcte Wifi is. Daarnaast kan u ook gebruik maken van VPN-diensten die al uw internetverkeer encrypteren zodat het voor een hacker zo goed als onmogelijk wordt om data te capteren.

Automatisch connecteren naar bekende Wifi netwerken

Zonder enige twijfel hebt u in uw mobile device (smartphone/tablet/laptop) bekende Wifi netwerken opgeslagen met de optie “automatisch connecteren”. Dit wil zeggen dat wanneer uw toestel geen Wifi verbinding heeft er constant gezocht wordt naar 1 van de opgeslagen Wifi netwerken die dan automatisch zullen worden aangesloten wanneer ze in bereik zijn. Wanneer u bv thuiskomt zal uw smartphone zich automatisch koppelen aan het Wifi netwerk bij u thuis. Maar het zoeken naar deze Wifi netwerken kan door een hacker misbruikt worden door 1 van de gezochte Wifi netwerken te simuleren en uw toestel te doen geloven dat het gaat aansluiten aan een bekende Wifi. Wanneer dat gebeurt (en aangezien u hebt ingesteld dat dit automatisch moet gebeuren) zitten we in hetzelfde scenario als hierboven: alle internetverkeer van uw device gaat langs de computer van de hacker.

Wat kan u doen?
Wanneer u geen Wifi verbinding kan maken met een gekend (en vertrouwd) Wifi netwerk kan u best de Wifi functionaliteit van het device uitschakelen. Zo bespaart u niet enkel energie/batterij maar zal er ook geen automatische Wifi verbinding worden gemaakt met een “gekend” Wifi netwerk.

Malicious USB drop

Let op met gevonden of gekregen USB-sticks. Naast het feit dat het altijd mogelijk is dat de USB-stick een virus of malware bevat kan het ook geen échte USB-stick zijn maar bv een “Rubber Ducky”. Deze zal bij het inbrengen in een USB-poort van een pc een toetsenbord emuleren dat automatisch wordt geïnstalleerd. Daarna zullen er commando’s worden uitgevoerd door ze gewoon automatisch in te typen. Zo kunnen er gegevens gestolen worden maar ook ransomware worden uitgevoerd.

Wat kan u doen?
Wanneer u een USB-stick vindt op straat geef hem dan aan de IT-afdeling die hem beter kunnen onderzoeken of openen in een beveiligde omgeving. Gaat dat niet gooi de stick dan in de vuilbak zodat niemand anders de stick kan vinden.

Malicious cable drop

Niet enkel USB-sticks die u ergens gevonden hebt kunnen gevaarlijk zijn. Hackers kunnen ook gebruik maken van een nagemaakte USB kabel die u gebruikt voor het opladen van uw smartphone of tablet. In de kabel (O.M.G. cable) zit een Wifi netwerk waardoor de hacker toegang kan krijgen tot uw smartphone of device die de kabel aan het gebruiken is.

Wat kan u doen?
Wanneer u een USB-kabel vindt gooi hem dan in de vuilbak of knip hem door.

2. De paswoordmanager

Hebt u veel accounts op verschillende websites en diensten dan kan het wel eens ingewikkeld worden om steeds een goed en veilig paswoord te hebben en dat ook te onthouden. Om het gemakkelijk te houden gebruiken we dan al wel eens hetzelfde paswoord op verschillende websites. Worden er op een website paswoorden gestolen (bv 600 miljoen paswoorden gestolen bij Facebook) of slaagt een hacker erin om uw login (vaak het email adres) en paswoord te phishen dan kan er geprobeerd worden om op tal van websites toegang te krijgen met dat login en paswoord. Met andere woorden: logins en paswoorden zijn tegenwoordig geen garantie meer op het goed beveiligen van uw toegangen en/of gegevens.

Met een paswoordmanager kan u al uw paswoorden op deze verschillende websites en diensten veilig opslaan én synchroniseren tussen uw verschillende devices. De meeste moderne paswoordmanagers kunnen ook geïntegreerd worden in uw browser waardoor u geen enkel paswoord meer moet intypen of zelfs nog maar onthouden. Enkel het master paswoord: het paswoord dat toegang geeft tot de paswoordmanager moet u nog onthouden. En dat kan u dan zeer veilig maken (lang en met vreemde karakters in). Doordat u geen paswoorden van websites en diensten meer moet onthouden wordt het ook mogelijk om paswoorden te gebruiken die a) zeer lang zijn en b) enkel maar bestaan uit letters, nummers en tekens en dus niet meer uit begrijpelijke woorden. Een voorbeeld zou kunnen zijn “asi_93(uk”. Neem het zeker wel lang genoeg langer dan 20 karakters. Bij voorkeur tot 128 lang of langer.

Paswoorden opslagen in de browser zelf is in principe geen goed idee.

3. Multi Factor Authenticatie of MFA

Wat is MFA?

MFA staat voor Multifactor Authentication en wordt soms ook wel eens 2-staps verificatie genoemd. Traditioneel logt u in op een applicatie, een website of een computer met een login en een paswoord. Gebruikt u vele websites, applicaties of toestellen dan kan het wel eens ingewikkeld worden om steeds een goed en veilig paswoord te hebben en dat ook te onthouden. U kan dan gebruik maken van een paswoordmanager (zie hierboven) maar een andere (of bijkomende optie) is MFA of 2-staps verificatie. Hierdoor wordt er een extra laag toegevoegd aan de authenticatie die gebaseerd is op het volgende:

- Iets dat u weet: een login, een paswoord, een (statische) pincode, …
- Iets dat u bezit: een authenticatie app, een pincode (gegenereerd of ontvangen via SMS), een token, …
- Iets dat u bent: vingerafdruk, retina scan, gezichtsherkenning, …

Inloggen vereist bij het gebruik van MFA op zijn minst 2 van deze zaken (2FA of Twee Factor Authenticatie) en in sommige speciale gevallen zelfs alle drie.

In principe kan u MFA gebruiken voor bijna alle websites of services die u gebruikt op het internet. Voorbeelden hiervan zijn online winkelen (Coolblue, Bol.com, Amazon, Zalando, …), Gmail, Hotmail, Facebook, LinkedIn, Insta(gram), Dropbox, PayPal en tal van andere digitale tools die u misschien elke dag gebruikt. Het gebruik van MFA is volledig gratis en het biedt een veel grotere veiligheid dan gewoon uw login en paswoord.

MFA via het gebruik van een Authenticatie App

2 van de meest bekende (gratis) Authenticatie Apps zijn de Microsoft Authenticator en de Google Authenticator. Beide zijn gelijkaardig in werking al heeft de Microsoft Authenticator (op dit moment) ook wel een optie om ook paswoorden bij te houden. U dient ze vooraf te installeren op uw smartphone (via de Google Play Store) of iPhone (via de Apple App Store). De manier waarop u de service/website koppelt met de Authenticatie app is min of meer dezelfde.

Installatie met de hulp van een pc

U logt op een pc in op de gewenste website met uw login en paswoord, gaat naar uw profiel, naar beveiligingsinstellingen en kiest MFA (of 2-staps verificatie) via het gebruik van een Authenticatie app. Een QR Barcode zal worden weergegeven. Op uw smartphone kiest u in de Authenticatie app naar keuze “account toevoegen”. U scant de QR-code in en … dat is alles. Soms zal u voor de eerste keer een code moeten ingeven die de Authenticatie app u geeft om de configuratie te bevestigen.

Installatie via de smartphone zelf

Wanneer de Authenticator is geïnstalleerd op uw smartphone en u gaat MFA of 2-stapsverificatie activeren via de app van die dienst op uw smartphone zal die app vaak kunnen communiceren met de Authenticator.

Wanneer u de volgende keer aanlogt op de website zal, afhankelijk van de graad van integratie, u op de smartphone gevraagd worden om uw login te bevestigen. In het andere geval moet u in de Authenticatie app naar het desbetreffende account gaan en de tijdelijk gegenereerde code die daar wordt weergegeven invullen op de website.

MFA via het gebruik van een SMS

Niettegenstaande het gebruik van een SMS om MFA te activeren op uw account de minst veilige is, is het nog steeds beter dan géén MFA te hebben. Het principe is gelijkaardig dan wanneer u MFA gebruikt via de app. Het verschil is dat er geen bevestiging of een code van de app gevraagd zal worden maar een code die via SMS naar uw gsm-nummer is gestuurd.

Let op voor MFA Fatigue

Aangezien hackers en oplichters het niet leuk vinden wanneer u MFA configureert op uw account, zullen ze proberen om toch toegang te krijgen tot uw account door middel van een techniek die we “MFA Fatigue” noemen. In principe komt het erop neer dat de hackers u gaan bombarderen met MFA requesten of u eerst een boodschap sturen dat het nodig is om de volgende MFA-code naar hen door te sturen voor “verificatie”. Zo krijgen ze dan toch toegang tot uw account. Er zijn ook gevallen bekend dat er eerst een hele boel MFA request worden verstuurd en er dan contact genomen wordt vanuit “de IT-dienst” om uw code aan hen te bevestigen.

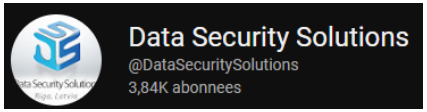
4. Nuttige links en andere informatie

Algemene info:	
Safeonweb.be	https://www.safeonweb.be/nl/ https://www.safeonweb.be/nl/hoe-veilig-ben-jij https://www.safeonweb.be/nl/gebruik-sterke-wachtwoorden en de app via de Google Play Store of Apple App Store
CENTRE FOR CYBER SECURITY BELGIUM	https://ccb.belgium.be/nl
CYBER SECURITY COALITION.be	https://www.cybersecuritycoalition.be/nl/
';--have i been pwned?	https://haveibeenpwned.com/
VSSE veiligheid van de staat sûreté de l'état	Mensen die naar het buitenland reizen: https://www.vsse.be/sites/default/files/1-passeport-version-nl-fond-hl.pdf
EUROPEAN CYBER SECURITY MONTH	https://cybersecuritymonth.eu/

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY	https://www.enisa.europa.eu/
National Cyber Security Centre	https://www.ncsc.gov.uk/
Nationaal Cyber Security Centrum Ministerie van Justitie en Veiligheid	https://www.ncsc.nl/
CSO FROM IDG	https://www.facebook.com/CSOonline https://www.csoonline.com/
TechTarget SearchSecurity	https://searchsecurity.techtarget.com/
SECURITY	https://www.securitymagazine.com/
Secplicity Security Simplified	https://www.secplicity.org/
SECURITYWEEK CYBERSECURITY NEWS, INSIGHTS & ANALYSIS	https://www.securityweek.com/
MSSP Alert	https://www.msspalert.com/
avatlas	https://portal.av-atlas.org/

CYBERCRIMEINFO.NL	https://www.cybercrimeinfo.nl/
CYBER SECURITY HUB	https://www.cshub.com/content-hub/incident-of-the-week
Governance:	
NIST	https://www.nist.gov/ https://nvd.nist.gov
CIS Center for Internet Security® Creating Confidence in the Connected World.	https://www.cisecurity.org/
MITRE	https://attack.mitre.org & https://d3fend.mitre.org
Maps:	
NETSCOUT	https://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=18763&view=map
Check Point SOFTWARE TECHNOLOGIES LTD.	https://threatmap.checkpoint.com/

Paswoord Managers	Besproken tijdens de sessie: Lastpass … https://www.lastpass.com/nl Maar er zijn er natuurlijk nog andere ook: Bv https://www.dashlane.com/nl/ Voor wat het waard is hier een overzichtssite: https://www.investopedia.com/best-password-managers-5080381 En de lijst van pcmag.com: https://www.pcmag.com/picks/the-best-password-managers Of Googelen
Youtube Channels	
	https://hak5.org/ & https://www.youtube.com/@hak5
	www.davidbombal.com & https://www.youtube.com/@davidbombal
	https://networkchuck.com/ & https://www.youtube.com/@NetworkChuck
	(Shannon Morse) https://snubsie.com/ & https://www.youtube.com/@ShannonMorse
	https://www.youtube.com/@pcsecuritychannel

	https://www.youtube.com/@LoiLiangYang
	https://www.youtube.com/@DataSecuritySolutions
Youtube films	
Kevin Mitnick over sessioncookies	https://youtu.be/xaOX8DS-Cto