EKCO SLBDIENSTEN.NL

Cyberaanvallen
van detectie tot respons

Thijs Bisseling — Presales Consultant

thijs.bisseling@ek.co

Agenda

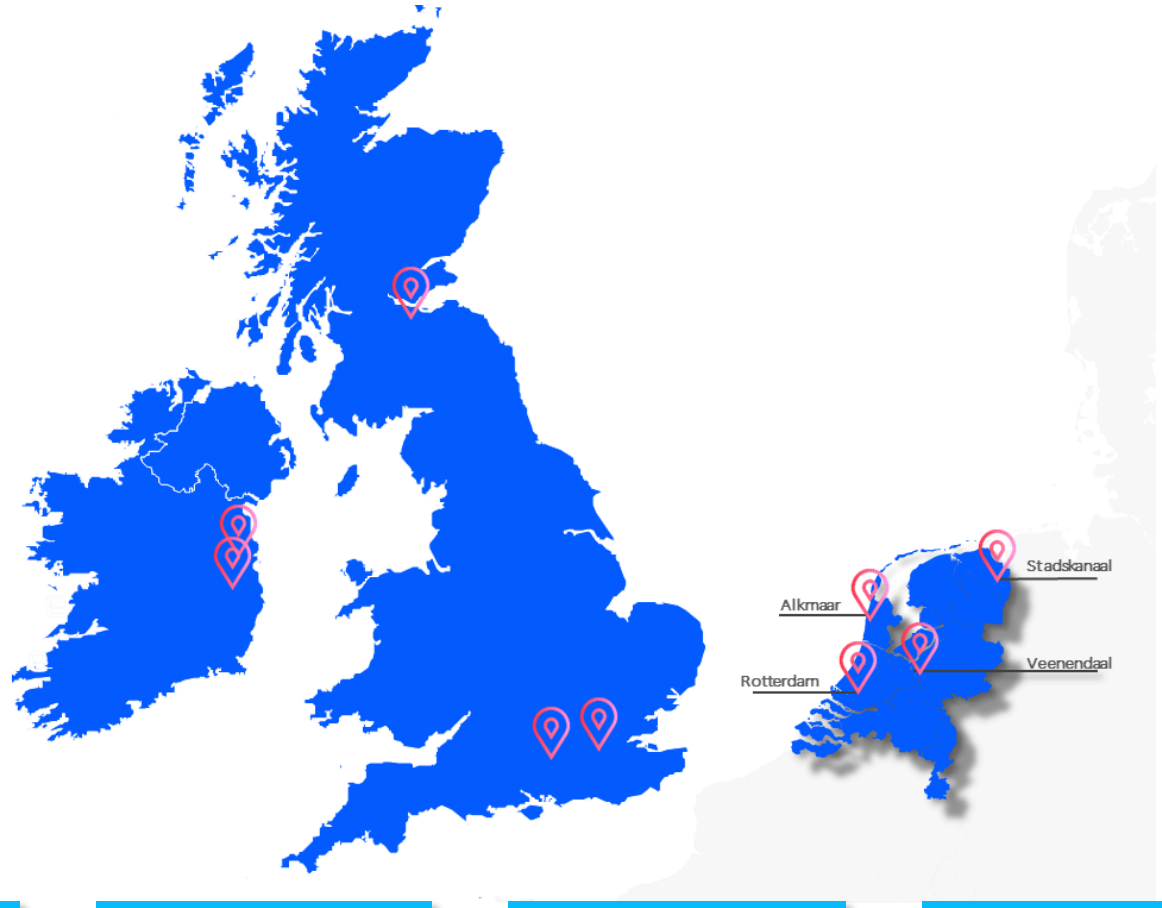
- Intro
- Welke fases zijn er bij een cyberaanval
- Je bent alsnog gehackt.... Wat nu? Praktijkvoorbeeld
- Samenvattend

Even voorstellen

Thijs Bisseling
Presales Consultant
LinkedIn

Over EKCO

- 1000+ IT professionals
- waarvan 110 in NL en 250 security specialisten
- 14 kantoor locaties in UK, IRL waarvan 4 in NL
- 44 jaar IT & beheer ervaring, 18 jaar cloud ervaring
- Focus 75 Tot 750 werkplekken
- Klantbeoordeling 4,7 van 5



Cloud Services

Workspace Services

Security Services

Managed Services

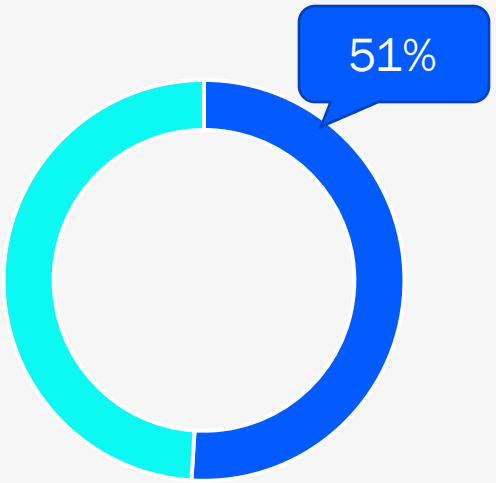
Business Continuity

Consultancy

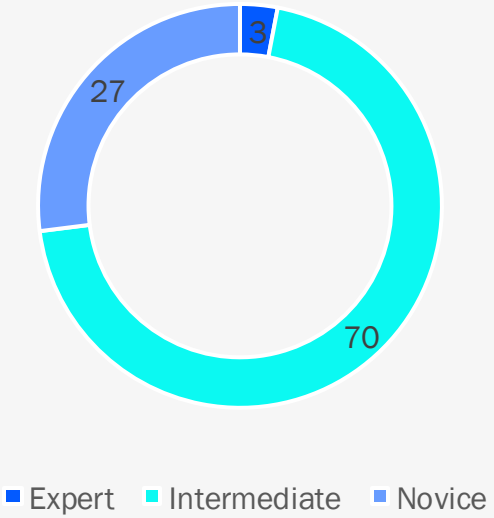
Cybersecurity

Waar staan we vandaag de dag?

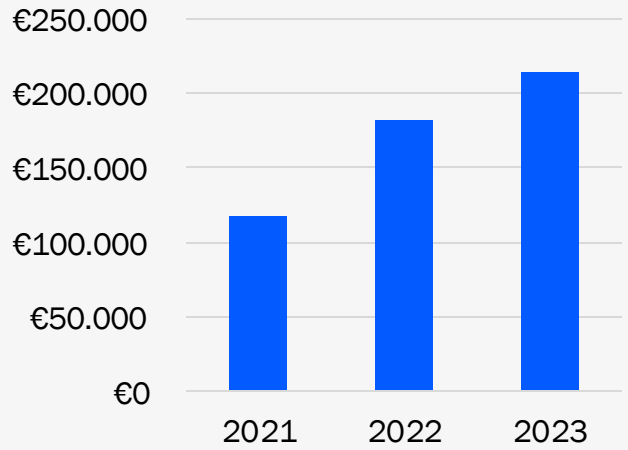
Meer dan de helft van de bedrijven heeft te maken gehad met een cyberaaanval



Cyber volwassenheid in Nederland



Mediaan schadekosten is gestegen met 55%



Bron: Hiscox-Cyber-Readiness-Report-2023.pdf (hiscoxgroup.com)

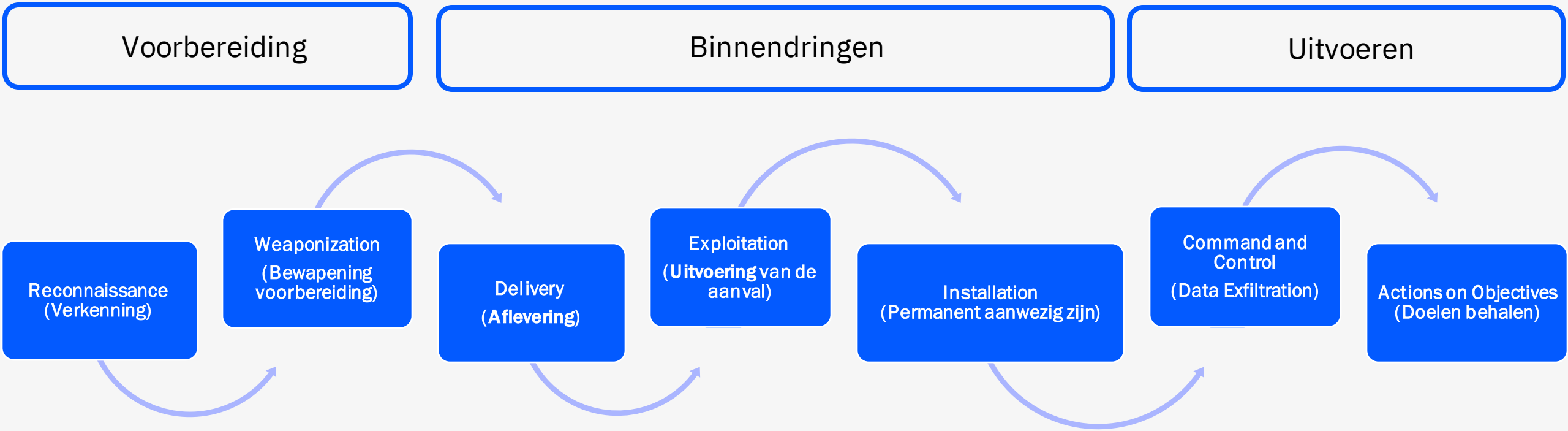
- Iedereen heeft een brandverzekering. De kans op een brand is 1 op 8000 en de schade gemiddeld € 13.790,-

- Inmiddels heeft 56% (in 2020 was het nog maar 20%) van het MKB een cybersecurity verzekering. De kans op een cyberaanval is 1 op 8 en de schade is gemiddeld € 270.000,-

Welke fases zijn er bij een Cyberaanval

Cyber Kill Chain

7 fases bij cybercrime



Fase 1: Reconnaissance

Verkenning (Informatie verzamelen)

- De aanvaller verzamelt informatie over het doelwit, zoals netwerkinfrastructuur, systeemconfiguraties, en mogelijke zwakke punten. Dit kan gebeuren via openbare bronnen, social media, of zelfs directe interacties met het doelwit.

Reconnaissance
(Verkenning)

Fase 2: Weaponization

Bewapening (Voorbereiding)

• De aanvaller verzamelt informatie over het doelwit, zoals netwerkinfrastructuur, systeemconfiguraties, en mogelijke zwakke punten. Dit kan gebeuren via openbare bronnen, social media, of zelfs directe inte
doe

Reconnaissance (verkenning)

Weaponization (Bewapening voorbereiding)

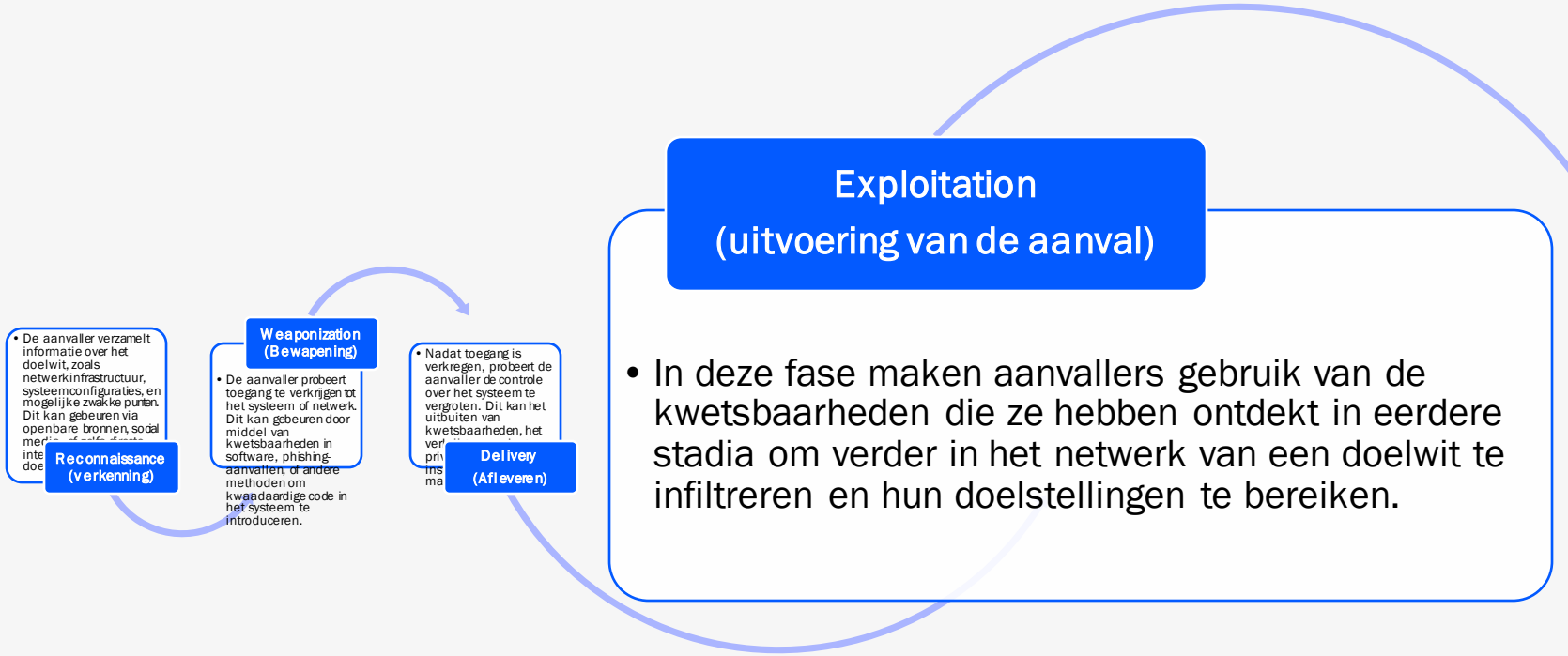
- De aanvaller bepaalt wat hij nodig heeft **om** binnen te komen. Dit kan gebeuren **doormiddel** van kwetsbaarheden in software, phishing-aanvallen, of andere methoden om kwaadaardige code in het systeem te introduceren.

Fase 3: Delivery

Aflevering

Fase 4: Exploitation

Uitvoering van de aanval

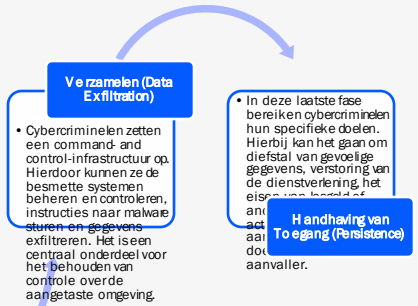


Fase 5: Installation (Persistence)

Permanent aanwezig zijn

- Zodra toegang is verkregen, installeert de cybercrimineel de schadelijke software of vestigt hij zich permanent in het aangetaste systeem. Hierbij kan het gaan om het creëren van “backdoors” of andere middelen om de toegang te behouden, zelfs nadat de eerste toegangspunten zijn gesloten.

Installation (Permanent aanwezig zijn)



Fase 6: Command and Control (C2)

In controle zijn van de besmette systemen

Command and Control (Data Exfiltration)

- Cybercriminelen zetten een command- and control-infrastructuur op. Hierdoor kunnen ze de besmette systemen beheren en controleren, instructies naar malware sturen en gegevens exfiltreren. Het is een centraal onderdeel voor het behouden van controle over de aangetaste omgeving.

- In deze laatste fase bereiken cybercriminelen hun specifieke doelen. Hierbij kan het gaan om diefstal van gevoelige gegevens, verstoring van de
eis
act
doelstellingen van de aanvaller.

Handhaving van Toegang (Persistence)

Fase 7: Actions on Objectives

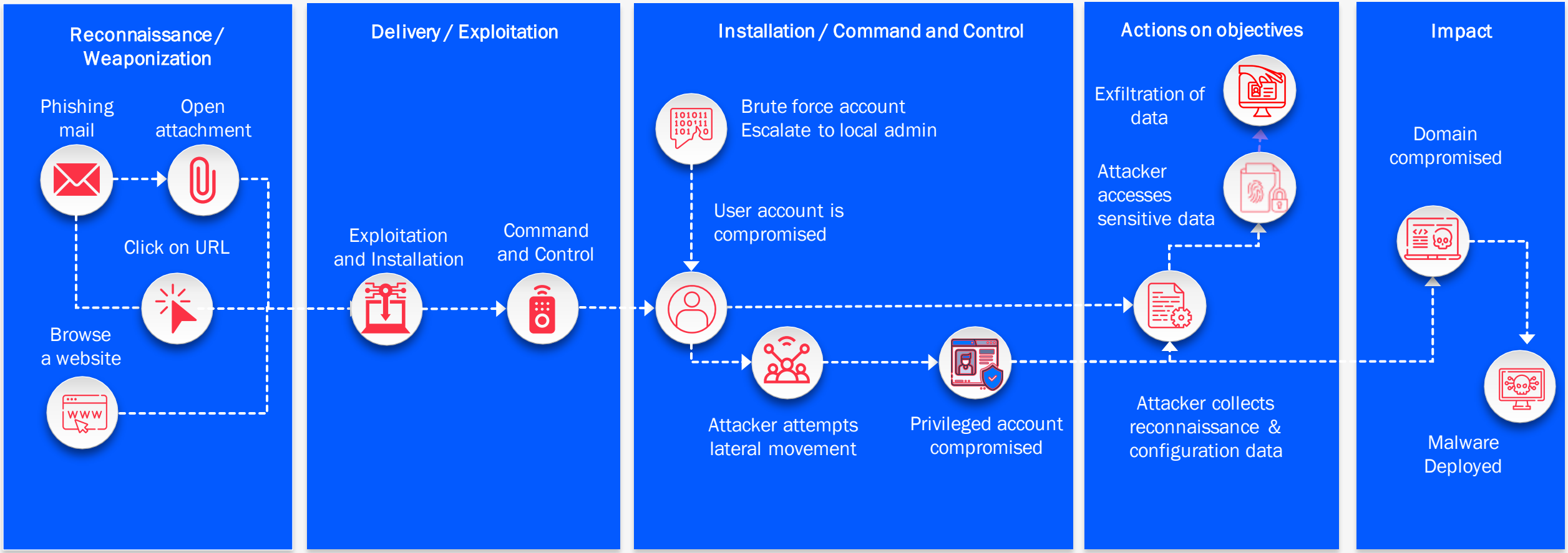
Doelen behalen

- In deze laatste fase bereiken cybercriminelen hun specifieke doelen. Hierbij kan het gaan om diefstal van gevoelige gegevens, verstoring van de dienstverlening, het eisen van losgeld of andere kwaadaardige activiteiten die aansluiten bij de doelstellingen van de aanvaller.

Actions on Objectives (Doelen behalen)

Voorbeeld: Ransomware Attack

Hoe een hacker binnenkomt op een systeem

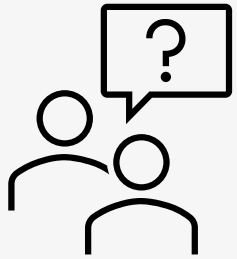


Je bent alsnog gehackt.... Wat nu?

Praktijkvoorbeeld

Wat gebeurde er?

Februari 2022



De IT-afdeling krijgt de eerste meldingen binnen van medewerkers **die melden** dat bepaalde applicaties niet functioneren.

Wat gebeurde er?

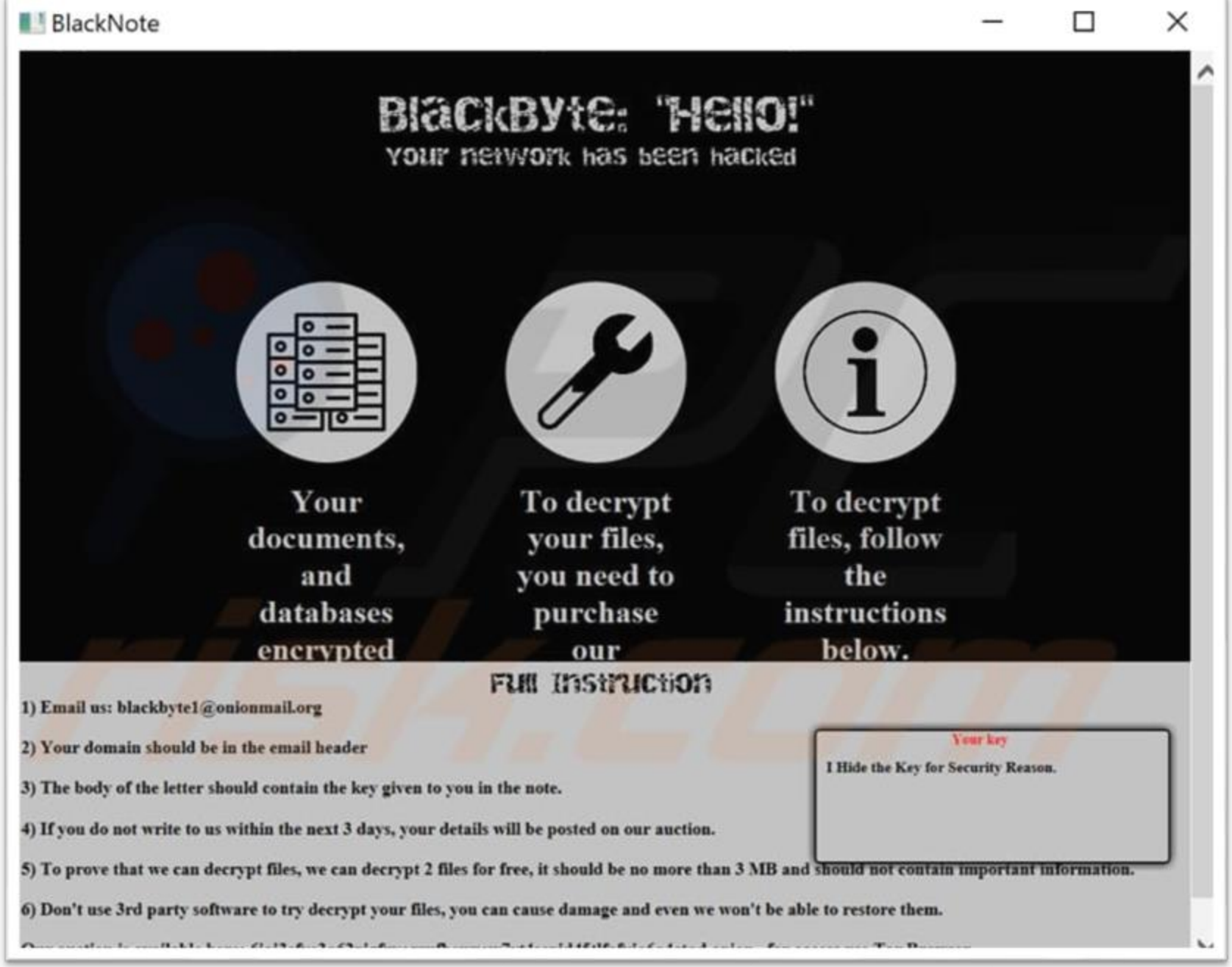
Februari 2022

Al snel constateert de IT-afdeling dat ze getroffen zijn door een ransomware aanval.

Wat gebeurde er?

Februari 2022

Ook verschijnen deze meldingen op werkplekken.


BlackNote
BlackByte: "Hello!"
Your network has been hacked
Your documents, and databases encrypted
To decrypt your files, you need to purchase our
To decrypt files, follow the instructions below.
Full Instruction
1) Email us: blackbyte1@onionmail.org
2) Your domain should be in the email header
3) The body of the letter should contain the key given to you in the note.
4) If you do not write to us within the next 3 days, your details will be posted on our auction.
5) To prove that we can decrypt files, we can decrypt 2 files for free, it should be no more than 3 MB and should not contain important information.
6) Don't use 3rd party software to try decrypt your files, you can cause damage and even we won't be able to restore them.
Your key
I Hide the Key for Security Reason.

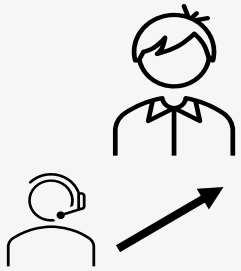
Wat gebeurde er?

Februari 2022

IT-afdeling neemt contact op met Ekco (stand-by).

Wat gebeurde er?

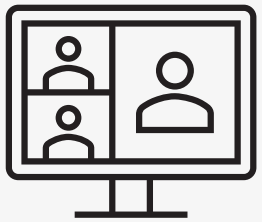
Februari 2022



Escalatie naar Incident Manager.

Wat gebeurde er?

Februari 2022



Conference call met IT afdeling en Ekco.

Vraag klant: “Ik denk dat we backups moeten terugzetten???”…

Wat gebeurde er?

Februari 2022

Op basis van de feiten die tot dan **bekend** waren… advies Ekco.

“ZET ALLE SYSTEMEN UIT”

“Klant beschikt niet over een Cybersecurity verzekering”

“Toch advies: Schakel een Cybersecurity Forensisch Expert in”

“Wacht op acties en advies van Cybersecurity Forensisch Expert”

Wat gebeurde er?

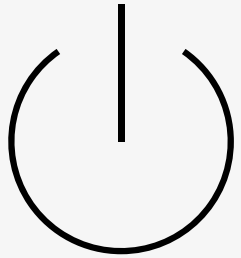
Februari 2022

Ondertussen treft Ekco al voorbereidingen.

“Hardware wordt geregeld voor een eventuele restore”

Hoe nu verder?

De tijd tikt door.....



Alles staat nog steeds uit. Ook geen internet toegang.

“Kritieke meetings werden gedaan via telefoon of mobiele hotspot”

“Ondanks mobiele hotspot werd toch nog tijdens een meeting en laptop gelocked”

Hoe nu verder?

De tijd tikt door.....

Er is inmiddels contact geweest met een Cybersecurity Forensisch Expert.

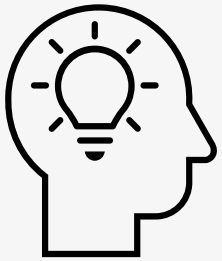
“Zij hebben de casus aangenomen”

“Een offerte / opdrachtbevestiging wordt gemaakt”

“Ondertussen wordt in de planning gekeken wanneer het onderzoek gestart kan worden. (Gelukkig de dag daarna)”

Hoe nu verder?

De tijd tikt door.....

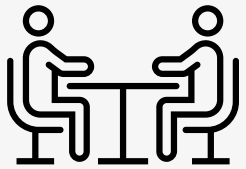


Er dient een analyse gedaan te worden op de besmette omgeving.

“Een kopie van de servers wordt naar de tijdelijke hardware geplaatst”

Ondertussen

Onderhandeling

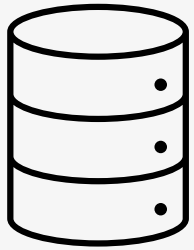


De Cybersecurity Forensisch Expert houdt nauw contact met de hackergroep.

“Om tijd te winnen wordt er onderhandeld over het losgeld”

Analyse

De tijd tikt door....

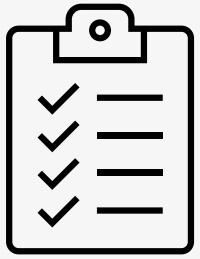


BACKUP! Eindelijk een lichtpuntje. De backup van de backup is niet geraakt.

“Doordat de backup immutable was, is de backup van de backup nog beschikbaar”

Plan maken

Tijd voor een Disaster Recovery Plan



Er was geen Disaster Recovery Plan. Deze werd samen met Ekco gemaakt.

“Welke applicaties zijn het meest belangrijk?”

“Welke servers moeten in welke volgorde opstarten?”

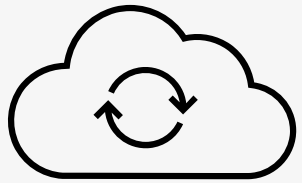
“Welke data meest belangrijk?”

“Wie kan wat testen?”

“Hoe weten we zeker dat we niet meer besmet zijn?”

Het herstel

Ook dit kost veel tijd



Nu kunnen de servers vanuit de backup hersteld worden....

“Het team test de IT omgeving”

“Het team test de applicaties”

De forensische experts blijven meekijken en houden alles nauwlettend in de gaten.

“Wie kan wat testen?”

“Hoe weten we zeker dat we niet meer besmet zijn?”

Het resultaat

Twee weken verder...

Na uitgebreide testen en onderzoek is de IT-omgeving hersteld en “schoon”.

Geen losgeld betaald aan de hackersgroep.

Tussen de €300.000,- en €400.000 schade (out of pocket). Derving en reputatieschade niet meegeteld.

Productie draait weer.

Kantoorautomatisering is hersteld.

Er is nog veel nazorg voor de organisatie. Denk aan facturatieprocessen, handmatige processen en communicatie met klanten en leveranciers.

Immutable BACKUP 🙏

Je bent alsnog gehackt.... Wat nu?

Wat was nu uiteindelijk de oorzaak?

De oorzaak

Een “on-premises” mailserver was niet up-to-date	Fase 1: Verkenning	
De hackers hebben een exploit voor de vulnerability	Fase 2: Weaponization	
De hackers krijgen toegang tot de mailserver en van daaruit tot meerdere systemen in de organisatie	Fase 3: Delivery	
Via Domain Admin rechten toegang tot AD en een GPO geïmplementeerd	Fase 3: Delivery	
Via deze GPO wordt de malware encryptie software over de hele organisatie gedistribueerd	Fase 4: Exploitation	
De aanval is gestart. Bestanden worden versleuteld	Fase 5: Installation	
De hackers hadden ook nog “achterdeurtjes” om de machines via Remote Control over te nemen	Fase 6: Command and Control	
Uit forensisch onderzoek bleek dat de hackers alle servers en werkplekken in controle hadden	Fase 6: Command and Control	
Nadat de aanval uit fase 4 in volle gang is, eisen de hackers “losgeld” via diverse schermen op de werkplekken.	Fase 7: Actions on Objectives	

Je bent alsnog gehackt.... Wat nu?

Wat kun je er nu al aan doen?

Kill Cyber Kill Chain

Stappen die jouw organisatie kan zetten om de “Kill chain” te verstoren

Reconnaissance (Verkenning)

- ✓ Let op je aanwezigheid op sociale media
- ✓ Wees geen doelwit
- ✓ Gebruik verschillende wachtwoorden
- ✓ Check “haveibeenpwned.com”

Weaponization (Bewapening voorbereiden)

- ✓ Men creëert wapen. Er kan geen actie worden ondernomen.

Delivery (Uitbouw)

- ✓ Antivirus
- ✓ E-mail en webfiltering
- ✓ Educatie
- ✓ Gebruikers awareness
- ✓ Limiteer gebruik van USB
- ✓ Blokkeer autorun

Exploitation (uitvoering van de aanval)

- ✓ Patchen en updates
- ✓ Vulnerability scanning
- ✓ Beveilig websites en webapplicaties

Installation (Permanent aanwezig zijn)

- ✓ Antivirus
- ✓ Goed beheer over admin credentials
- ✓ Multifactor Authenticatie
- ✓ Whitelist tools voor software

Command and Control (Data Exfiltration)

- ✓ Firewalls
- ✓ Intrusion Protection Systemen
- ✓ Proxy filters

Actions on Objectives (Doelen behalen)

- ✓ Beveiligde backups
- ✓ Disaster Recovery Plan
- ✓ Cybersecurity verzekering

Je bent alsnog gehackt.... Wat nu?

Samenvattend

Samenvattend

- Assume Breach and take measures.
- Mocht je wel in het bezit zijn van een Cybersecurity verzekering. Let dan goed op het volgende:
  - Polisvoorwaarden worden jaarlijks aangescherpt
- Herdefinieer de huidige IT infrastructuur voor security maatregelen. (Bijv. Backup)
  - Backup is niet meer alleen voor bestandsherstel, wet- en regelgeving, juridisch
  - Backup is nog belangrijker geworden in het geval van een “Cyberaanval”
- Is er een patchbeleid en systeem (niet alleen van je servers)?
- Is er een incident response plan (weet iedereen wat er moet gebeuren)?
- Zet de risico’s centraal en stel een incident response team samen.
- Is er een Disaster Recovery plan?
- Tijd is van essentieel belang tijdens een cyberincident.
- Specificeer de meeste kritische processen en assets.
- Detect and Respond.
- Betrek specialisten.

Integrated Baseline voor Information security (IBI) als paraplu voor security improvements

Een transparante aanpak die leidt tot continue verbeteringen

Integrated
Baseline for
Information security

IDENTIFY PROTECT

IBI Essentials

- Security best practices voor de Microsoft 365 tenant

IDENTIFY PROTECT

IBI Securepacks

- Configuration best practices
- Vulnerability scanning
- Security recommendations voor servers & werkplekken

IDENTIFY PROTECT

IBI Platform

- Security best practices & security recommendations Voor Azure platform

IDENTIFY PROTECT

IBI Governance

- Beleid, procedures
- Incident response plan
- Business continuity plan
- Warroom simulatie
- Security Awareness

IDENTIFY PROTECT

IBI kwetsbaarheden

- Dagelijkse controle op acute dreigingen
- Maandelijkse bespreking van de gevonden kwetsbaarheden

DETECT RESPOND

Managed Extended Detection and Response (XDR) & Managed Endpoint Detection and Response (EDR)

- 24x7 Analytics, SOAR
- Alert monitoring & triage
- Incident Response
- Custom Analytics rule

Recover

Recovery

- Herstellen van beveiligings-incidenten

Security Awareness

Vergroot bewustzijn van gebruikers

Baseline testen

We bieden baseline-tests om het phish-gevoelige percentage van jouw gebruikers te beoordelen via een gesimuleerde phishing-, vishing- of smishing-aanval.

Train jouw gebruikers

's Werelds grootste bibliotheek met trainingsinhoud over beveiligingsbewustzijn: inclusief interactieve modules, video's, games, posters en nieuwsbrieven. Geautomatiseerde trainingscampagnes met geplande herinneringsmails.

Phish jouw gebruikers

Best-in-class, volledig geautomatiseerde gesimuleerde phishing, vishing- en smishing-aanvallen, honderden sjablonen met onbeperkt gebruik en phishing-sjablonen voor de gemeenschap.

PHISHED

Bekijk de resultaten

Rapportage op bedrijfsniveau. Zowel high-level als granulaire statistieken en grafieken klaar voor managementrapportages. We hebben zelfs een persoonlijke tijdlijn voor elke gebruiker.

Managed eXtended Detection & Response (XDR)

Wat zit er in deze 24x7 security dienst

Multilaag proactieve dreigingsanalyse en response

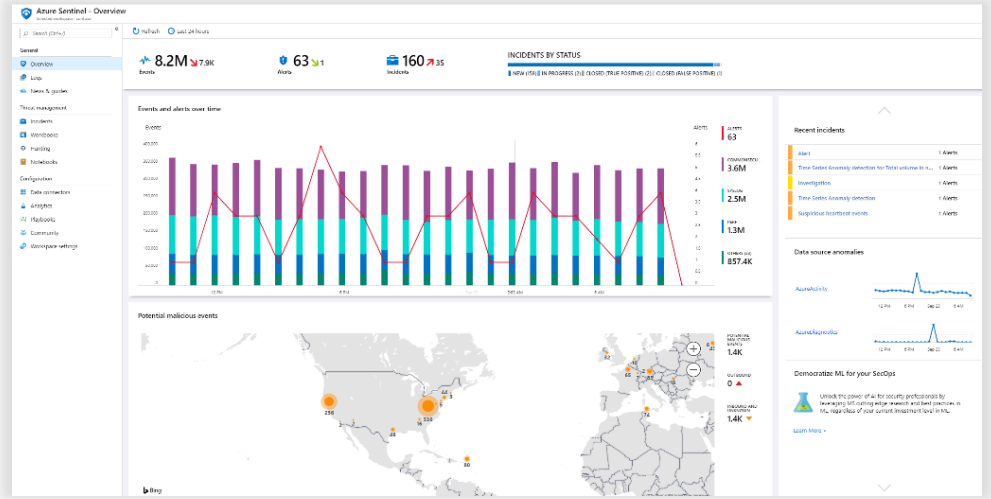
- Voor de gehele infrastructuur : van M365, Azure workloads, on-premises workloads, werkplekken en netwerk
- Versnelt detectie en optimaliseert onderzoek- en reactietijd

Managed security & Incident management (SIEM)

- 24/7 dienst voor bedreigingsmonitoring
- Inzet van de modernste technologie, door automatisering en AI worden risico's ontdekt, aangevuld door de expertise van een team van ervaren beveiligingsanalisten
- Het starten van het incident response proces is inbegrepen. De werkzaamheden voor het beperken, wegnemen of herstellen van een dreiging zijn geen onderdeel van de maandprijs, maar worden apart in rekening gebracht. In combinatie met een cyberverzekering is dit meestal kosteloos voor jouw organisatie

24x7 toezicht vanuit het Security Operating Center (SOC)

- Always-on SOC maakt gebruik van een 24x7 team van Ekco cybersecurity-experts die zorgen voor monitoring, analyse en herstel
- Dienst met inzet van Azure Sentinel (kosten Sentinel niet inbegrepen) en Microsoft Defender componenten

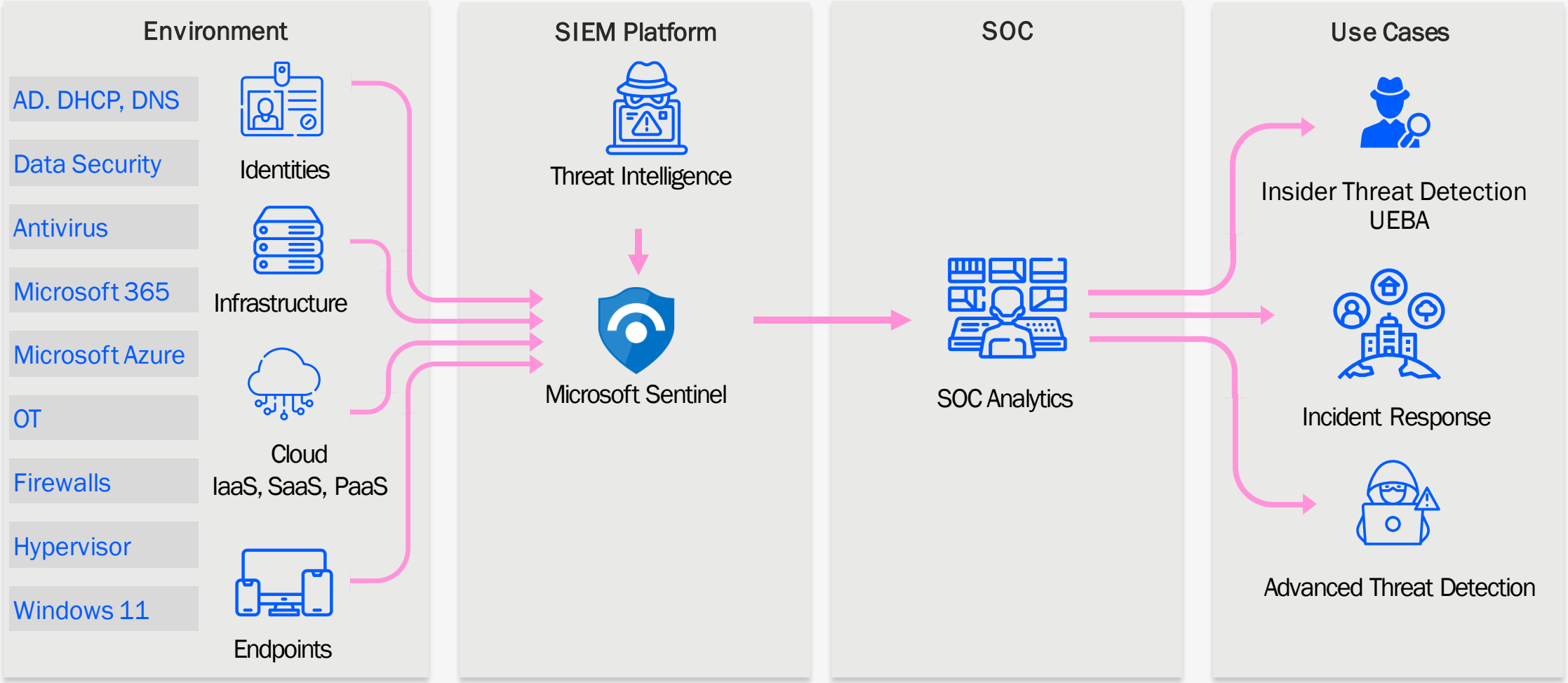


Business Continuity: incident response plan is cruciaal

- Het hebben en up-to-date houden van zowel een incident response plan als een Business Continuity plan is cruciaal om de voordelen van deze dienst te ervaren.
- Het opstellen is geen onderdeel van dienst, Ekco kan uiteraard ondersteuning bieden bij het opstellen van een dergelijk plan. Daarnaast adviseren wij om het plan regelmatig te testen en up-to-date te houden. Het periodiek uitvoeren van een zogenaamde warroom sessie kan hierbij helpen.

eXtended Detect and Respond aanpak

Hoe gaat XDR precies in zijn werk?



Managed XDR 3 varianten

Beschrijving	Frontline	Essentials	Comfort
24x7 Security Operations Center (SOC) • Beoordeling en analyse van logbronnen • Beoordeling van beschikbare dreigingsinformatie • Identificatie, verificatie, communicatie/escalatie van significante waarschuwingen en incidenten. • Het verstrekken van aanvullende informatie bij significante waarschuwingen en incidenten • Identificatie, analyse en gebruik van Microsoft Sentinel/XDR-rapporten	✓	✓	✓
Beheer en optimalisatie van het Microsoft Sentinel Platform	✓	✓	✓
Threat Intelligence	✓	✓	✓
Threat Hunting	✓	✓	✓
Bijhouden en bewaken van de omgeving via Ekco Analytics Best practices	✓	✓	✓
Creëren en bewaken van custom analytic rules	✓	✓	✓
Creëren en bewaken van Custom Playbooks en Dashboards		✓	✓
Geautomatiseerde acties op veel voorkomende dreigingen		✓	✓
Optimaliseren van log sources			✓
Beveiligingsbronnen			
Azure Activity Logs	✓	✓	✓
Microsoft Entra ID Protection	✓	✓	✓
Office 365 Activity (inclusief Teams)	✓	✓	✓
Microsoft Defender for Identity [1]	✓	✓	✓
Microsoft Defender for Endpoint voor werkstations[5]		✓	✓
Microsoft Defender for Endpoint voor servers[5]		✓	✓
Microsoft Defender for IOT[1]		✓	✓
Microsoft Defender for Cloud Apps[1]		✓	✓
Microsoft Defender for Vulnerability Management[1]		✓	✓
Microsoft Data Loss Prevention[1]		✓	✓
Microsoft App Governance[1]		✓	✓
Microsoft Defender for Containers[1]			✓
Microsoft Defender for Databases[1]			✓
Microsoft Defender for Storage[1]			✓
Microsoft Defender for API's[1]			✓
Microsoft Defender for App Service[1]			✓
Microsoft Defender for Key Vault[1]			✓
Microsoft Defender for Resource Manager[1]			✓
Firewalls[2, 4]			✓
Extra third party sources[3, 4]			✓

EKCO

Vragen?

Bedankt