Hoe reageren op een cyberaanval?

Inspiratiesessie: Sterke praktijken rond cyberveiligheid
08 maart 2022

Kurt Penninck
Directeur Privacy & Security V-ICT-OR
DPO Lokaal Bestuur Blankenberge

V-ICT-OR
VLAAMSE ICT ORGANISATIE

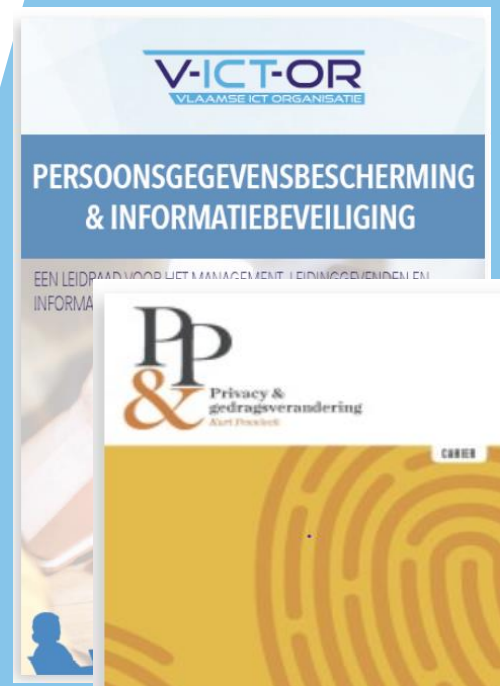
Spreker

Spreker

- Kurt Penninck
- Data Protection Officer en diensthoofd Lokale Economie bij het Lokaal Bestuur van Blankenberge
- Directeur Privacy & Security, docent GDPR, informatieveiligheid en cyberveiligheid bij de Vlaamse ICT Organisatie (vzw V-ICT-OR)
- Auteur van het boek ‘Persoonsgegevensbescherming en informatiebeveiliging’ (2018) en ‘Privacy en Gedragsverandering’ (2020), beide uitgegeven door Politeia
- Lid van de ‘Taskforce Cyberveilige Gemeenten’ (Vlaamse overheid)
- Lid van de Werkgroep Informatieveiligheid van de Vlaamse Steden en gemeenten (VVSG)

Aan alle deelnemers

- **Welkom in jullie virtuele stoel**, thuis op het werk of waar jullie zich ook mogen bevinden



Vlaamse ICT Organisatie (V-ICT-OR)

Vlaamse ICT Organisatie

- Missie
  - Deskundigheid bevorderen
  - Belangenbehartiging bij het ICT-beleid op het lokale overheidsniveau
  - Netwerk en forum
  - Onderlinge samenwerking en synergie tussen overheidsniveaus (lokaal, provinciaal, Vlaams, Federaal, Europees) bevorderen
  - Extern klankbord
- Effectieve leden (op heden): 1220
  - Aantal gemeenten: 235
  - Aantal leden gemeenten: 902
  - Gemiddeld # leden per gemeente: 2,97
  - Aantal Vlaamse agentschappen: 11
  - Aantal leden Vlaamse Agentschapen: 318
  - Actieve gebruikers (2021): 1335

Inhoudsopgave

Inhoudsopgave

Inhoud

Programma en inhoud

- Helpende handen
- Initiatieven verhogen digitale weerbaarheid
- 10 geboden - Cyberincidenten voorkomen (Audit Vlaanderen)
- Nuttig
- Vragen
- Contact V-ICT-OR
- Bijlage: The Cyber Kill Chain (uitbreiding met o.a. technische maatregelen)

Cybercriminaliteit

Trends, facts & figures

Inleiding

Trends

- De **digitale transformatie** verloopt met de dag in versneld tempo (zie inleiding **burgemeester Geel Vera Celis)**
  - Nieuwe apps, communicatieplatformen (WhatsApp, Signal), IoT, City of Things, AI, …
- Digitalisering en nieuwe technologieën zijn dé **sleutels tot succes, bieden heel wat voordelen**
  - Bijv. 24/7 bereikbaar én service aan de klant
- Maar, digitale transformatie heeft ook zijn **prijs**
  - Met elke nieuwe ontwikkeling neemt de **afhankelijkheid** van technologie toe
  - Zonder ons bewust van te zijn of bij stil te (willen) staan, **domineert** technologie in mindere, wellicht meerdere mate ons dagelijks leven, thuis én op het werk

Cybercriminaliteit

Inleiding

Trends

- Een verregaande digitalisering in versneld tempo is **koren op de molen** voor cybercriminelen
  - Dat steeds meer apparaten softwarematig worden aangestuurd via internet, geeft hen in toenemende mate de kans **digitale kwetsbaarheden** uit te buiten en **cyberaanvallen** te lanceren
- Sommige overheden en bedrijven staan op vandaag te weinig stil bij **hoe digitaal kwetsbaar** ze zijn
  - Eén simpele, foute muisklik of touch op het scherm is de afstand én de tijd om een overheid of bedrijf, zelfs kritische delen van de samenleving (**kritische infrastructuren**), te ontwrichten
- Anderen denken dan weer dat ze voor cybercriminelen **niet belangrijk** zijn
  - Onterecht! **Elke onderneming in élke sector**, overheid en privé, groot en klein, is een **potentieel doelwit** voor hackers of andere cybercriminelen

❗ Elk, en met zijn allen moeten we daarom even **waakzaam** blijven

Cybercriminaliteit

Inleiding

Trends

- Ondernemingen met een **minder uitgewerkte cyberstrategie** horen tot de **grootste risicogroep** om te worden aangevallen, schade op te lopen, in het slechtste geval niet te overleven
- Cybercriminelen buiten met gemak en zonder empathie of terughoudendheid, want **money time**, hun digitale kwetsbaarheid uit > Vragen van losgeld (ransom) > **Stelregel**: **overheden**: niet betalen / **privé**: opmaken kosten-baten analyse
- Cybercriminelen proberen zoveel mogelijk **onder de radar** te blijven (geen sporen nalaten > hierdoor is de **pakkans** niet onbestaande, **uitlevering** grootste probleem)

Cybercriminaliteit

Inleiding

Trends

- Wie zijn die cybercriminelen?
  - Pukkelige tiener met een overschot aan IT-talent maar fout moreel kompas + hoodie
  - Vooral overwegend 'geweldig' professioneel en goed georganiseerd
    - Overheden (Statelijke actoren): Rusland, China, Noord-Korea, Iran, …
    - Terroristen
    - Beroepscriminelen
    - Hacktivisten
    - Insiders
- Wat zijn hun doelen?
  - Voor de fun, spionage, financieel gewin, sabotage, diefstal informatie voor concurrenten, nastreven van een sociaal, ideologisch of politiek doel, onbruikbaar maken van kritische infrastructuren > steeds een voordeel

Cybercriminaliteit

Inleiding

Trends

- Top 4 cyberdreigingen
  - Malware
  - Phishing
  - DDoS (bijv. Aanval op Belnet)
  - Spam

Cybercriminaliteit

Facts & figures

Trends

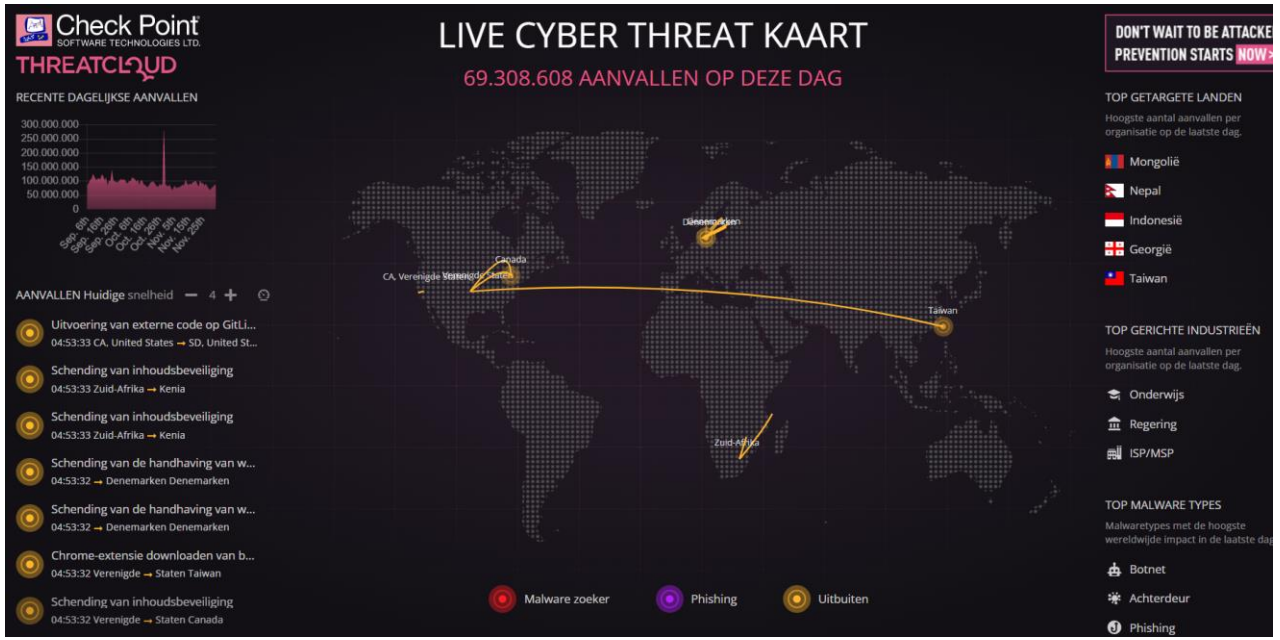
- Elke dag worden er wereldwijd duizenden servers, websites en computers met succes gehackt
- Wereldwijde jaarlijkse kosten van cybercriminaliteit overschrijden de 6 biljoen euro (2021) … en zullen de komende jaren nog veel verder doorstijgen
- Cyberbeveiligingsstatistieken, trends en feiten die er toe doen voor 2021 (websiterating.com)
- Kost cybercriminaliteit in België: 3,7 á 4,5 miljard euro per jaar (= 1% BNP)
- Het aantal aanvallen neemt in steeds snellere mate toe, vinden voortdurend plaats:
  - Cybermap Kapersky real time

Cybercriminaliteit

Facts & figures

Trends

- Threatmap Checkpoint: 10-tallen miljoenen bedreigingen per dag



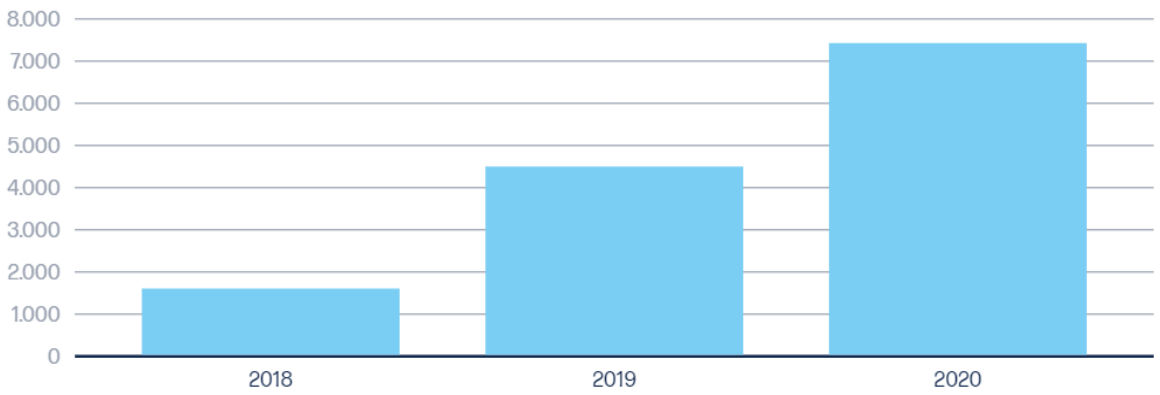
Cybercriminaliteit

Facts & figures

Trends

- Meldingen cyberincidenten bij het **Centrum voor Cybersecurity België (CCB)** nemen elk jaar toe. De cijfers in grafiek zijn zwaar **onderschat** (want vele slachtoffers van cybercriminaliteit doen **geen aangifte** bij het Cert, Politie, …

Aantal meldingen van cyberincidenten bij het Centrum voor Cybersecurity België



Gemaakt met LocalFocus

Bron: CCB

CENTRE FOR CYBER SECURITY BELGIUM

Cybercriminaliteit

Facts & figures

Trends

- Meldingen **SafeonWeb**
  - In 2020 werden er **3.200.000** berichten doorgestuurd naar verdacht@safeonweb.be. De verdachte URL's uit deze e-mails worden doorgestuurd naar Google SafeBrowsing en Microsoft SmartScreen. Browsers maken van deze info gebruik om bezoekers te waarschuwen voor kwaadaardige websites
- Verhalen cybercriminaliteit
  - **Verhalen zeggen meer dan de grote getallen**
    - ✓ Back-Ups: Anthony (54) verloor tien jaar werk
    - ✓ Microsoft scam: Nicole (84) verloor al haar spaarcenten door phishing
    - ✓ DDoS-aanval: Belnet-netwerk werd slachtoffer van een volumetrische DDoS-aanval

Belnet dedicated connectivity

Safeonweb.be

V-ICT-OR VLAAMSE ICT ORGANISATIE

Cybercriminaliteit

Facts & figures

Trends

- Criminaliteit digitaliseert
  - De politie krijgt steeds meer met digitale criminaliteit, waaronder cybercriminaliteit, en steeds minder met 'klassieke' criminaliteit als woninginbraken en overvallen te maken
    - ✓ Zie Criminaliteitsstatistieken & veiligheidsmonitor (policefederale.be)
    - ✓ Cybercriminaliteit treft ook overheden

Waarom cybercriminaliteit

Omdat het kan!

- De vraag ‘WAAROM neemt cybercriminaliteit toe?’ heeft een simpel antwoord:
  - Omdat het aantal kwetsbaarheden, bedreigingen, **risico’s** toeneemt omdat de maatschappij razendsnel digitaliseert
- De vraag ‘WAAROM kan het?’ heeft ook een simpel antwoord:
  - Omdat je **(basis)cyberbeveiliging onvoldoende**, niet op orde is
    - ✓ Het hoge aantal cyberaanvallen is voor een groot deel te wijten aan **onvoldoende ‘digitale basishygiëne’** waardoor cybercriminelen makkelijk bij je kunnen aankloppen … en binnenkomen!
    - ✓ **Audit Vlaanderen** bevestigt: ‘Veel haalbare **beschermingsmaatregelen** blijven **onderbenut**’ (zie verder)
    - ✓ Cyberveiligheid op vandaag lijkt vooral te bestaan in PowerPoints en beleidsnota’s … **Schijnveiligheid**

Waarom cybercriminaliteit

Omdat het kan!

- Onvoldoende beveiliging
  - Vele bedrijven en organisaties beschermen zich de dag van vandaag niet goed en onvoldoende
    - ✓ Thema-audit Informatieveiligheid 2018 – Audit Vlaanderen
    - ✓ Thema-audit Informatieveiligheid 2020 – Audit Vlaanderen

Cybercriminaliteit

Waarom cybercriminaliteit

Omdat het kan!

- Vaststellingen thema-audit informatiebeveiliging 2018

	+ 19.000 inwoners									aantal inwoners < 19.000 en > 12.000									< 12.000 inwoners									gemiddelde
Organisatiebeheersing	3	3	2	2	3	0	3	0	2	3	0	3	3	2	2	2	2	0	2	0	3	0	0	0	0	2	3	1,67
BELEID EN ORGANISATIE	**3**	**2**	**2**	**1**	**2**	**1**	**2**	**1**	**2**	**2**	**3**	**2**	**2**	**2**	**2**	**2**	**1**	**2**	**2**	**2**	**2**	**1**	**1**	**2**	**2**	**1**	**1**	**1,78**
informatiebeveiligingsbeleid	3	3	2	1	1	2	1	1	2	3	3	1	1	2	2	2	2	2	2	1	2	2	2	2	2	1	2	1,85
verantwoordelijkheden	3	3	2	1	2	2	2	1	2	3	3	2	2	2	2	2	1	2	2	2	1	2	1	3	2	1	1	1,93
leveranciersrelaties	2	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,07
naleving	3	2	2	2	2	1	2	1	1	1	4	3	3	1	1	1	1	2	2	2	2	1	1	1	2	1	1	1,70
BEWUSTZIJN	**2**	**2**	**2**	**1**	**2**	**1**	**1**	**1**	**1**	**3**	**3**	**3**	**2**	**2**	**2**	**1**	**1**	**2**	**2**	**2**	**2**	**2**	**2**	**1**	**1**	**2**	**2**	**1,78**
veilig personeel	2	3	3	2	1	1	2	1	1	2	3	3	2	3	2	1	1	1	2	2	2	2	2	1	1	1	2	1,81
omgang met informatiedragers	3	2	2	1	2	2	1	2	1	3	3	3	1	2	1	1	1	2	1	3	2	2	1	1	1	2	2	1,78
TECHNISCH BEHEER	**2**	**2**	**2**	**2**	**1**	**1**	**2**	**1**	**1**	**2**	**1**	**1**	**2**	**1**	**2**	**1**	**2**	**1**	**2**	**1**	**2**	**2**	**1**	**1**	**1**	**1**	**1**	**1,44**
cryptografie	3	2	2	1	1	1	2	1	1	1	1	1	2	0	1	1	2	0	1	1	1	1	1	1	1	1	0	1,15
fysieke beveiliging	2	2	3	3	2	2	nvt	2	1	3	3	2	3	2	2	2	2	2	2	2	3	2	1	2	1	3	1	2,04
beveiliging van de IT-omgeving	2	2	2	2	1	1	2	1	1	2	1	1	2	1	2	2	2	1	2	2	2	1	2	1	1	1	1	1,52
netwerkbeveiliging	2	2	2	2	2	2	2	1	1	2	1	1	2	1	2	1	2	1	2	2	2	2	1	2	1	2	1	1,63
ontwikkeling	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,04
LOGISCH TOEGANGSBEHEER	**2**	**2**	**2**	**2**	**2**	**1**	**1**	**1**	**1**	**3**	**2**	**2**	**1**	**2**	**2**	**1**	**1**	**1**	**2**	**2**	**2**	**2**	**1**	**1**	**1**	**1**	**1**	**1,56**
uitdiensttreding	1	2	2	2	2	1	1	1	0	3	2	3	1	2	3	1	1	1	2	2	1	2	1	1	0	2	1	1,52
beheer en classificatie	2	2	2	2	2	1	1	2	1	3	2	2	1	2	1	1	1	2	1	2	2	1	1	1	1	1	2	1,56
toegangsbeveiliging	2	1	2	2	2	2	1	1	2	2	3	2	1	2	1	2	1	1	3	2	2	2	2	1	1	1	1	1,67
CONTINUÏTEIT	**2**	**3**	**3**	**3**	**3**	**3**	**2**	**3**	**2**	**3**	**1**	**3**	**3**	**3**	**3**	**3**	**2**	**1**	**3**	**1**	**1**	**1**	**2**	**1**	**3**	**1**	**1**	**2,22**
INCIDENTENBEHEER	**3**	**1**	**1**	**2**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**2**	**2**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**2**	**1**	**1**	**1**	**2**	**1**	**1**	**1,26**
gemiddelde maturiteit informatiebeveiliging	2,25	2,00	2,00	1,75	1,69	1,50	1,47	1,31	1,19	2,19	2,06	1,94	1,75	1,63	1,63	1,44	1,38	1,31	1,75	1,69	1,69	1,50	1,31	1,31	1,31	1,31	1,19	1,61
	1,68									1,70									1,45									

- In de realiteit resulteert dit in een scala aan incidenten met grote impact!

Cyberaanval

Autopsie van een cyberaanval

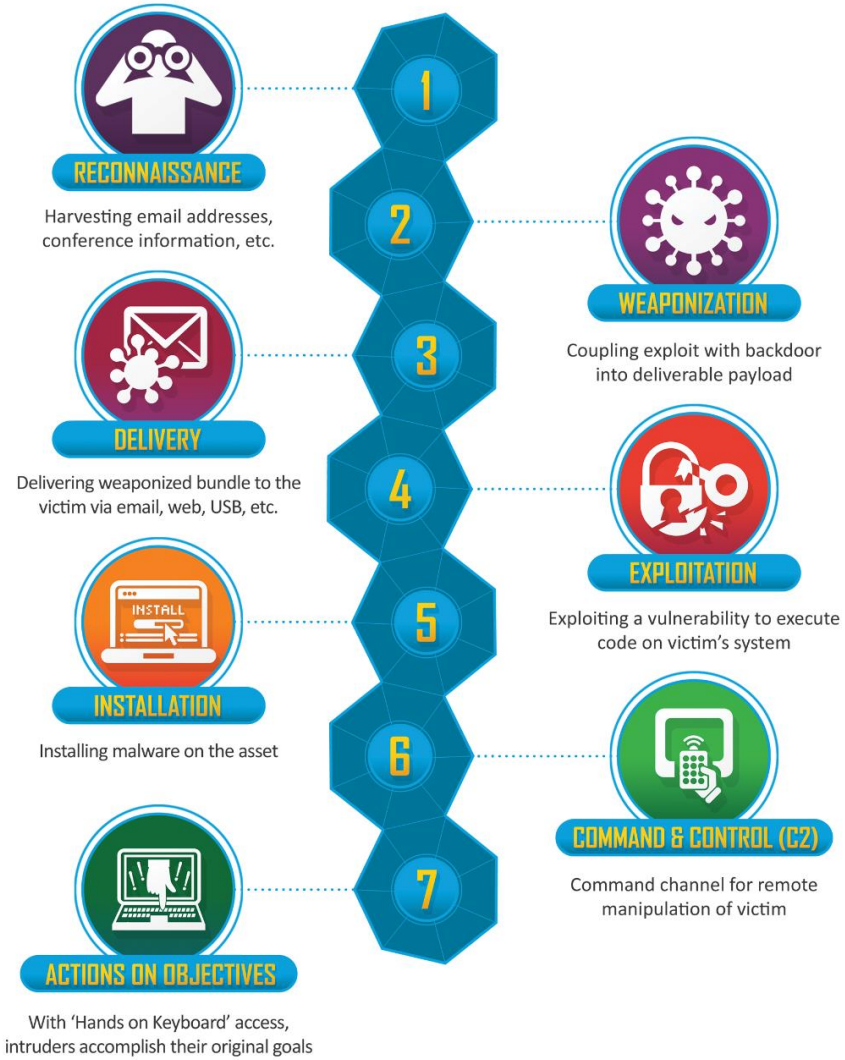
The Cyber Kill Chain

Autopsie van een cyberaanval

Fasen

De 7 fasen van een cyberaanval: ‘The Cyber Kill Chain’

Belangrijk: in elke fase van de ketting de passende maatregelen nemen om erger te Voorkomen!



Autopsie van een cyberaanval

Fasen

De 7 fasen van een cyberaanval

- Cyberaanval komt niet als een donderslag bij heldere hemel uit de lucht vallen
  1. **Reconnaissance-fase (verkenning)**: de aanvallers zoeken zwakke plekken in de organisatie (aanvalsoppervlak in kaart brengen).
     - Fysiek: Inbrekers verkennen villa's waar ramen openstaan en deuren niet op slot zijn
     - Digitaal: Scannen op kwetsbaarheden, op open poorten, op onbeveiligde koppelingen naar externen
  2. **Weaponization-fase (bewapening)**:
     - Fysiek: inbrekers voorzien zich van een koevoet
     - Digitaal: de aanvallers ontwikkelen malware om deze zwakke plekken te misbruiken, om te kunnen inbreken
  3. **Delivery-fase (aflevering)**:
     - Fysiek: De inbrekers gaan met hun breekijzer naar de villa waar ze willen inbreken
     - Digitaal: de aanvallers bezorgen de malware, bijvoorbeeld via e-mail

Autopsie van een cyberaanval

Fasen

De 7 fasen van een cyberaanval

4. **Exploitation-fase (uitbuiting)**:
   - Fysiek: de inbrekers forceren met hun koevoet de deur open
   - Digitaal: een medewerker activeert per ongeluk de malware, door op een link in een onbetrouwbare e-mail te klikken
5. **Installation-fase (installatie)**:
   - Fysiek: De inbrekers verkennen geruisloos de villa
   - Digitaal: de aanvallers installeren zich in het netwerk en gaan op verkenning
6. **Command and control-fase (beheer en controle)**:
   - Fysiek: De inbrekers nemen contact op met een handlanger om bijvoorbeeld de code van de kluis te vernemen
   - Digitaal: de aanvallers installeren vervolgens nieuwe malware (bijv. voor ransomware aanval)

Autopsie van een cyberaanval

Fasen

De 7 fasen van een cyberaanval

7. **Actions on objectives-fase (uitvoeren van het doel)**:
   - Fysiek: De inbrekers vinden de juwelen, het geld en gaan er zo onopgemerkt mogelijk mee (geen sporen nalaten) aan de haal
   - Digitaal: De aanvallers bereiken hun doel en kunnen ongemerkt informatie wegsluizen, ransom cashen

- Tip: Neem voor elke fase de nodige veiligheidsmaatregelen (zie bijlage)

Wat moet je doen als je gehackt bent?

Draaiboek

Wat doe je onmiddellijk, wat doe je post-mortem?

Wat moet je doen als je gehackt bent?

Draaiboek

Aandachtspunten

- Welke stappen moet je ondernemen als je gehackt bent? Zowel **technisch-organisatorisch**, **juridisch** als qua **communicatie**. Want als je gehackt bent zijn er heel wat dingen waar je aan moet denken en waar je rekening mee moet houden

⚠ Opmerkingen:

- Zorg vooraf voor een **draaiboek** (continuïteitsplan incl. cyberoefeningen / = scenario's en OEFEN)
- Maak gebruik van **bestaande modellen** (zie verder) en of laat je **begeleiden** (cyberbeveiliging is een vak apart)
- Stem je draaiboek af op het **ANIP** (Algemeen nood- en interventieplan) en / **BNIP** (Bijzonder nood- en interventieplan)

Wat moet je doen als je gehackt bent?

Draaiboek

Ben ik gehackt?

- **Controleer** eerst of werkelijk sprake is van een aanval, of je effectief gehackt bent!

  Soms **duidelijk**:

  - Website offline gehaald of aangepast door hackers
  - Ransomware: eis tot betalen losgeld, data versleuteld

  Soms minder duidelijk:

  - Waarom: omdat hackers onder de radar willen blijven (bv. bij spionage)

Wat moet je doen als je gehackt bent?

Draaiboek

Signalen dat je gehackt bent

- Voor servers
  - Je ontdekt verdachte **cron jobs** (automatische taken die niet door jou opgezet werden)
  - Je staat opeens op **zwarte lijsten voor spam** (bepaalde malware gebruikt je server om spam mails te versturen)
  - **Extra activiteit** in de server **logs**
  - **Verhoogde belasting** van de server
  - Applicaties die **offline** gaan

Wat moet je doen als je gehackt bent?

Draaiboek

Signalen dat je gehackt bent

- Voor computers
  - Je **computer** is plots veel **trager**
  - **Pop-ups**, pop-ups en nog eens pop-ups
  - **Wachtwoorden** zijn ineens **veranderd**, je account is gehackt
  - Er staan **nieuwe programma's** op je computer
  - **Nep (antivirus) waarschuwingen**
  - Je contacten ontvangen **nepmails** van jou (bevatten meestal schadelijke links of bijlagen)
  - Je krijgt een **ransomware-bericht** (betalen van losgeld, bestanden en toepassingen op slot)
  - De **muis** beweegt uit zichzelf (computer werkt zonder interne input)

Wat moet je doen als je gehackt bent?

Draaiboek

Signalen dat je gehackt bent

- Voor websites
  - Je **hosting provider** laat je weten dat je website gehackt is (omdat ze gevaarlijke code ontdekt hebben)
  - Je merkt dat je website **onbeschikbaar** is, traag laadt of regelmatig crasht
  - Je kan niet meer inloggen op je **CMS of op de beheertool** voor je website (hackers hebben de wachtwoorden aangepast)
  - Je vindt **onbekende user accounts** in je CMS
  - Je ziet een **fikse daling in je bezoekersaantallen** (bepaalde malware stuurt bezoekers naar andere websites)
  - Je merkt dat er **onbekende plug-ins** geïnstalleerd zijn
  - Je krijgt **pop-ups te zien** die niks met jouw website te maken hebben

Wat moet je doen als je gehackt bent?

Draaiboek

Wat moet je onmiddellijk doen als je gehackt bent?

Er zijn een aantal dingen die je meteen moet doen vanaf het moment dat je effectief gehackt bent

- Keep calm, don't panic
  - De eerste gouden raad: **schiet niet meteen in paniek** maar laat een verdacht signaal zo snel mogelijk onderzoeken en verifiëren. Je kan de klok helaas niet terugdraaien. En het is best mogelijk dat vreemde signalen te wijten zijn aan een **andere oorzaak**
  - Probeer **niet te doen alsof er niks gebeurd is** of dingen te verbergen (onder de mat schuiven) want het kwaad is al geschied
    - Sensibiliseer medewerkers om verdachte signalen te melden bij IT, DPO
  - Hou het hoofd koel en denk goed na welke **stappen** je moet ondernemen om de gevolgen van de hack zo klein mogelijk te houden
    - Makkelijker gezegd dan gedaan want gevoelens van ongeloof, verbijstering, **machteloosheid** (Vgl. inbreker die in de nacht in je slaapkamer staat) (onderschat de psychologische factor niet > daarom: zorg voor een draaiboek met scenario's en oefen!)

Wat moet je doen als je gehackt bent?

Draaiboek - Organisatorisch

Wat moet je onmiddellijk doen als je gehackt bent?

1. Organisatorisch
   - **Rapporteer/meld** (volg het vooraf opgemaakt verwittigingsschema / escalatieprocedure)
     - Stel de **hoogste leiding** van de organisatie op de hoogte van de hack zodat op elk moment de besluitvorming snel kan plaats vinden
     - Neem direct contact op met de ICT-dienst van je organisatie en informeer de DPO en bespreek het cyberincident
   - Als organisatie sta je voor een **keuze**: zelf het incident verder afhandelen en onderzoeken en/of externe specialisten inschakelen
     - Voordelen externe specialist: up-to-date technische kennis en ervaring, specifieke expertise, specialistische apparatuur en extra handen die gespecialiseerd je organisatie kunnen helpen met het opsporen en bepalen van reikwijdte van de hack

Wat moet je doen als je gehackt bent?

Draaiboek - Organisatorisch

Wat moet je onmiddellijk doen als je gehackt bent?

1. Organisatorisch

   Activeer de coördinatie op dubbel niveau**: de beleidscoördinatie** en **operationele coördinatie (n.a.v. ANIP/BNIP)**

   Samenstelling

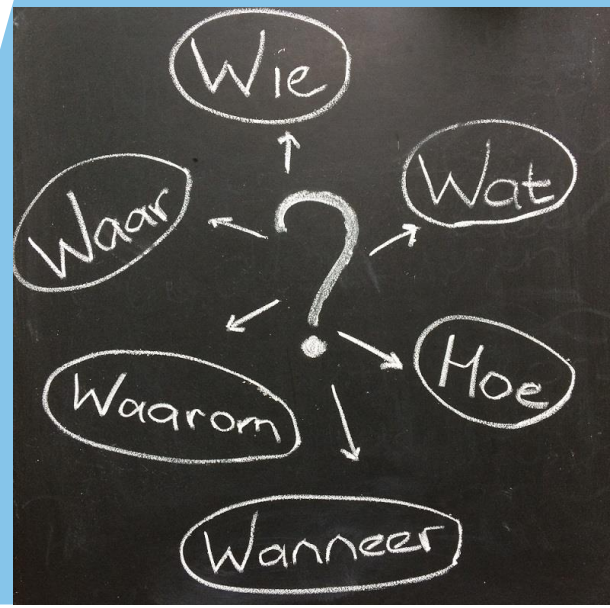
   - **Beleidscoördinatie**:
     - Doel strategische knopen doorhakken (bijv. beroep op externe expertise of niet, aankopen, losgeld wel of niet betalen, wanneer communiceren, …)
     - Rollen (niet limitatief)
       - Bijv. burgemeester, schepen, Algemeen directeur, leden MAT … ieder die beslissingsbevoegdheid heeft

Wat moet je doen als je gehackt bent?

Draaiboek - Organisatorisch

Wat moet je onmiddellijk doen als je gehackt bent?

1. Organisatorisch
    - **Operationele coördinatie (incident respons team)**
        - Doel: operationele knopen doorhakken: ‘Wie, Wat, Hoe, Wanneer, Waarom, Waar’
        - Rollen (niet limitatief):
            - **Crisismanager**: heeft de taak om de werking van het incident response team te coördineren, in samenspraak met de beleidscoördinatie
            - **Secretaris of notulist**: De secretaris staat in voor het bijhouden van het logboek en de notulen voor de overlegmomenten van het incident respons team



Wat moet je doen als je gehackt bent?

Draaiboek - Organisatorisch

Wat moet je onmiddellijk doen als je gehackt bent?

1. Organisatorisch
   - **Diensthoofd ICT**: Het diensthoofd ICT stuurt de IT-medewerkers en/of externe leveranciers aan, en is het centrale aanspreekpunt voor IT-gerelateerde vragen
   - **Data Protection Officer**: contactpunt met toezichthouders, voorbereiden melding datalek
   - **Diensthoofd Communicatie**: Het diensthoofd communicatie coördineert de interne en externe communicatie voor en door het lokaal bestuur tijdens de crisisfase
   - **Noodplanningscoördinator**: Ondersteunt de crisiswerking met inzichten uit eerdere noodsituaties en courante lokale processen

Draaiboek - Organisatorisch

Wat moet je onmiddellijk doen als je gehackt bent?

1. Organisatorisch
    - **Diensthoofd HR**: Het diensthoofd HR heeft een overzicht op de kwalificaties en profielen binnen het lokaal bestuur en kan zo adviezen geven om de beschikbare menselijke capaciteit optimaal in te zetten
    - **Preventieadviseur**: Een crisissituatie kan lange(re) tijd aanslepen, het is dan ook aangewezen om een lid binnen het incident response team te hebben die zich toelegt op het welzijn van de voornaamste actoren en medewerkers

Wat moet je doen als je gehackt bent?

Draaiboek - Organisatorisch

Wat moet je onmiddellijk doen als je gehackt bent?

1. Organisatorisch
   - Waar nodig kan deze samenstelling aangevuld worden met **bijkomende profielen**. Hou er wel rekening mee dat daadkrachtige beslissingen en snelheid aan de orde zijn, dus vermijd een te logge crisisstructuur. Enkele mogelijke aanvullende profielen zijn:
     - **Coördinator Logistiek, Facilitair beheer, Technische dienst**: voor gebouwen, uitwijklocaties en voorraden
     - **Interne juridische deskundige**: voor vraagstukken rond schadeclaims en strafonderzoek
     - **Coördinator Financiën**: voor contracten, facturen, uitkeringen, verzekering, ...
     - **Coördinator voor specifiek zwaar getroffen of vitale diensten**: OCMW, RVT, onderwijs, …

Wat moet je doen als je gehackt bent?

Draaiboek - Organisatorisch

Wat moet je onmiddellijk doen als je gehackt bent?

1. Organisatorisch
   - Breng je **hosting provider** op de hoogte ingeval je je extern gehoste website is gehackt
   - Contacteer het federaal **Computer Emergency Response Team**, kortweg CERT om het incident te melden, hulp in te roepen en te horen of er vergelijkbare incidenten spelen bij andere organisaties (zie verder)
   - Doe aangifte bij de **politie** (zie verder)
   - Als er persoonsgegevens gelekt zijn (**datalek**), moet je dit aan de **Gegevensbeschermingsautoriteit / Vlaamse Toezichtcommissie** melden (zie verder)

Wat moet je doen als je gehackt bent?

Draaiboek - Organisatorisch

Wat moet je onmiddellijk doen als je gehackt bent?

2. Technisch
   - **Verbreek de netwerkverbinding** van de server
     - Dit moet ervoor te zorgen dat hackers niet meer bij de server kunnen en dat de server ook geen andere componenten in het netwerk verder kan verspreiden. Isoleer de geïnfecteerde apparaten (computers, laptops …)
     - ⚠ Zet je computer NIET uit, want op die manier wis je sporen die de daders achterlaten
   - Gooi niets weg (bijv. mails, bestanden) en laat op deze server / computer **geen (nieuwe)virusscanner** lopen die mogelijk aanwijzingen kan verwijderen

Wat moet je doen als je gehackt bent?

Draaiboek - Organisatorisch

Wat moet je onmiddellijk doen als je gehackt bent?

2. Technisch
   - Indien er vermoeden is dat meerdere servers / computers (bijv. met ransomware) besmet zijn, **zet de automatische back-ups uit**
     - Bij besmetting (bijv. met ransomware) kunnen er diverse bestanden reeds aangetast zijn en zullen besmette/versleutelde bestanden naar de back-up worden weggeschreven
   - Maak een back-up
     - Maak een **volledige back-up van je gehackte server** / computer
     - Dit is NIET de back-up die je later zal gebruiken om alles terug te herstellen, want de malware bevindt zich mee in deze back-up
     - Deze back-up is vooral bedoeld om zoveel mogelijk **bewijsmateriaal** te kunnen bewaren over de hack en wat de hacker allemaal gedaan heeft

Wat moet je doen als je gehackt bent?

Draaiboek - Technisch

Wat moet je onmiddellijk doen als je gehackt bent?

2. Technisch
   - Vervang alle **wachtwoorden** op alle toestellen
     - Vervang alle wachtwoorden – en we bedoelen ook echt ALLE wachtwoorden - die gebruikt werden op de server
       - ✓ Denk aan wachtwoorden van e-mail, control panels, CMS-systemen, enz.
     - Doe dit ook op alle toestellen die toegang hadden tot de gehackte website of server
   - **Controleer ook andere apparaten**
     - Als de kans bestaat dat de hacker via de gehackte server / computer ook toegang had tot andere apparaten controleer die dan grondig
       - ✓ Geef extra aandacht aan apparaten waarop eventuele belangrijke of gevoelige (persoons)gegevens staan

Draaiboek – Post-mortem

Wat moet je post-mortem doen als je gehackt bent?

3. Post-mortem onderzoek
   - **Zoek uit hoe de hacker is binnengeraakt**
     - ✓ Bedoeling is om te gaan bepalen wat er is misgelopen, hoe de hacker erin geslaagd is binnen te komen en welke schade hij allemaal heeft kunnen aanrichten
   - Zoek **sporen**
     - ✓ Dit is de verantwoordelijkheid van IT-specialisten (intern, Incident Respons Team, FCCU, RCCU). Ze gaan je geïnfecteerde systemen onderzoeken en proberen sporen te vinden die het patroon van de dader verraden, bv. wijzigingen in het systeem, configuratiebestanden of bedrijfsgegevens. Ze gaan ook na of de daders malware hebben geïnstalleerd. Alle logbestanden moeten hierbij grondig worden onderzocht

Wat moet je doen als je gehackt bent?

Draaiboek – Juridisch

Wat moet je op juridisch vlak doen als je gehackt bent?

Datalek

- Wat
  - De GDPR definieert een datalek of een gegevenslek als “een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens
- Voorbeelden van datalekken
  - Verliezen van usb-stick
  - Mail versturen naar een verkeerd adres
  - Verliezen van smartphone
  - Crashen van computer zonder back-up
  - Hacking van gegevens
  - Database per ongeluk openbaar maken

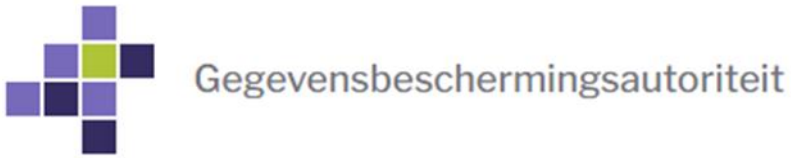
Wat moet je doen als je gehackt bent?

Draaiboek – Juridisch

Wat moet je op juridisch vlak doen als je gehackt bent?

Melding bij de **Gegevensbeschermingsautoriteit (GBA) / Vlaamse Toezichtcommissie (VTC)**

- Je moet ieder datalek melden bij de toezichthoudende overheid. De enige uitzondering is wanneer het onwaarschijnlijk is dat er risico's zijn voor de privacy van de betrokkene(n)
  - ✓ Melding GBA / Melding VTC
- Meld het datalek **binnen 72 uur** na ontdekking aan de toezichthouder (bij een complex datalek: maak een eventuele een voorlopige melding)

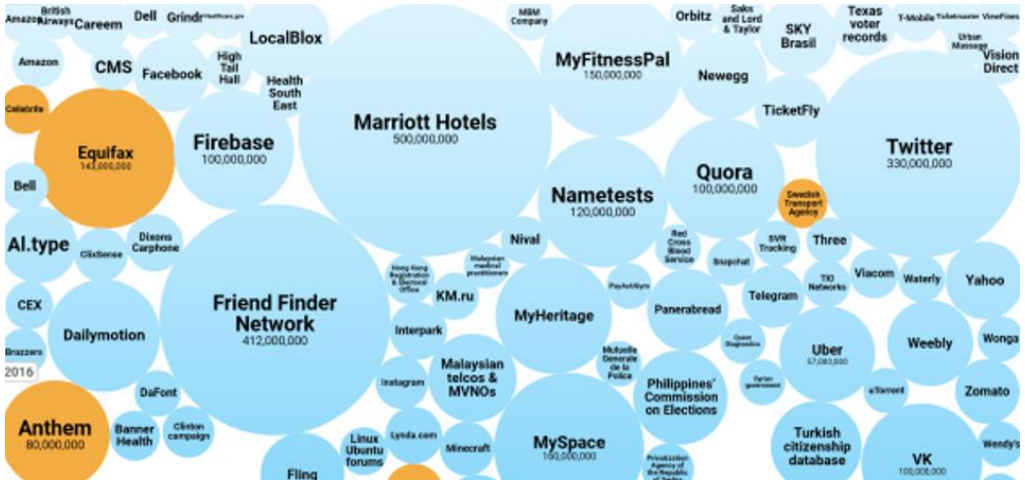


Wat moet je doen als je gehackt bent?

Draaiboek – Juridisch

Wat moet je op juridisch vlak doen als je gehackt bent?

3. **Melding** bij de **betrokkenen**
   - Wanneer een datalek een **groot risico voor de rechten en vrijheden van betrokkenen** oplevert, moeten die hierover zo snel mogelijk geïnformeerd worden. Die mededeling moet dezelfde informatie bevatten als de melding aan de toezichthoudende autoriteiten



Wat moet je doen als je gehackt bent?

Draaiboek – Communicatie

Wat moet je op het vlak van communicatie doen als je gehackt bent?

1. Communiceer intern
   - Lijst je **kernboodschappen** op met wat je al weet en informeer alle medewerkers
   - De inhoud van die eerste interne communicatie is simpel. Je vertelt:
     - ✓ Wat je op dat moment weet
     - ✓ Wie aan welke oplossing werkt
     - ✓ Op welke manier klanten geïnformeerd zullen worden
     - ✓ Wat de roles & responsibilities van je kernteam zijn
     - ✓ Wat je verwacht van je medewerkers
     - ✓ Wanneer ze een volgende update krijgen
   - Zijn er nieuwe **ontwikkelingen**? **Hou de medewerkers regelmatig op de hoogte**

Wat moet je doen als je gehackt bent?

Draaiboek – Communicatie

Een medewerker heeft de hack om 6.30u vastgesteld IT is op de hoogte en werkt aan een oplossing

Interne mail

Beste collega's,

Omstreeks 6.30u vanochtend werd vastgesteld dat een deel van onze database vannacht gehackt werd, waardoor mogelijk gegevens van onze klanten in verkeerde handen zijn gevallen. Onze collega's van IT werken aan een oplossing. In principe kan je mailen en aan documenten werken die lokaal zijn opgeslagen.

Er werd een kernteam opgesteld dat bestaat uit (namen personen). Zij werken onder andere aan de communicatie voor onze klanten. De bedoeling is om hen zo snel mogelijk op de hoogte te brengen van de situatie. Mocht je een klant aan de lijn krijgen met vragen, verbind hem of haar dan door met (naam collega). Gelieve voorlopig zelf niet proactief extern te communiceren over de situatie. Het is belangrijk dat we onze klanten en partners dezelfde en meest up-to- date informatie bezorgen.

Ik hou jullie uiteraard op de hoogte van de situatie. Van zodra er iets nieuws te melden valt, krijgen jullie een update.

Mochten er intussen vragen of bemerkingen zijn, kan je terecht bij (naam collega). Als je zelf technische problemen ondervindt, laat dat dan meteen weten aan (naam collega).

Alvast bedankt voor jullie support, (naam)

Wat moet je doen als je gehackt bent?

Draaiboek – Communicatie

Wat moet je op het vlak van communicatie doen als je gehackt bent?

1. Communiceer extern
   - De inhoud van die externe communicatie. Je vertelt:
     - ✓ Wat je op dat moment weet
     - ✓ Hoe het probleem binnen korte termijn opgelost werd of wordt
     - ✓ Wat de gevolgen zijn voor klanten en partners
     - ✓ Welke next steps ze moeten ondernemen
     - ✓ Bij wie ze terecht kunnen voor vragen
   - Eerst rechtstreeks en zo gepersonaliseerd mogelijk aan klanten via telefoon/mail/direct messaging
   - Daarna algemeen via verschillende kanalen: social media, pers, nieuwsbrief, etc.

Draaiboek – Communicatie

Extern statement

Op 30/8 hebben we vastgesteld dat er - wellicht slechts enkele uren voordien – een inbraakpoging geweest is op onze server. Daardoor zijn mogelijk enkele klantgegevens gestolen. Onze experts zoeken op dit moment uit om welke gegevens het potentieel gaat en hoe een potentieel lek gedicht kan worden.

Er is geen reden tot paniek, maar het is aangeraden dat klanten het wachtwoord van hun account wijzigen. Gevoelige informatie zoals betaalgegevens zijn NIET betrokken bij de hack.

We gaan ervan uit in de loop van de dag meer zicht te hebben op de precieze omvang van de inbraak, en zullen op dat moment alle klanten informeren over welke stappen zij kunnen ondernemen.

Draaiboek – Communicatie

Externe mail

Beste (naam klant),

Afgelopen nacht heeft er een inbraakpoging plaatsgevonden op onze servers. Daarbij zijn geen gevoelige gegevens zoals betaalinformatie gestolen. Wellicht zijn enkele accountgegevens in handen van de hackers gevallen. Het is daarom van groot belang dat u zo snel mogelijk het wachtwoord van uw account wijzigt. Dat doet u zo (werkwijze toevoegen).

Ons IT-team werkt non-stop verder om onze omgeving, die al sterk beveiligd was, nog verder te beschermen en de hackers op te sporen in samenwerking met de bevoegde instanties. Mocht er daarover binnenkort meer nieuws zijn, dan hoort u dat zo snel mogelijk.

Indien u vragen heeft, kunt u terecht op onze website, of kunt u contact opnemen met (naam contact).

Bedankt voor uw begrip.

Vriendelijke groeten (naam)

Helpende handen

Organisaties die je kunnen helpen

Organisaties die je kunnen helpen

Computer Emergency Response Team (CERT)

Melding bij het CERT

- 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**
- **Informatie over hoe een incident te melden** vind je op CERT.be:
  - Een incident melden | Cert
  - Voor de melding naar het CERT verzamel je volgende informatie:
    - Datum, tijdstip en locatie van het incident
    - Vermoedelijke oorzaak
    - Naam van virus of malware
    - (Mogelijks) getroffen data
    - Ondernomen acties
    - Getroffen besturingssystemen en/of software
    - Contactpersoon/-personen

V-ICT-OR VLAAMSE ICT ORGANISATIE

CERT.be The Federal Cyber Emergency Team

EEN INCIDENT MELDEN

Ik ben *

- Select -

Ik wil *

- ☐ een incident melden
- ☐ ondersteuning bij een incident (gelieve je gegevens hieronder in te vullen)
- ☐ een phishingbericht doorsturen (stuur het door naar verdacht@safeonweb.be)

Heb je een verdacht verdacht bericht ontvangen? Stuur het door naar verdacht@safeonweb.be en verwijder het daarna. Als je een verdacht bericht op het werk ontvangt, moet je de procedures die daar gelden voor phishing opvolgen, bv. doorsturen naar de ICT-dienst. Vragen over verdachte berichten worden niet door ons behandeld. Voor meer info over verdachte berichten: www.safeonwweb.be

E-mail

Vul contactgegevens in als je ondersteuning nodig hebt.

Telefoon

+32 479 12 34 56

Contactpersoon

Type incident *

- ☐ Weet niet
- ☐ PC/netwerk wordt gegijzeld door een ransomware
- ☐ PC/netwerk is gehackt
- ☐ PC/netwerk is besmet met een virus
- ☐ CEO-fraude
- ☐ Scam
- ☐ DDOS aanval
- ☐ Ander (nl…)

Als je bijstand wil bij een incident, gelieve dan hierboven het hokje 'ondersteuning bij een incident' aan te vinken en je e-mailadres in te vullen. Als je een phishingbericht wil melden, stuur het bericht dan door naar verdacht@safeonweb.be.

Wanneer vond het incident plaats? *

7 | Dec | 2021

Waar vond het incident plaats?

Locatie van de getroffen systemen

Is het incident opgelost? *

- ○ Ja
- ○ Nee

Organisaties die je kunnen helpen

Computer Emergency Response Team (CERT)

Melding bij het CERT

- CERT.be kan expertise aanbieden om de aanval te stoppen of bij de analyse van de gegevens. Dit kan telefonisch of per e-mail. CERT.be geeft ook **advies** over veel voorkomende kwetsbaarheden en aanvallen. De informatie kan je vinden op:
  - https://cert.be/nl
- Zij kunnen je helpen en kunnen de informatie over het incident gebruiken om andere organisaties te helpen

Organisaties die je kunnen helpen

Lokale Politie

Aangifte bij de lokale politie

- Neem voor **aangifte** van de cyberaanval contact op met de **lokale politie**
- Contacteer hen vooraf zodat zij zich kunnen voorbereiden op jouw verklaring
- De lokale politie zal je eventueel doorverwijzen naar gespecialiseerde diensten binnen de politie, met name de Federal Computer Crime Unit (FCCU) (zie verder)
- Het PV van aangifte bij de politie is noodzakelijk wanneer je voor **schadeloosstelling** je wenst te beroepen op je **cyberverzekering**

Organisaties die je kunnen helpen

Lokale Politie

Aangifte bij de lokale politie

- Met je klacht kan de politie de opsporing naar mogelijke daders starten
- Als je aangifte gaat doen bij de politie, **probeer dan zoveel mogelijk informatie over het incident te verzamelen**:
  1. Het **tijdstip** van het incident: wanneer begon het, wanneer merkte je het op?
  2. De **oorsprong** en de **oorzaak** van de aanval als je deze tenminste kent; dit wordt ook de vector van het incident genoemd. Een geïnfecteerde e-mail (foute link of bijlage) is een veelvoorkomende infectievector
  3. De naam van het **virus of de malware** is nuttig om te delen
  4. Aarzel niet om **screenshots** of foto's (bv. via GSM) van infectiemeldingen te nemen
  5. Deel ook welk soort **data** werd aangetast

Organisaties die je kunnen helpen

Lokale Politie

Aangifte bij de lokale politie

6. En laat weten welke **acties** je ondernomen hebt
7. Vertel de politie ook welk besturingssysteem en welke software je gebruikt
8. Voeg ook volgende **informatie** toe
    a) Logbestanden die wijzen op criminele acties
    b) Screenshots van relevante sporen en meldingen
    c) Images van de harddisk(en)
    d) Netwerkverkeersgegevens van en naar de gecompromitteerde apparatuur Met je klacht kan de politie de opsporing naar mogelijke daders starten

- **Betrek de dienst ICT en DPO bij de aangifte** want technische/juridische vragen

Organisaties die je kunnen helpen

V-ICT-OR

Cyber- en informatieveiligheid

- QRC
  - Via QRC wil V-ICT-OR een netwerk uitbouwen van betrokkenen, zowel vanuit de publieke als private sector, alarmeren om bij gevaar in actie te komen en hen - indien nodig - de juiste informatie te verschaffen.
  - Daarnaast moet dit platform ook gebruikt worden om kennis te delen en om preventief informatie te verspreiden
  - Het is belangrijk dat informatie kan worden gedeeld met anderen, want dan weten anderen dat er ook dreigingen kunnen zijn waar ze zich kunnen op kunt voorbereiden

QRC (V-ICT-OR)

NIEUWS & UPDATES

RSS

Hoe de cyberweerstand van een organisatie snel verhogen?

2022-03-06 0 NIEUWS

Checklist voor een snelle sterkere beveiliging

Ransomware of wiperware voorkomen

- Het is belangrijk dat je toestellen beschermd zijn met een antivirussoftware, maar daarnaast is ook specifieke bescherming tegen ransomware een must. Installeer...

Waarschuwing - Kritieke Gitlab kwetsbaarheid kan aanvallers toelaten om runner registratie tokens te stelen

2022-03-06 0 NIEUWS

Risico's
Ongepatchte versies van Gitlab CE/EE zijn kwetsbaar voor het openbaar maken van informatie door gebruik te maken van quick actions commando's, waardoor een ongeautoriseerde gebruiker loperregistratietokens kan stelen.

Beschrijving
Er is een...

Gemeente Maldegem slachtoffer van cyberaanval

2022-03-06 0 NIEUWS

Cyberparaatheid beoordelen: waar te beginnen?

2022-03-03 0 ARTIKEL

AAN HET WOORD

DPO's ... hou het simpel alsjeblief!

Eddy Van der Stock
V-ICT-OR vzw

Het is eigen aan domeinspecialisten om hun gespecialiseerde materie zo ingewikkeld mogelijk te...
Verder lezen »

NOTIFICATIEVOORKEUREN

Om jouw notificatievoorkeuren te beheren moet je eerst inloggen. Nog geen lid van onze community? Geen nood, registreer jezelf hier!

WIL JE NIEUWS EN DREIGINGEN DELEN MET DE COMMUNITY?

- Tip de redactie via deze website
- Via e-mail
- Via API

Wil je de ingezonden nieuwstips ook mee helpen cureren en zelf ook een redacteur of redactrice van de community worden? Contacteer ons!

V-ICT-OR VLAAMSE ICT ORGANISATIE

Organisaties die je kunnen helpen

Taskforce Cyberveilige Gemeente

Taskforce

Draaiboek Cybercrime

Business continuïteitsplan

Crisiscommunicatieplan

Checklist crisisbeheer

Beleid voor responsible disclosure

Register voor cyberincidenten

Procedure melding cyberincidenten

Interne en externe contactlijsten

Richtlijnen Secure Software Development

Veiligheids- en opvolgingsplan

Richtlijnen organisatiebeheersing

Cybertips en -tricks

Initiatieven verhogen digitale weerbaarheid

Initiatieven

Vlaamse ICT Organisatie (V-ICT-OR)

- Informatieveiligheidstool
- Centraal Aanmeldingsregister
- Begeleiding informatieveiligheid / GDPR
- Begeleiding beleidsplanning
- Cybersecurity
- Oplossingscatalogus
- VlaVirGem
- Aankoopondersteuning
- Opleidingen informatieveiligheid
- Digitaal Horecaloket
- Sokaris - digitale aangifte overlijden
- Begeleiding premiumpakket

Samen met ABB, Audit Vlaanderen, Digitaal Vlaanderen en de VVSG :

- Ontwikkeling Cyber Security Toolkit
- ICT-veiligheidsaudits via Audit Vlaanderen
- Traject Ethisch Hacken in samenwerking met Howest
- Training en Sensibilisering

VLAIO

- Cybersecurity verbetertrajecten (subsidies)

Cyberincidenten voorkomen en bestrijden

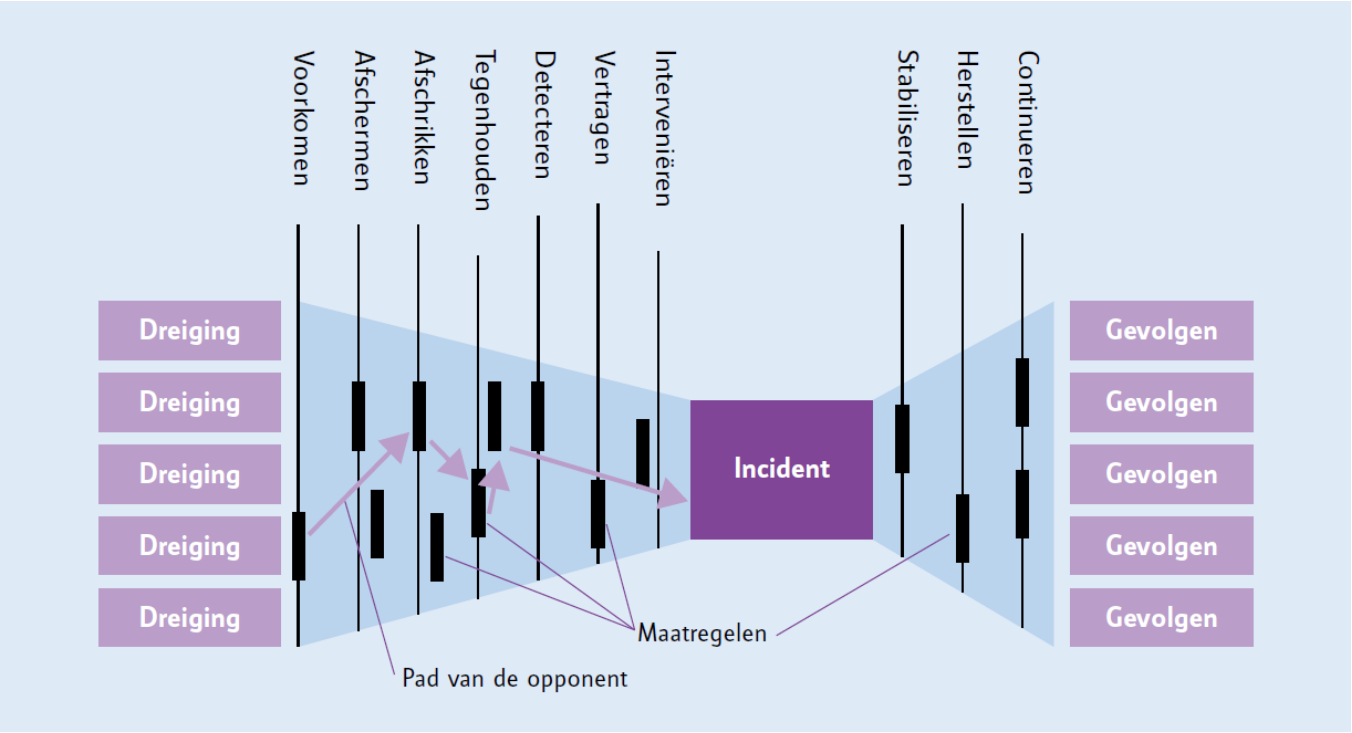
10 geboden - Aanbevelingen Audit Vlaanderen

Cyberincidenten voorkomen

10 geboden voor het voorkomen van cyberincidenten

Cyberincidenten kunnen worden voorkomen door basismaatregelen te nemen

⚠ **Neem zowel preventieve als herstellende maatregelen!**

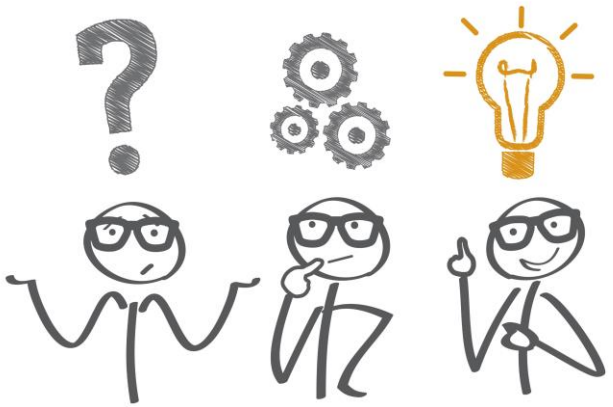


Cyberincidenten voorkomen

10 geboden voor het voorkomen van cyberincidenten

Cyberincidenten kunnen worden voorkomen door basismaatregelen te nemen

1. Gebruik goede **antivirussoftware**. Vraag desgewenst advies aan een expert
2. Zet '**automatisch updaten**' aan; softwareprogramma's en websites blijven zo up-to-date
3. Sta geen korte wachtwoorden toe; kies bijvoorbeeld een **wachtzin** in plaats van een wachtwoord. En: vergeet wachtwoordhergebruik
4. **Vervang** wachtwoorden regelmatig, dwing elk kwartaal wachtwoordwijzigingen af
5. Zorg dat een account na meer dan **vijf foutieve loginpogingen** wordt geblokkeerd
6. Maak altijd gebruik van de **twee-factorauthenticatie** op externe (via het internet beschikbare) systemen of portalen
7. Investeer in goede beveiliging van **routers en firewalls**



V-ICT-OR VLAAMSE ICT ORGANISATIE

10 geboden voor het voorkomen van cyberincidenten

Cyberincidenten kunnen worden voorkomen door basismaatregelen te nemen

- Investeer continu in het **bewustzijn** van je gebruikers inzake veilig gebruik van data en systemen. Zo is mijn bijvoorbeeld bewust kritisch op ontvangen van e-mails
- Zorg voor goede **back-ups**. Die zijn niet zelden de redder in nood bij ransomware
- Laat je adviseren door een **expert** als je er zelf niet uitkomt, **cyberveiligheid is een vak**

Nuttig

Nuttige linken

Nuttig

Nuttige linken

- Community cyber- en informatieveiligheid: informatieveiligheid.be - V-ICT-OR
- Cybersecurity voor jouw organisatie? Start hier!: Eerste hulp bij cyberpreventie - V-ICT-OR
- Centrum voor Cybersecurity België (CCB)
- verdacht@safeonweb.be (mailadres om verdachte mails te melden)
- Computer Emergency Response Team (CERT)
- De politie
- Meldpunt (belgie.be)

Nuttige linken

- Check je link: Checkjelinkje - checkjelinkje.nl
- Analyseer verdachte bestanden en URL's op malware: VirusTotal - Home
- Test je website, e-mail en je verbinding: Test voor moderne Internetstandaarden zoals IPv6, DNSSEC, HTTPS, DMARC, STARTTLS en DANE.
- Verkorte link omzetten naar normale link: Unshorten that URL! - Unshorten.It!
- Analyseer een bestand: Kaspersky Threat Intelligence Portal
- Scan je website: Analyse your HTTP response headers (securityheaders.com)
- Cookie Checker Tool voor websites: Cookieserve - Free online cookie checker for sites
- Identificeer ransomware: ID Ransomware (malwarehunterteam.com)
- Hulp bij het ontsleutelen van uw digitale bestanden: Home | The No More Ransom Project
- Nagaan of je gebruikersnaam en wachtwoord is gelekt: Have I Been Pwned: Check if your email has been compromised in a data breach

VRAGEN?

Dank aan …

Deelnemers Infosessie

Ward van Hal, Liesbeth Belmans (VVSG)

Vlaamse ICT Organisatie (V-ICT-OR)

Werkgroep Informatieveiligheid V-ICT-OR

Digitale Transformatie van jouw lokaal bestuur?

Word lid van de Grootste Digitale Club!

Zet deze 3 belangrijke data alvast in uw agenda

1. Donderdag 12 mei 2022 > Shopt IT in Flanders Expo Gent
2. Donderdag 6 oktober 2022 > CIS-dag in Lamot Mechelen
3. Donderdag 8 december 2022 > Manage IT in Hilton Antwerpen met Gouden Bit en Gouden awards 2022

V-ICT-OR VLAAMSE ICT ORGANISATIE

CONTACT

V-ICT-OR vzw

Gentstraat 9 - 9250 Waasmunster

www.v-ict-or.be
info@v-ict-or.be

Bijlage

Autopsie van een cyberaanval

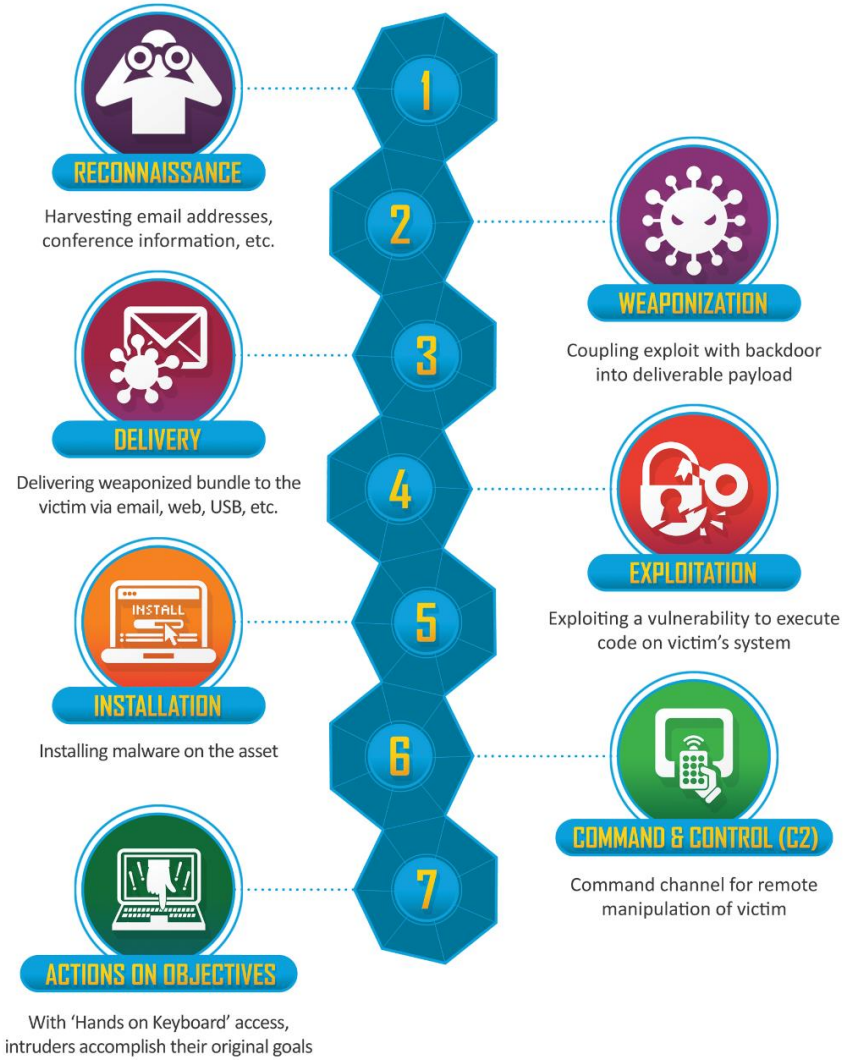
The Cyber Kill Chain

Autopsie van een cyberaanval

Fasen

De 7 fasen van een cyberaanval: ‘The Cyber Kill Chain’

Belangrijk: in elke fase van de ketting de passende maatregelen nemen om erger te Voorkomen!



Autopsie van een cyberaanval

Fasen

De 7 fasen van een cyberaanval

1. **Reconnaissance-fase (verkenning)**: de aanvallers zoeken zwakke plekken in de organisatie (aanvalsoppervlak in kaart brengen).
   - Fysiek: Inbrekers verkennen villa's waar ramen openstaan en deuren niet op slot zijn
   - Digitaal: Scannen op kwetsbaarheden, op open poorten, op onbeveiligde koppelingen naar externen
2. **Weaponization-fase (bewapening)**:
   - Fysiek: inbrekers voorzien zich van een koevoet
   - Digitaal: de aanvallers ontwikkelen malware om deze zwakke plekken te misbruiken
3. **Delivery-fase (aflevering)**:
   - Fysiek: De inbrekers gaan met hun breekijzer naar de villa waar ze willen inbreken
   - Digitaal: de aanvallers bezorgen de malware, bijvoorbeeld via e-mail

Autopsie van een cyberaanval

Fasen

De 7 fasen van een cyberaanval

4. **Exploitation-fase (uitbuiting)**:
   - Fysiek: de inbrekers forceren met hun koevoet de deur open
   - Digitaal: een medewerker activeert per ongeluk de malware, door op een link in een onbetrouwbare e-mail te klikken
5. **Installation-fase (installatie)**:
   - Fysiek: De inbrekers verkennen geruisloos de villa
   - Digitaal: de aanvallers installeren zich in het netwerk en gaan op verkenning
6. **Command and control-fase (beheer en controle)**:
   - Fysiek: De inbrekers nemen contact op met een handlanger om bijvoorbeeld de code van de kluis te vernemen
   - Digitaal: de aanvallers installeren vervolgens nieuwe malware (bijv. voor ransomware aanval)

Autopsie van een cyberaanval

Fasen

De 7 fasen van een cyberaanval

7. **Actions on objectives-fase (uitvoeren van het doel)**:
   - Fysiek: De inbrekers vinden de juwelen, het geld en gaan er zo onopgemerkt mogelijk (geen sporen nalaten) mee aan de haal
   - Digitaal: De aanvallers bereiken hun doel en kunnen ongemerkt informatie wegsluizen
   - Tip: neem voor elke fase de nodige veiligheidsmaatregelen (zie verder)

Autopsie van een cyberaanval

Fasen

Fase 1: **Reconnaissance (verkenning)** - De aanvallers zoeken zwakke plekken in de organisatie

Vergelijking met een fysieke inbraak

- Inbrekers zijn op zoek naar doelwitten. Eenmaal gekozen gaan ze de omgeving van de doelwitten fysiek verkennen. Ze verkennen de wegen die naar hun doelwitten leiden. Ook onderzoeken ze op welk tijdstip bepaalde mensen aanwezig zijn, of er alarmsystemen zijn en of er camera's hangen. Daarnaast gaan ze op zoek naar deuren die niet op slot zitten of ramen die vaak openstaan

Digitale inbraak

- In de Reconnaissance-fase verzamelen cyberaanvallers zoveel mogelijk informatie over de zwakke plekken van hun doelwit
  - Zwakke plekken kunnen zowel personen als technische kwetsbaarheden zijn

Autopsie van een cyberaanval

Fasen

Fase 1: **Reconnaissance (verkenning)** - De aanvallers zoeken zwakke plekken in de organisatie

- Werkwijze aanvallers
  - Scannen op bekende kwetsbaarheden in systemen en apparaten die gekoppeld zijn met het internet
  - Scannen op openstaande poorten om inzicht in de infrastructuur van uw organisatie te krijgen
- Beveiligingsmaatregelen
  1. Zet ongebruikte poorten dicht
  2. Houd aan het internet gekoppelde systemen en apparaten up-to-date en voorzie ze van de laatste patches en configuraties
  3. Beschouw partnerkoppelingen niet standaard als vertrouwd en stel eisen aan de beveiliging van de systemen van uw partners
  4. Maak gebruik van detectieoplossingen
     - ✓ Bijv. een Network based Intrusion Detection System (NIDS) - Monitort en analyseert inkomend en uitgaand netwerkverkeer op verdachte activiteiten

Autopsie van een cyberaanval

Fasen

Fase 2: **Weaponization (bewapening) -** De aanvallers ontwikkelen malware om deze zwakke plekken te misbruiken

- Als aanvallers een zwakke plek hebben gevonden ontwikkelen ze gereedschap, bijvoorbeeld malware, om deze te misbruiken

Vergelijking met een fysieke inbraak

- De inbrekers hebben besloten om in te breken in de villa van het doelwit. Tijdens hun verkenningen kwamen ze erachter dat ze het gebouw makkelijkst kunnen binnenkomen door met een breekijzer de achterdeur te openen

Digitale inbraak

- Cyberaanvallen kiezen op basis van hun verkenningen welke kwetsbaarheid ze willen misbruiken
- Tijdens de Weaponization-fase kiezen of ontwikkelen aanvallers gereedschap met een zo hoog mogelijke slagingskans
- Aanvallers zetten exploits in om toegang te krijgen tot systemen. Via deze toegang kan vervolgens malware (kwaadaardige software) worden geïnstalleerd, waarmee de aanvallers controle kunnen krijgen over deze systemen

Autopsie van een cyberaanval

Fasen

Fase 2: **Weaponization (bewapening)** - De aanvallers ontwikkelen malware om deze zwakke plekken te misbruiken

Advies – Wat kunt u doen?

In de Weaponization-fase bereiden aanvallers zich voor op een cyberaanval. In deze fase is er nog geen interactie met het doelwit. Daarom is het zeer lastig om de aanvaller in deze fase te herkennen of stoppen. Dit betekent niet dat u niets kunt doen

Autopsie van een cyberaanval

Fasen

Fase 3: **Delivery (aflevering) -** De aanvallers bezorgen de malware, bijvoorbeeld via e-mail

- Als het doelwit geselecteerd is en de malware klaar ligt voor gebruik, bezorgen de aanvallers de malware bij de organisatie met behulp van bijvoorbeeld een e-mail

Vergelijking met een fysieke inbraak

- De inbrekers rijden met hun breekijzer achterin hun bus naar de villa

Digitale inbraak

- Het versturen van (spear)phishingmails is daarom een veelgebruikte methode om malware bij het slachtoffer af te leveren
- Hacken van een website die kwetsbaarheden bevat en die vaak bezocht wordt door medewerkers. Op deze website brengen de aanvallers vervolgens malware aan waardoor bezoekers geïnfecteerd worden zodra ze de website bezoeken.
- Gratis USB-sticks uitdelen waarop al malware geïnstalleerd staat, in de hoop dat medewerkers van het beoogde doelwit de USB-sticks gebruiken op de systemen van de organisatie.

Autopsie van een cyberaanval

Fasen

Fase 3: **Delivery (aflevering) -** De aanvallers bezorgen de malware, bijvoorbeeld via e-mail

Advies – Wat kunt u doen?

In de Delivery-fase moeten beveiligingsmaatregelen gekozen worden die voorkomen dat de malware die in de Weaponization-fase is ontwikkeld, daadwerkelijk wordt afgeleverd

- beveiligingsmaatregelen
  1. Inkomende e-mails en eventuele bijlagen scannen op malware en verdachte URL's
     - ✓ Gebruik van een proxyserver, sandboxes, VPN
  2. Herkomst van e-mails controleren aan de hand van technieken als Domain-based Message Authentication, Reporting and Conformance (DMARC), Domain Keys Identified Mail (DKIM) of Sender Policy Framework (SPF). Deze technieken blokkeren e-mails van onbekende herkomst.
  3. Ook kunt u met behulp van policies instellen dat uitvoerbare bestandstypen als .exe of .msi niet zijn toegestaan in de bijlage van een e-mail, zodat deze niet in de inbox van een gebruiker kunnen komen.

Autopsie van een cyberaanval

Fasen

Fase 3: **Delivery (aflevering) -** De aanvallers bezorgen de malware, bijvoorbeeld via e-mail

4. Daarnaast kunt u browsers en applicaties hardenen om het risico te verkleinen dat systemen van medewerkers besmet kunnen raken door het bezoeken van geïnfecteerde webpagina's. Met het hardenen van browsers wordt bijvoorbeeld het uitschakelen van plug-ins bedoeld die als kwetsbaar bekend staan. Denk bij het hardenen van applicaties aan het uitschakelen van Office macro's die de gebruiker niet nodig heeft. Macro's worden vaak ingezet om malware over te brengen
5. Stel ook beleid op voor het gebruik van verwijderbare media en datadragers en het koppelen van eigen hardware (Bring Your Own Device) met het bedrijfsnetwerk. Denk hierbij bijvoorbeeld aan USB-sticks. Zet USB-poorten dicht en sta alleen geregistreerde USB-media toe die is uitgegeven en onder controle is van de eigen organisatie. Schakel daarbij ook de autorun-functionaliteit uit op verschillende media
6. Het gebruik van een antivirusprogramma of een Next-Generation Antivirus (NGAV) helpt in de Delivery-fase bij het vinden van eventuele malware.

Autopsie van een cyberaanval

Fasen

Fase 4: **Exploitation-fase (uitbuiting)** - Een medewerker activeert per ongeluk de malware, door op een link in een onbetrouwbare e-mail te klikken

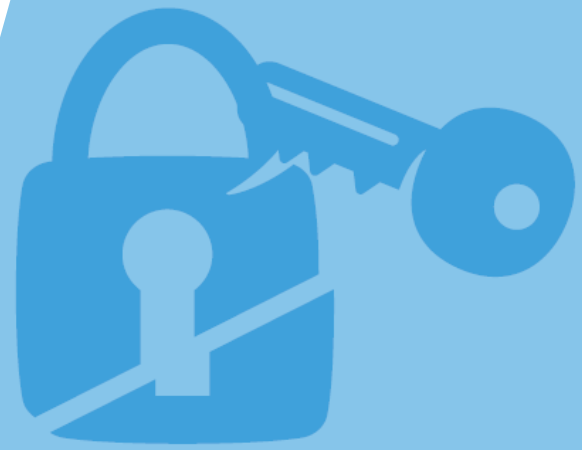
- In deze fase wordt de malware geactiveerd, doordat bijvoorbeeld een van de medewerkers op een link in een malafide e-mail klikt

Vergelijking met een fysieke inbraak

- Een van de inbrekers wrikt met het breekijzer de deur open. In deze fase gaat de inbreker nog niet naar binnen. Hij heeft alleen toegang voor zichzelf weten te creëren

Digitale inbraak

- Het laatste deel om toegang te krijgen gebeurt in de Exploitation-fase. Aanvallers moeten de 'deur' nog forceren. De Exploitation-fase is daarom gericht op het activeren van de malware. Denk hierbij aan een medewerker die op de link in de (spear)phishingmail moet klikken om de malware te activeren waarmee aanvallers toegang kunnen krijgen



Autopsie van een cyberaanval

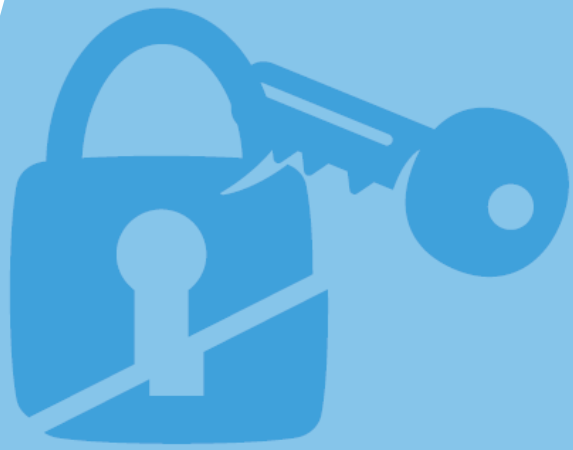
Fasen

Fase 4: **Exploitation-fase (uitbuiting)** - Een medewerker activeert per ongeluk de malware, door op een link in een onbetrouwbare e-mail te klikken

Advies – Wat kunt u doen?

Aanvallers hebben in deze fase nog geen stevige voet aan de grond. De beveiligingsmaatregelen in deze fase richten zich op het ontdekken en blokkeren van kwaadaardige code of scripts

- Beveiligingsmaatregelen
    1. Maak in deze fase gebruik van application whitelisting. Deze maatregel verbiedt alle software op systemen met uitzondering van software die op een door de organisatie samengestelde vertrouwde lijst (whitelist) staat. Hiermee verlaagt u het risico dat malware kan worden geïnstalleerd of uitgevoerd
    2. Aanvallers proberen gebruikers in deze fase te misleiden om een handeling uit te voeren. Maak uw medewerkers daarom bewust van de risico's van (spear)phishing en het klikken op onbekende links. Adviseer medewerkers om eerst de afzender van een verdachte e-mail te bellen of te mailen voor zij de bijlage of URL openen

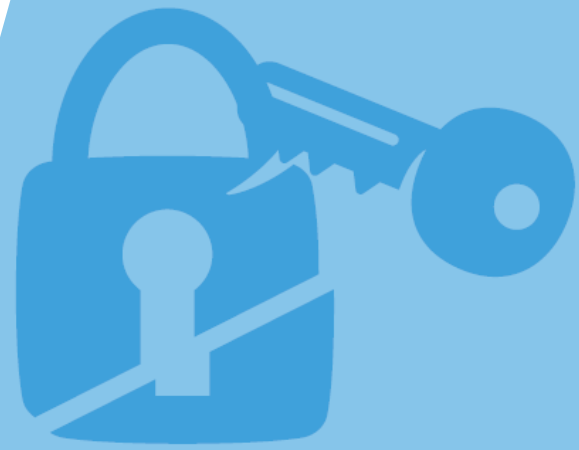


Autopsie van een cyberaanval

Fasen

Fase 4: **Exploitation-fase (uitbuiting)** - Een medewerker activeert per ongeluk de malware, door op een link in een onbetrouwbare e-mail te klikken

3. Het is belangrijk om periodieke beveiligingstesten als kwetsbaarhedenscans, pentesten en red teaming-oefeningen uit te voeren, zodat u kwetsbaarheden en gevonden toegangspaden tijdig kunt mitigeren.



Autopsie van een cyberaanval

Fasen

Fase 5: **Installation-fase (installatie)** - de aanvallers installeren zich in het netwerk

- In de installatiefase nestelen aanvallers zich in het netwerk van het doelwit en proberen hierbij permanente toegang te krijgen

Vergelijking met een fysieke inbraak

- De inbreker gaat in deze fase via de opengebroken achterdeur binnen en zet zijn telefoon aan, zodat hij in de volgende fase contact kan opnemen met zijn handlanger. Vervolgens gaat hij de villa zo geruisloos mogelijk verkennen: op kousenvoeten en zonder lampen aan te doen. Hierbij kan hij op deuren stuiten die gesloten zijn of een kluis tegenkomen. Afhankelijk van de gereedschappen die hij zelf heeft meegenomen, kan hij deze openen. Anders moet hij hiermee wachten tot hij (in de volgende fase) contact heeft gehad met zijn handlanger

Autopsie van een cyberaanval

Fasen

Fase 5: **Installation-fase (installatie)** - de aanvallers installeren zich in het netwerk

- In de installatiefase nestelen aanvallers zich in het netwerk van het doelwit en proberen hierbij permanente toegang te krijgen.

Digitale inbraak

- Als aanvallers toegang tot het computersysteem van het doelwit hebben gekregen, proberen ze zo snel mogelijk de meest uitgebreide rechten binnen het netwerk te krijgen. Dit zijn bij voorkeur de rechten van een beheerder. Met deze rechten is het mogelijk om het netwerk zo uitgebreid mogelijk te verkennen. Dit wordt lateraal bewegen genoemd.

Autopsie van een cyberaanval

Fasen

Fase 5: **Installation-fase (installatie)** - de aanvallers installeren zich in het netwerk

Advies – Wat kunt u doen?

Kies in deze fase beveiligingsmaatregelen die voorkomen dat aanvallers zich permanent op meerdere plekken in het netwerk kunnen nestelen.

1. Een effectieve maatregel is het compartimenteren van systemen en het segmenteren van netwerken. Compartimenteren doet u door niet noodzakelijke verbindingen uit te schakelen. Bij segmenteren deelt u het netwerk in verschillende stukken in. Zo beperkt u de toegang tot vertrouwelijke informatie of kritieke processen tot de medewerkers, applicaties en computers die deze toegang daadwerkelijk nodig hebben.
2. Ook is het minimaliseren van rechten belangrijk. Beperk daarom het aantal beheerdersaccounts en beperk de rechten voor beheerdersactiviteiten binnen deze accounts
3. Multifactorauthenticatie (MFA)
4. Gebruik maken van een SOC en een SIEM

Autopsie van een cyberaanval

Fasen

Fase 5: **Installation-fase (installatie)** - de aanvallers installeren zich in het netwerk

Advies – Wat kunt u doen?

1. Als u een Security Operations Center (SOC) heeft, kunt u samen een detectiestrategie bepalen. Een SOC maakt gebruik van een Security Information & Event Management Systeem (SIEM) waar logging en relevante data centraal op binnenkomen. Zij kunnen bijvoorbeeld zien of accounts hebben ingelogd die eerder nog niet actief waren of waarbij de laatste inlogpoging langere tijd geleden was. Als er meerdere foutieve inlogpogingen zijn gezien is dit verdacht.
2. Een SOC kan daarbij ook vaststellen of gebruikersaccounts extra rechten hebben gekregen of onderdeel zijn geworden van de beheerdersgroep en onderzoeken of deze wijziging klopt. Als u geen SOC heeft, kunt u overwegen om een security dienstverlener in te schakelen.

Autopsie van een cyberaanval

Fasen

Fase 6: **Command and control-fase (beheer en controle)** - De aanvallers komen dankzij de malware op afstand binnen en installeren vervolgens nieuwe malware

- In deze fase leggen de aanvallers op afstand contact met de geïnstalleerde malware binnen het netwerk en kunnen via dit communicatiekanaal nieuwe malware installeren.

Vergelijking met een fysieke inbraak

- De fysieke inbreker neemt contact op met zijn handlanger. Die geeft hem instructies en voorziet hem van extra gereedschappen die hij nodig heeft. Soms bestaat dat gereedschap uit een (inlog)code voor een computer of een kluis die telefonisch doorgegeven kan worden. Vaak zal de inbreker een achterdeur van het slot doen om gereedschappen aangereikt te krijgen. Hiermee creëert de inbreker ook meteen een andere in- en uitgang voor zichzelf als het raam geen optie meer is als uitgang.

Autopsie van een cyberaanval

Fasen

Fase 6: **Command and control-fase (beheer en controle)** - De aanvallers komen dankzij de malware van afstand binnen en installeren vervolgens nieuwe malware

Digitale inbraak

- In de digitale wereld neemt de malware op enig moment na de installatie contact op met de Command and Control-server, ook wel C2-server genoemd. De aanvaller heeft in deze fase permanente toegang tot het netwerk gekregen en kan op afstand de malware via de achterdeuren die hij in de Installation-fase heeft geplaatst besturen en nieuwe malware het netwerk binnenbrengen.
- Deze communicatie wordt Command and Control-verkeer (C2-verkeer) genoemd. Met nieuwe malware kunnen aanvallers nog dieper het netwerk binnendringen om op zoek te gaan naar de data waarin zij geïnteresseerd zijn..

Autopsie van een cyberaanval

Fasen

Fase 6: **Command and control-fase (beheer en controle)** - De aanvallers komen dankzij de malware van afstand binnen en installeren vervolgens nieuwe malware

Advies – Wat kunt u doen?

- Deze fase is het laatste moment dat u heeft om ervoor te zorgen dat aanvallers niet de volgende en laatste stap kunnen zetten. In deze fase moeten beveiligingsmaatregelen gekozen worden die het C2-verkeer ontdekken en voorkomen dat aanvallers via de C2-server kunnen communiceren.
- Beveiligingsmaatregelen
    1. In deze fase wilt u de kans verkleinen dat aanvallers succesvol hun C2-server kunnen aanspreken. Beperk bijvoorbeeld het aantal internettoegangen, zodat aanvallers minder geschikte plekken hebben om achterdeuren te plaatsen. Ook kan al het netwerkverkeer via een proxy of next-generation firewall (NGFW) geleid worden. Een proxy kan op afwijkend verkeer filteren waardoor C2-verkeer geblokkeerd wordt.

Autopsie van een cyberaanval

Fasen

Fase 6: **Command and control-fase (beheer en controle)** - De aanvallers komen dankzij de malware op afstand binnen en installeren vervolgens nieuwe malware

Advies – Wat kunt u doen?

2. Daarnaast kunt u gebruikmaken van DNS-sinkholing. Dit is een techniek waarbij domeinnamen die aanvallers voor hun C2-server gebruiken niet meer geresolved worden. In de praktijk zorgt deze beveiligingsmaatregel ervoor dat er geen verkeer meer mogelijk is tussen het organisatienetwerk en de C2-server van aanvallers.
3. Zorg voor actieve monitoring.

Autopsie van een cyberaanval

Fasen

Fase 7: **Actions on objectives-fase (uitvoeren van het doel)** - De aanvallers bereiken hun doel en kunnen ongemerkt informatie wegsluizen

- Vanaf het moment dat aanvallers permanente toegang hebben gekregen, kunnen zij zich focussen op het bereiken van het doel waarvoor ze de cyberaanval zijn gestart, bijvoorbeeld het ongemerkt wegsluizen van informatie.

Vergelijking met een fysieke inbraak

- In deze fase overhandigt de inbreker uw kroonjuwelen aan zijn handlanger via het openstaande raam waarlangs hij is binnengekomen of via een eerder opengezette achterdeur.

Autopsie van een cyberaanval

Fasen

Fase 7: **Actions on objectives-fase (uitvoeren van het doel)** - De aanvallers bereiken hun doel en kunnen ongemerkt informatie wegsluizen

Digitale inbraak

- In deze fase sluizen aanvallers de informatie weg waar zij op uit waren via de verkregen toegang of via het communicatiekanaal met de C2-server. Bij cyberspionage wordt bedrijfs- of overheidsgevoelige informatie van uw organisatienetwerk overgeheveld naar het systeem van de aanvaller. In deze fase wordt steeds vaker niet alleen informatie gestolen die interessant is voor het land waar de opdracht vandaan komt, maar wordt ook andere informatie (bijvangst) buitgemaakt. Aanvallers maken bij hun cyberaanvallen regelmatig gebruik van ingehuurde hackers, die buitgemaakte bijvangst online op zwarte markten te koop aanbieden. Ook kunnen aanvallers in deze fase overgaan tot het saboteren van systemen of het aantasten van de integriteit van uw data.

Autopsie van een cyberaanval

Fasen

Fase 7: **Actions on objectives-fase (uitvoeren van het doel)** - De aanvallers bereiken hun doel en kunnen ongemerkt informatie wegsluizen

Advies – Wat kunt u doen?

- Beveiligingsmaatregelen
    1. U kunt besmette systemen het best isoleren om verdere besmetting te voorkomen. Bij het opschonen van de systemen is het belangrijk dat de aanvaller niet meer op het betreffende systeem aanwezig is en dat alle besmette systemen geschoond worden. U kunt overwegen om nieuwe en ongebruikte systemen in te zetten. Het herstellen van een schone en geverifieerde back-up is de effectiefste manier om zo snel mogelijk de geraakte functionaliteiten weer beschikbaar te stellen. Houd er bij het isoleren van systemen rekening mee dat aanvallers zeer waarschijnlijk opnieuw zullen proberen het netwerk binnen te dringen.

Autopsie van een cyberaanval

Fasen

Fase 7: **Actions on objectives-fase (uitvoeren van het doel)** - De aanvallers bereiken hun doel en kunnen ongemerkt informatie wegsluizen

Advies – Wat kunt u doen?

2. Een goed incident respons-proces is nodig om onderzoek naar een incident te kunnen doen, maar ook om te bepalen welke stappen u als eerst zet. Voordat u de 'oude' situatie kunt herstellen, is het belangrijk dat u vaststelt hoe de aanval is ontstaan en welke informatie de aanvaller heeft buitgemaakt. Daarbij kunt u gebruikmaken van onafhankelijke organisaties die gespecialiseerd zijn in digitaal forensisch onderzoek. Binnen uw organisatie moet u daarnaast duidelijke processen opstellen en duidelijke verantwoordelijkheden afspreken om adequaat te kunnen reageren. Oefen periodiek een dergelijke crisissituatie binnen de organisatie.

Autopsie van een cyberaanval

Fasen

Fase 7: **Actions on objectives-fase (uitvoeren van het doel)** - De aanvallers bereiken hun doel en kunnen ongemerkt informatie wegsluizen

Advies – Wat kunt u doen?

3. Als uw organisatie een vitale rol heeft in de maatschappij, wordt aangeraden om deze vitale ICT-functionaliteiten binnen een apart geïsoleerd netwerk te plaatsen ten opzichte van het kantoorautomatiseringsnetwerk. Veilige koppelingen kunnen het mogelijk maken om informatie tussen de netwerken uit te wisselen. Zeker in het geval van vitale processen is het (laten) inrichten van een SOC en een Computer Emergency Response Team (CERT) van cruciaal belang om adequaat te kunnen reageren. Zo kunt u direct handelen en beperkt u eventuele schade.

Autopsie van een cyberaanval

Fasen

Fase 7: **Actions on objectives-fase (uitvoeren van het doel)** - De aanvallers bereiken hun doel en kunnen ongemerkt informatie wegsluizen

Advies – Wat kunt u doen?

2. Met Data Loss Prevention (DLP) voorkomt u dat gevoelige of vertrouwelijke data onbedoeld terechtkomt bij personen buiten de organisatie. Hiermee kunt u data die de organisatie dreigt te verlaten ontdekken en deze datastromen op tijd blokkeren. Aanvullend kunnen er beveiligingsmaatregelen gekozen worden die voorkomen dat deze data bekeken kan worden. Denk hierbij aan het versleutelen van data. Als u in deze fase aanvallers ontdekt, is het belangrijk om te bedenken of u direct mitigerende maatregelen neemt.