Hackersperspectief op informatiebeveiliging

Scholingsdag Prisma-RT

Ir. Julius Duijts CISSP CEH CIPP/E, Partner Informatiebeveiliging
Classificatie: Intern gebruik

Presentatie| 30 oktober 2025

Partners in verbetering

Julius Duijts

ISO 27001 Lead Auditor

Adviseur
- Organisatie, processen en verandering
- Verbinden van de 'softe' en de 'harde' kant
- Expert Privacy en Informatiebeveiliging BIO, ISO27001, NEN7510, Avg, Wpg
- Governance, Risk & Compliance

Verander-/Programmamanager
- verbinding van verschillende disciplines, zoals Zorg, HR, Finance, IT

Trainer/coach (NLP, TA)
- Privacy/Informatiebeveiliging
- Netwerkregie, Waardebewust veranderen
- Trainingsontwikkeling

Vrije tijd
- Koken, Zeilen/-instructie, Koorzang

✉ Julius.Duijts@bmc.nl ✆ 06-2952 5531

NCTV: Turbulente tijden, onvoorziene effecten

Grote en diverse digitale dreiging

- Cyberaanvallen komen vooral van statelijke en criminele actoren.
- Statelijke actoren breiden hun capaciteiten uit en gebruiken een bredere gereedschapskist.
- Criminele actoren handelen opportunistisch en voeren grootschalige aanvallen uit.
- Grootschalige uitval van digitale processen vormt een serieuze dreiging.

Digitale risico's staan niet op zichzelf, maar worden beïnvloed door vele verschillende factoren

- Digitale risico's vragen om een brede manier van beheersing.
- Digitale risico's zijn dynamisch en beïnvloed door diverse factoren.
- Het digitale ecosysteem, monoculturen en hoge digitalisering vergroten onderlinge verbondenheid van risico's.

Digitale veiligheid als nationaal belang

- Veiligheid van digitale processen is cruciaal voor de maatschappij.
- De veiligheid van digitale processen is en blijft essentieel in onze maatschappij en is dus onlosmakelijk verbonden met de nationale veiligheid.
- Digitale veiligheid moet concurreren met andere nationale belangen.

Bron: Cybersecuritybeeld Nederland CSBN, NCTV, 2024

Context van de NIS2-Richtlijn en de CER-richtlijn

- Hogere dreiging en grotere kwetsbaarheid
  - digitalisering in organisaties en de maatschappij
  - uitbreiding van het cyberdreigingslandschap
  - verschillen per land leiden tot versnippering met nadelen mbt effectiviteit en de interne markt
- NIS2-Richtlijn
  - vervangt NIS richtlijn (EU 2016/1148), die in Nederland is geïmplementeerd in de Wet beveiliging netwerk- en Informatiesystemen (WBNI) e.a.
  - wordt omzet in de Nederlandse Cyberbeveiligingswet
- CER-Richtlijn
  - wordt omzet in de Nederlandse Wet Weerbaarheid Kritieke Entiteiten
  - is onder andere van toepassing op zorginstellingen

Op wie is de Cyberbeveiligingswet van toepassing?

- De Wet weerbaarheid kritieke entiteiten op basis van de CER-richtlijn
  - **Kritieke entiteiten**
    - **Zorgaanbieders** indien aangewezen door de minister (Art 7 lid 1 Wwke)
      - https://www.datavoorgezondheid.nl/documenten/2025/04/01/beslisboom-cyberbeveilingswet
      - Bevoegde autoriteit voor zorgorganisaties is de Minister van VWS (Art 8 lid 1 Wwke)

- De Cyberbeveiligingswet op basis van de NIS2 richtlijn
  - **Essentiële entiteiten**
    - **Kritieke entiteiten** (Art 8 lid 1 onder i Cbw)
    - **Ministeries, ZBO, provincies, gemeenten, waterschappen en GR** (Art 8 lid 2 onder g en h Cbw)
      - Bevoegde autoriteit voor de overheid is de Minister van BZK (Art 16 lid 1 Cbw)

NB in het kader van keten-/leveranciersmanagement zullen ook dienstverleners aan kritieke/essentiële entiteiten te maken krijgen met aanvullende eisen van hun klanten

BMC

Impact Cyberbeveiligingswet voor zorginstellingen

- Governance
  - Verantwoordelijkheid en opleidingsverplichting voor bestuurders
- Zorgplicht
  - In lijn met NEN 7510 voor informatiebeveiliging
  - Bedrijfscontinuïteit
- Meldplicht
  - Significante incidenten
- Toezicht
  - door de IGJ

NB NEN 7510 is een bestaande wettelijke verplichting

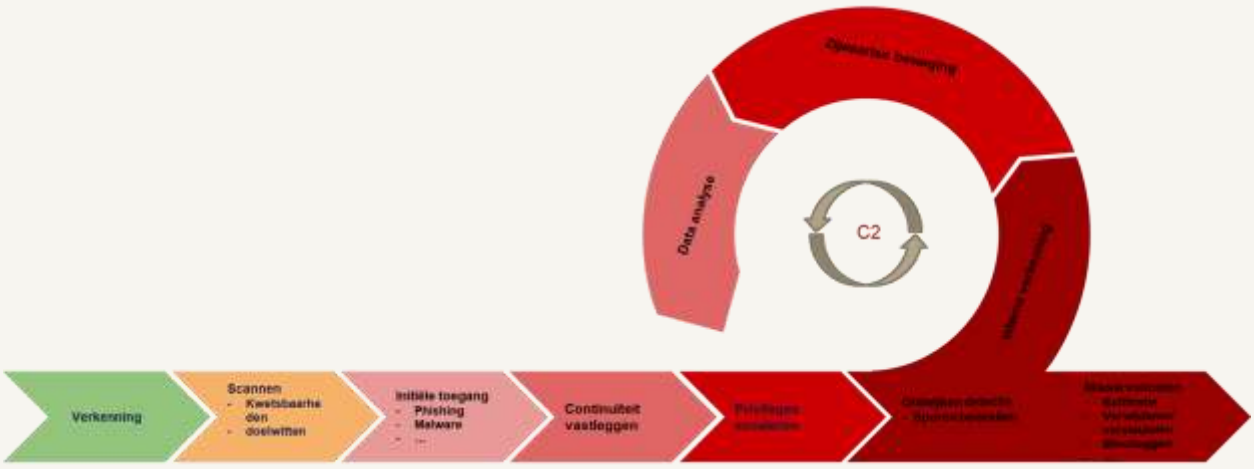
BMC

Hackers heb je in soorten en maten

- Black Hat - de kwaadaardige hacker
  - Crimineel - uit op geldelijk gewin
  - Statelijk
    - uit op geldelijk gewin
    - ondermijning van de samenleving
    - informatiepositie
  - Hybride: crimineel, maar getolereerd/gesponsord door de staat
    - ook: Industriële spionage
- White Hat - de ethische hacker
  - in opdracht (penetratietest, Red Team)
  - op eigen initiatief - responsible/coordinated disclosure

BMC

Hoe hackers te werk gaan: de Cyber kill-chain



BMC

Verkenning

- Over de organisatie en personen
  - via website, LinkedIn, KvK, Darkweb, google, AI
  - levert op: namen, mailadressen (phishing), rollen (zich uitgeven als)
- Technisch
  - Website (zichtbare softwareversies, links naar andere sites (leveranciers)
  - DNS (internet telefoonboek, laat zien welke (web)sites de organisatie heeft
  - Openbare scanners (open poorten, softwareversies, algemeen beeld van beveiliging (basisbeveiling.nl))
- Wat kun je doen?
  - Terughoudend met informatie op de website
  - Weet wat zichtbaar is: Zelf scannen en evt. aanpassen

Scanning

- Passief - zonder contact met het target
  - via openbare scanners (zie ook verkenning)
  - Shodan.io, Censys.io
- Reflectief
  - via websites die een scandienst aanbieden
  - Bijvoorbeeld: https://www.ipfingerprints.com/portscan.php
- Actief
  - Zelf scannen met hackerstools
- Wat kun je doen?
  - Zelf scannen en evt. corrigeren

Shodan.io

Een leeuw kiest de zwakste gazelle als prooi

Ook een hacker kiest het zwakste slachtoffer
op basis van een kosten/baten afweging

De informatie daarvoor komt uit de verkenning:

- Wat kan het mij opleveren?
  - Financieel op basis van een jaarverslag
  - Informatie op basis van de bedrijfsactiviteiten (ook gezondheidsinformatie is waardevol)
  - Informatie over de klanten (toegang via de leverancier)
- Hoe veel moeite gaat het kosten?
  - Zijn er (veel) mailadressen en/of gelekte wachtwoorden op het darkweb?
  - Is men slordig met onderhoud/configuratie van websites? actuele softwareversies, sterke configuratie/versleuteling
  - Is er informatie over kwetsbaarheden?
  - Informatie over (kwetsbare) leveranciers?

BMC

Initiële toegang

- Menselijke kwetsbaarheden - Social Engineering
  - Social engineering speelt in op urgentie, autoriteit, vertrouwen en waarden van het slachtoffer, bijv Phishing
  - Mensen verleiden iets te doen: inloggen, wachtwoorden invullen, bijlage of link openen (malware)
- Technische kwetsbaarheden
  - Kwetsbaarheden in (oude) software, Configuratiefouten, Malware, Wachtwoorden raden (standaard wachtwoorden)
  - ook de 2e fase na social engineering (malware)
- Toegang via een leverancier (Supply-chain)
- Wat kun je doen?
  - Afspraken: "ik vraag je nooit per mail om geld over te maken"
  - Bewustwording en training bij medewerkers
  - Veilige configuraties (conform security baselines)
  - Actuele softwareversies "Patching" (als dat niet kan: hek er om)
    voorwaarde: weten wat je hebt (Asset/Configuration mgt.)
  - Zorg dat software(versies) niet zichtbaar zijn van buiten
  - Leveranciersmonitoring (ook: ISO27001/NEN7510)

BMC

Vervolgstappen na initiële toegang

Van eerste toegang tot bereiken van het doel
- Ransomware-aanval (afpersing)
- Stelen van informatie
- Verstoren van de bedrijfsvoering
- ….

BMC

Vervolgstappen na initiële toegang

Wat kun je doen?
- Gevoelige gegevens afschermen en minimaliseren
- Security Monitoring (SOC/SIEM, MDR)
  - Uitvoeren van bepaalde programma's
  - Toewijzing van bijzondere rechten
  - Aanpassen/verwijderen logfiles
  - Netwerkverkenning
  - Detectie van data extractie/versleuteling
- Incident response/Forensisch onderzoek
  - "Waakvlam" contract
- Bedrijfscontinuïteitsplan

BMC

Gelaagde verdediging, ook digitaal

- Meerdere lagen,
  die elk alleen ook voldoende zouden zijn
  - voorbeeld: twee-factor authenticatie
- Gecontroleerde toegang (choke points)
- Compartimentering/Isolatie

BMC

Onderwerpen in een Bedrijfscontinuïteitsplan (BCP)

Het BCP bevat:

1. Organisatie: Rollen en governance, o.a. leden van het BedrijfsContinuïteitsTeam (BCT) incl. uitwijklocatie BCT
2. Proces:
   a. Activeren (wie mag dat doen?)
   b. Noodscenario/Uitwijk
   c. Herstel reguliere bedrijfsvoering
   d. Evaluatie
3. Test en onderhoud van het BCP
4. Uitwerking per kritiek proces:
   a. Noodscenario's
   b. Randvoorwaarden/voorbereiding

BMC

Aanpak Bedrijfscontinuïteit

Eenmalig	Inhoud	Periodiek
Business Impact Analyse (BIA)	Per proces: - Impact - Benodigde middelen - Verkenning noodscenario's	Actualiseren
Business continuity plan (BCP)	- Crisisorganisatie - Procedures - Globale noodscenario's per proces	Testen, evalueren, actualiseren
Draaiboeken (als globale beschrijving onvoldoende is)	Bijvoorbeeld (naar keuze) - Brand - Overstroming - Uitwijk burgerzaken - Epidemie - ICT uitwijk - Malwareinfectie - Ransomware - …	Testen, evalueren, actualiseren

BMC

Databankweg 26D
3821 AL Amersfoort

Postbus 490
3800 AL Amersfoort

(033) 496 52 00
info@bmc.nl

KvK BMC Advies 32078667
IBAN NL91ABNA0504035754
BTW NL80.86.63.598 B.01

Kijk voor meer info op onze website: bmc.nl