CYBERVEILIG NEDERLAND

Ransomware aanvallen anno 2023

De grootste (digitale) dreiging voor de zorg

FME


Tubantia

REGIO ALGEMEEN SPORT VIDEO PODCAST OPINIE FU

Regio wijzigen Enschede e.o. Hengelo e.o. Almelo e.o. Oldenzaal e.o. Reggestreek

▲ Liesbeth Holterman, manager van de cybersecurity hub van Novel-T. © Frans Nikkels Fotografie

Treurig gesteld met cyberveiligheid in Twentse maakindustrie

ENSCHEDE - Vrijwel geen van de veertig Twentse maakbedrijven die meededen aan een vrijwillige check, heeft de cybersecurity op orde. Af en

Novel T

NEDERLAND ICT
VOOR DE DIGITALE ECONOMIE

Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

deVolkskrant

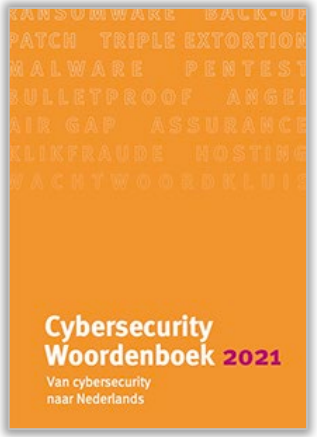
Volgens Liesbeth Holterman van Cyberveilig Nederland, een brancheorganisatie van cybersecuritybedrijven en betrokken bij het initiatief, zijn bedrijven de afgelopen maanden slachtoffer geworden van een cyberaanval die voorkomen had kunnen worden als bekend was dat hun IP-adres of andere indicator was gecompromitteerd. Holterman: 'Het NCSC deelt nu vanuit de wettelijke taak alleen risico en dreigingsinformatie met bedrijven die tot de doelgroep horen, daar gaat het mis.'

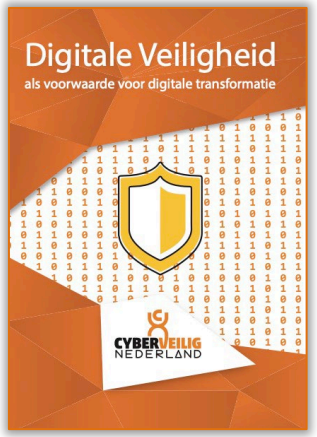
Het platleggen van transportbedrijf Bakker Logistiek, waardoor er geen kaas in winkels van Albert Heijn lag, was bijvoorbeeld het gevolg van een kwetsbaarheid in Microsoft Exchange die al langer bekend was.

CYBERVEILIG NEDERLAND

Den Haag

Cyberveilig NL is dé belangenorganisatie voor een optimaal ondernemingsklimaat voor cybersecurity bedrijven in NL



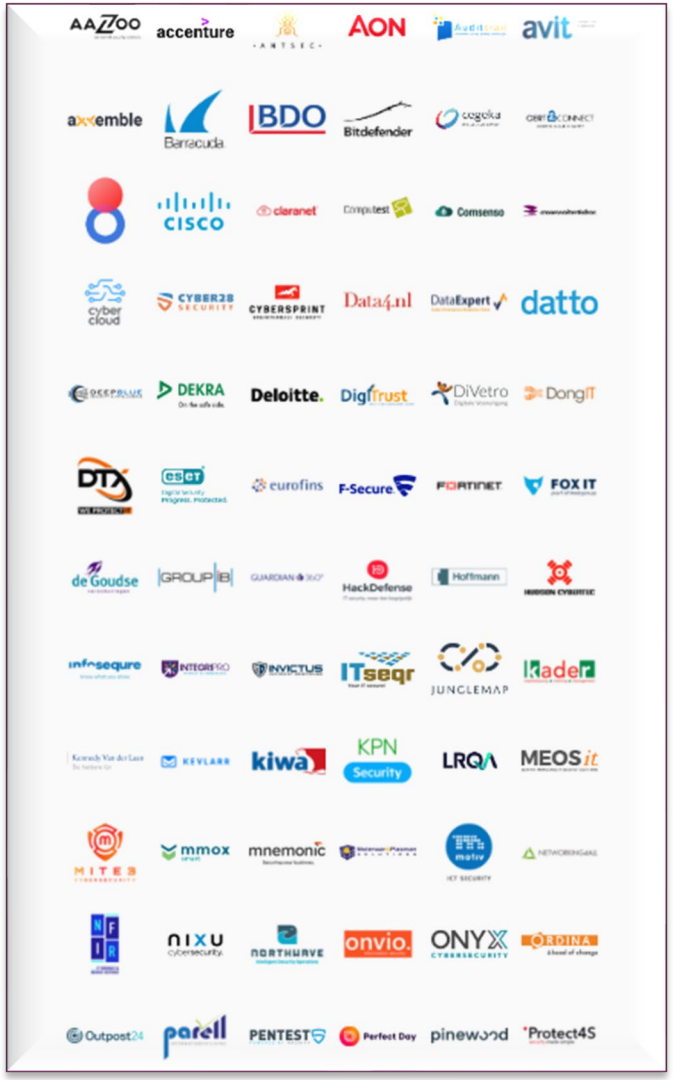


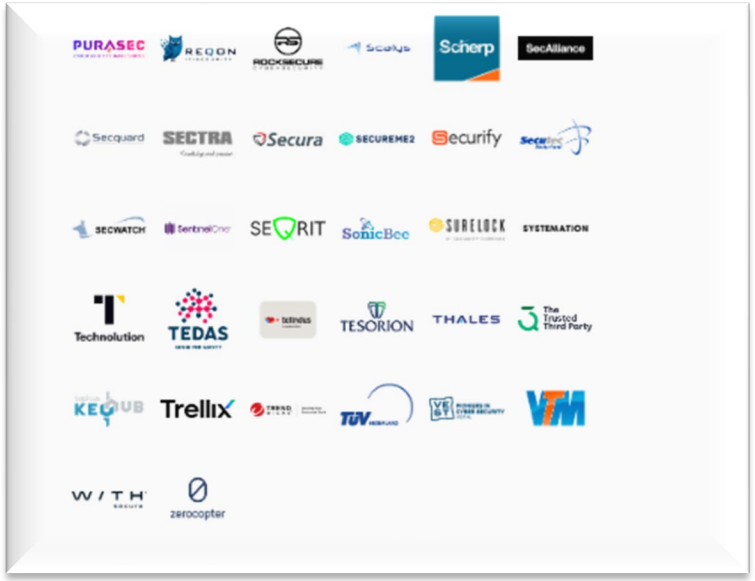
Cyberveilig NL is OKTT-organisatie[1] waardoor we informatie kunnen delen met het NCSC

[1] OKTT = Organisaties die Kenbaar Tot Taak hebben informatie te delen

We hebben een brede achterban van cybersecurity dienstverleners

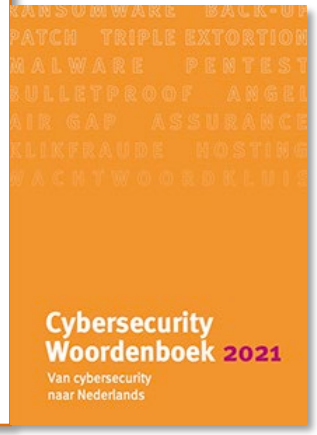
100+



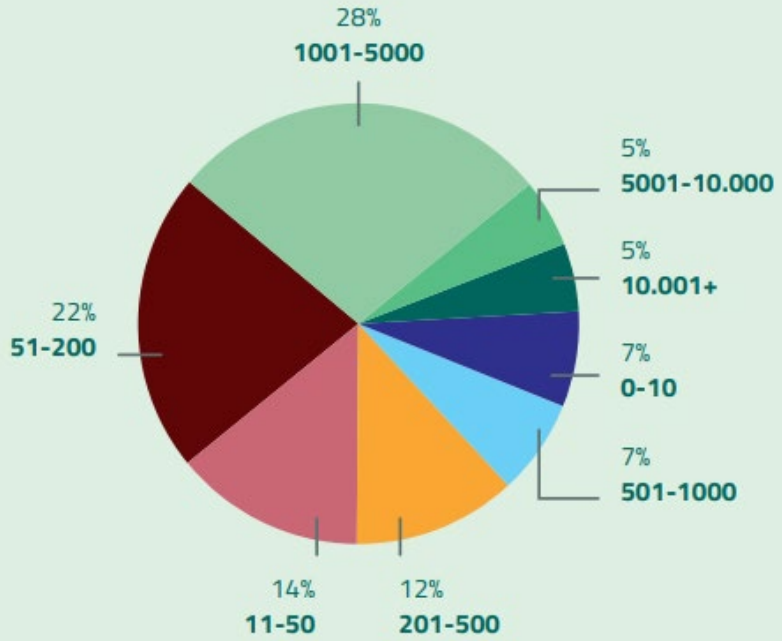


Ransomware = ransom + software

Ransomware	...	*Gijzelsoftware*
Gijzelsoftware	Kwaadaardige software waarbij een slachtoffer afgeperst wordt, nadat zijn digitale systeem of de bestanden erop met een code op slot zijn gezet. De aanvaller biedt de code tegen betaling aan, zodat hij er weer bij kan. Maar zelfs dat is niet zeker.	

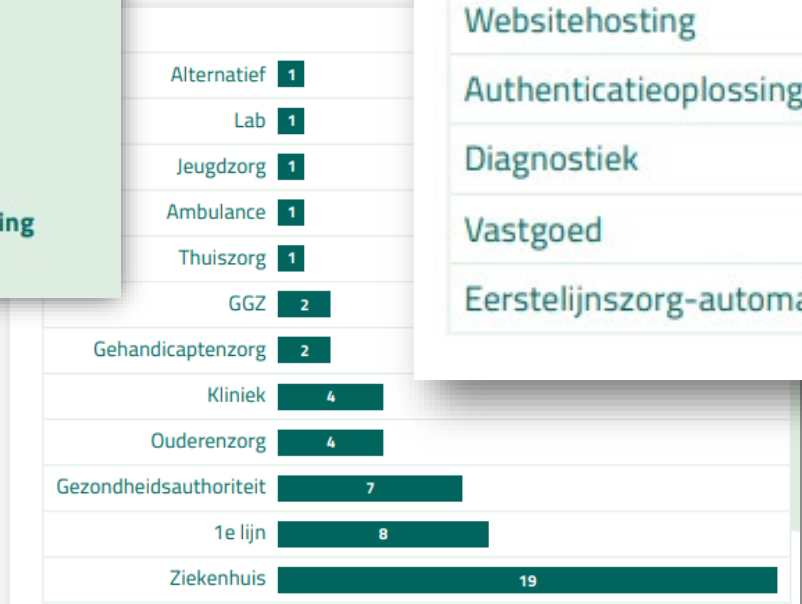


https://www.z-cert.nl/wp-content/uploads/2023/03/Z-CERT_RapportDreigingsbeeld2022.pdf



Figuur 2

Percentage ransomware-incidenten per grootte van de zorginstelling
(hoeveelheid personeel)



Figuur 1

Hoeveelheid ransomware-incidenten in Europese zorgsector in 2022

Impact op Nederlandse zorginstellingen door ransomware-aanvallen op leveranciers van zorginstellingen in 2022

Product/dienst geraakte bedrijf	Impact zorginstelling
Apothekerssoftware	Uitstel onderhoud
Crediteuren/facturatie	Enkele dagen niet factureren
Websitehosting	Website enkele uren niet online
Authenticatieoplossing	Datalek
Diagnostiek	Uitstel onderhoud
Vastgoed	Datalek
Eerstelijnszorg-automatisering	Bedrijf niet bereikbaar

Hackers delen naaktfoto's borstkankerpatiënten om ziekenhuis te chanteren

Cybercriminelen hebben gestolen foto's van borstkankerpatiënten van een Amerikaans zorginstituut online geplaatst, de beelden tonen volgens RTL Nieuws de patiënten en hun ontblote borsten voor de operatie. De hackers dreigen ermee nog meer privégegevens en beelden te publiceren als het zorginstituut niet het geëiste losgeld betaalt.

MGDS 07-03-23, 12:00 **Laatste update:** 07-03-23, 12:04

Vrouw sterft tijdens ransomware-aanval op ziekenhuis Düsseldorf

18 september 2020 13:39 • Aangepast 18 september 2020 13:39

Net binnen

14:27 Oosting neemt ... Duits mee naar ...

14:12 Oproep Consun... consument moe... gebruik AI'

13:53 Dochters Russel... beschuldigen h...

13:23 Linda de Mol 'st... op een man

13:21 EU-landen stem... natuurherstelwe...

Meer n...

Door een ransomware-aanval op het universiteitsziekenhuis in Düsseldorf is een vrouw overleden.

Het is mogelijk het eerste sterfgeval dat direct is gelinkt aan een cyberaanval op een ziekenhuis. Door de ransomware-aanval kon het ziekenhuis geen nieuwe patiënten aannemen op de spoedeisende hulp, melden Duitse media.

Iers nationaal zorgsysteem sluit registratiesysteem af na 'ransomware-aanval'

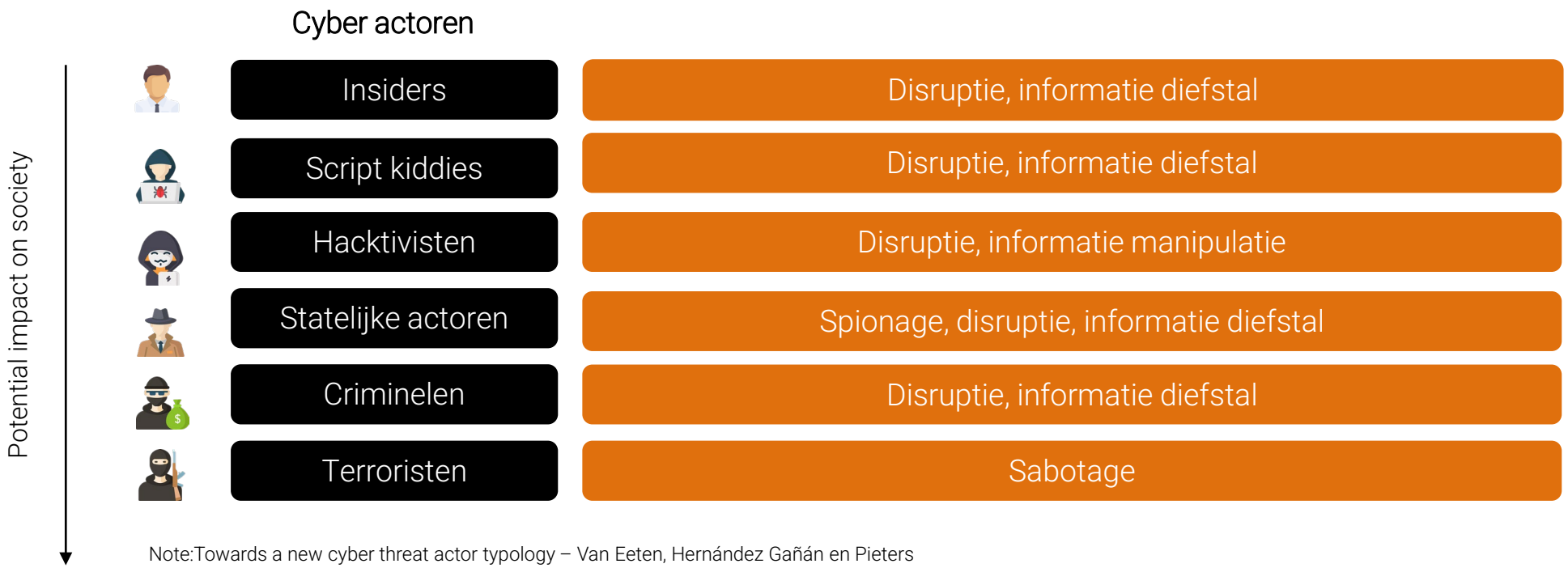
Het Ierse zorgsysteem Health Service Executive is getroffen door wat de dienst een ransomware-aanval noemt. Volgens de HSE gaat het om een gerichte aanval 'die door mensen wordt gestuurd' en zijn de aanvallers uit op het stelen van data.

HSE weet niet wie er achter de aanval zit, zegt de publieke gezondheidsdienst tegen RTÉ. Uit voorzorg worden de IT-systemen afgesloten om deze te beschermen tegen de aanval en te kunnen onderzoeken. Onder meer het patiëntenregistratiesysteem is vanwege de aanval afgesloten. HSE spreekt over een 'significante, geavanceerde aanval', maar er zou nog geen losgeld zijn geëist. Het is niet duidelijk om wat voor ransomware-aanval het gaat.

Het Franse Hospital Center Sud Francilien (CHSF) werd op 21 augustus slachtoffer van een ransomware-aanval. Het ziekenhuis is genoodzaakt om operaties uit te stellen en patiënten naar andere inrichtingen door te verwijzen.

Het CHSF heeft meer dan 1.000 bedden en bedient 600.000 inwoners in de buurt van Parijs. Elke storing zet het leven van inwoners op het spel. "Door de aanval op het computernetwerk zijn alle bedrijfssoftware, opslagsystemen en het informatiesysteem met betrekking tot patiëntenopnames voorlopig ontoegankelijk", deelde de organisatie in een verklaring.

KWAADWILLENDEN



Note:Towards a new cyber threat actor typology – Van Eeten, Hernández Gañán en Pieters

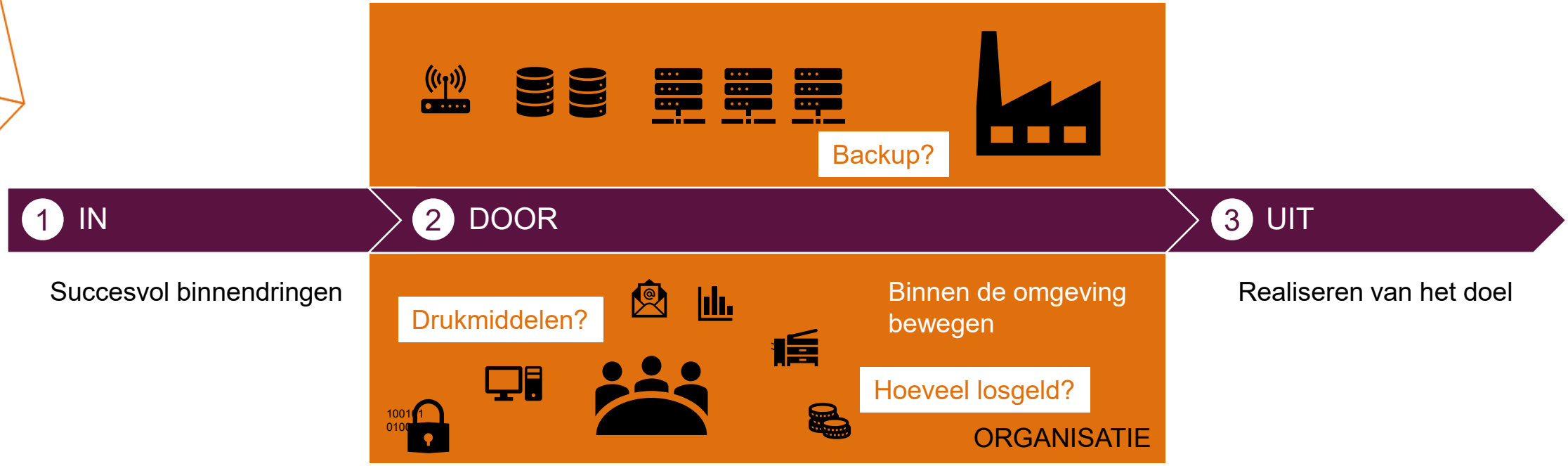
Een ransomware-aanval kent doorgaans drie fasen

Vereenvoudigd model van de Unified Kill Chain - https://www.csacademy.nl/images/scripties/2018/Paul_Pols_-_The_Unified_Kill_Chain_1.pdf

In de IN fase wordt handig gebruik gemaakt van actualiteit

Vereenvoudigd model van de Unified Kill Chain - https://www.csacademy.nl/images/scripties/2018/Paul_Pols_-_The_Unified_Kill_Chain_1.pdf

In de DOOR fase wordt geprobeerd maximale toegang en informatie te verkrijgen



Vereenvoudigd model van de Unified Kill Chain - https://www.csacademy.nl/images/scripties/2018/Paul_Pols_-_The_Unified_Kill_Chain_1.pdf

De UIT fase bestaat voor ransomware uit twee stappen

1. Aanrichten van schade (versleutelen, backup vernietigen, gegevens stelen)
2. Afpersen van een slachtoffer (extortion)

Vereenvoudigd model van de Unified Kill Chain - https://www.csacademy.nl/images/scripties/2018/Paul_Pols_-_The_Unified_Kill_Chain_1.pdf

De UIT fase bestaat voor ransomware uit twee stappen

1. Aanrichten van schade (versleutelen, backup vernietigen, gegevens stelen)
2. Afpersen van een slachtoffer (extortion)

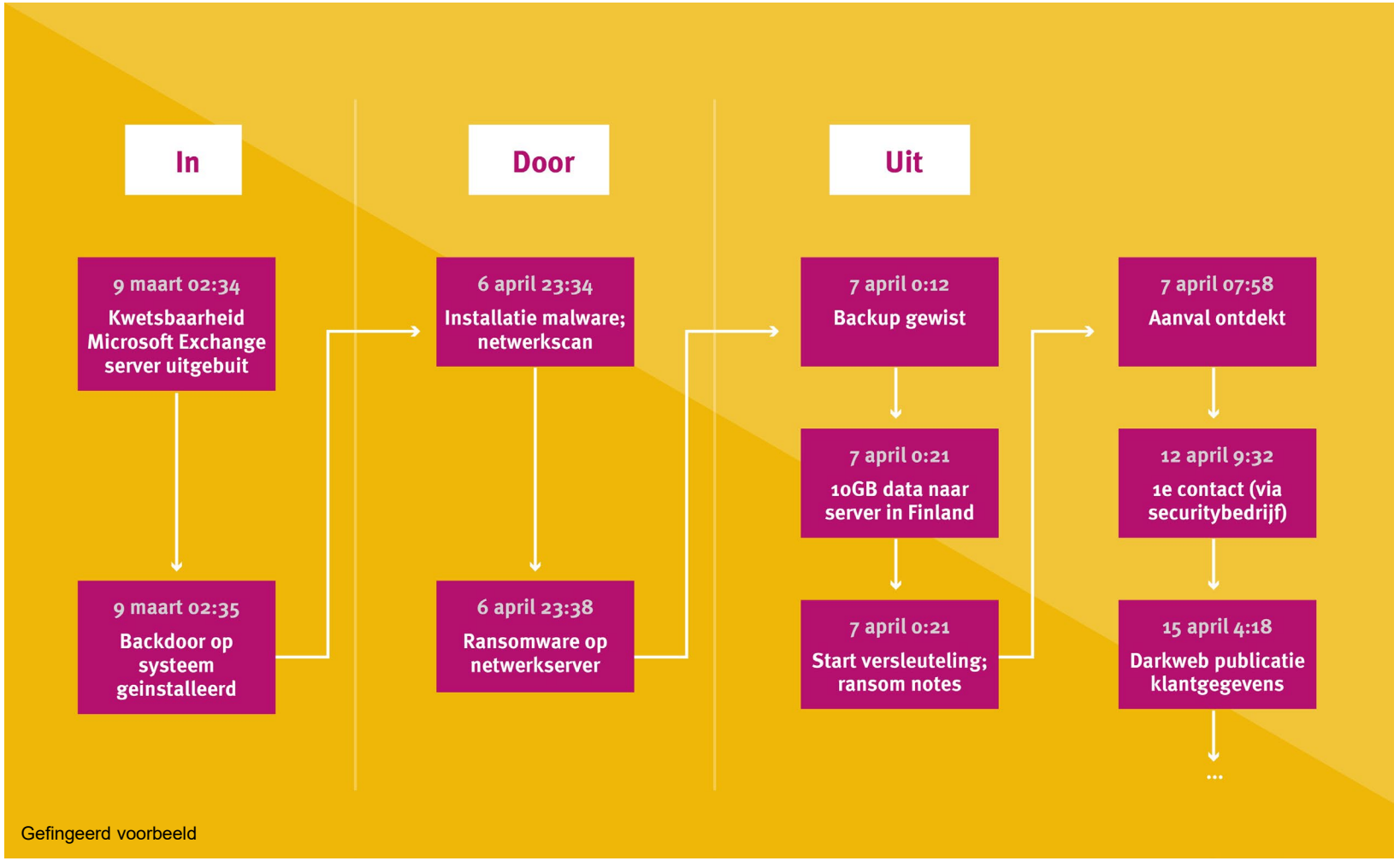
Vereenvoudigd model van de Unified Kill Chain - https://www.csacademy.nl/images/scripties/2018/Paul_Pols_-_The_Unified_Kill_Chain_1.pdf

Data-exfiltratie komt steeds meer voor

Data-exfiltratie bij een ransomware-aanval ziet er schematisch zo uit:

Data-exfiltratie is een proces tijdens een ransomware-aanval waarbij data wordt gestolen en eventueel openbaar gepubliceerd als het slachtoffer niet betaald. Het doel van aanvallers is dus om druk uit te oefenen op het slachtoffer. Voor het gemak verstaan we onder data-exfiltratie alle stappen van dataverzameling op het netwerk van het slachtoffer, het exfiltreren van die data en publiceren van deze data.

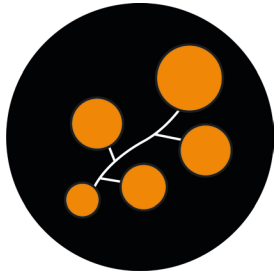
Samengevat…



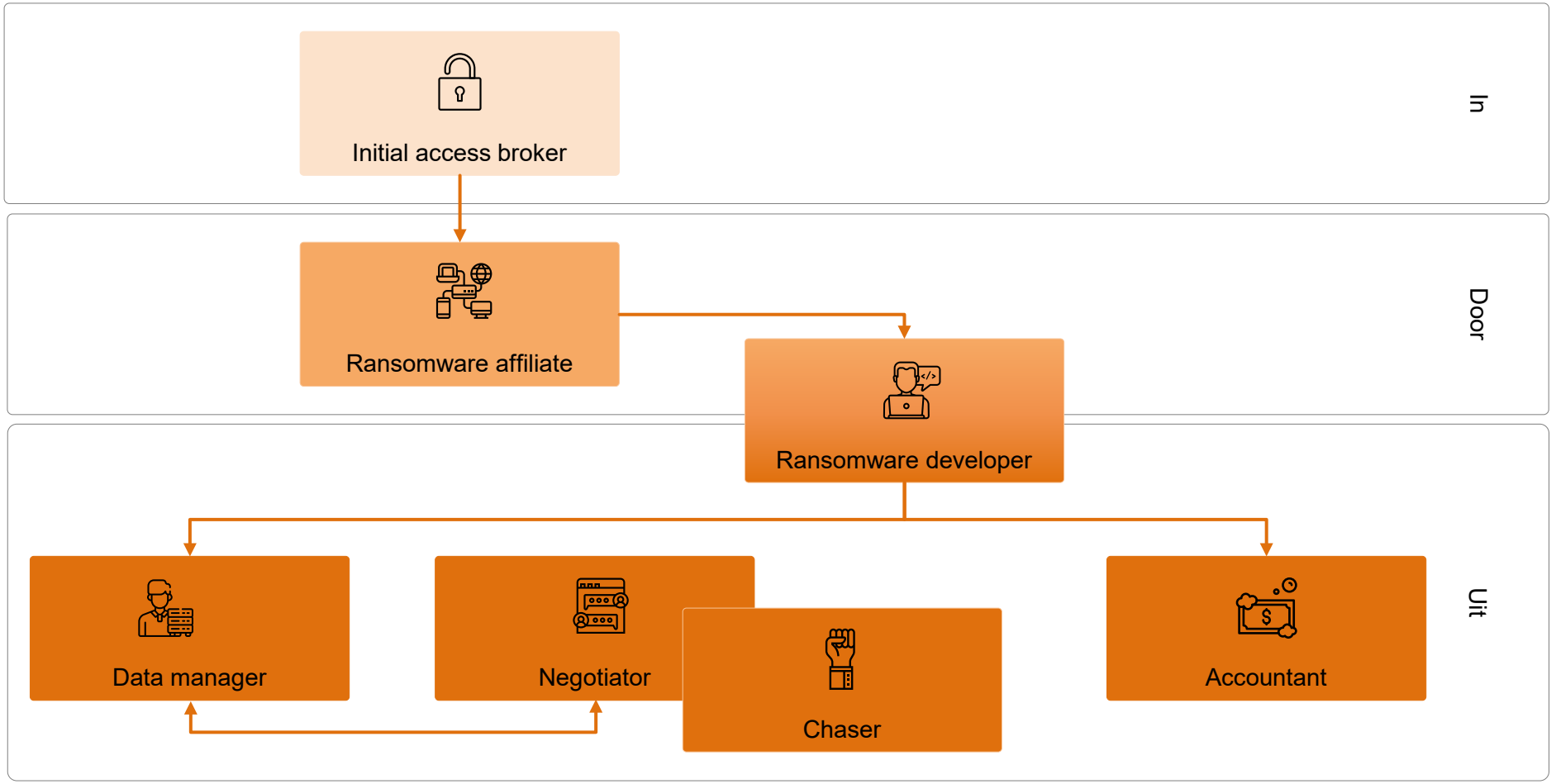
Gefingeerd voorbeeld

Ransomware is geëvolueerd tot een professionele vorm van cyberaanvallen

ASPECT	10 JAAR GELEDEN	NU
KWALITEIT	Slecht	Zeer professioneel
VORM	Opportunistische aanvallen op eindgebruikers	Volwassen criminele markt met gerichte en ongerichte aanvallen op organisaties van elke grootte
BETROUWBAARHEID	Niet reageren op betaling	Hoogwaardige service bij betaling
DRUKMIDDELEN	Social engineering / single extortion (alleen versleutelen)	Double (versleuteling + diefstal informatie) en triple extortion (versleuteling + diefstal informatie + afpersen relaties van slachtoffer)
BEDRAGEN	Enkele tientjes per slachtoffer	Tot tientallen miljoenen per slachtoffer
ACTOREN	Amateurs	Ransomware as a service, gespecialiseerde samenwerkende groeperingen



Dé cybercrimineel bestaat niet



Verschillende **groepen aanvallers** zijn vaak betrokken bij een **stap-voor-stap proces** om slachtoffers grote bedragen aan geld afhandig te maken

De gevolgen van een ransomware-aanval zijn vaak groot

Coveware[1]: in Q4 2020 bedroeg de gemiddelde losgeldeis $220.298, met een mediaan van $78.398

De gemiddelde downtime bij slachtoffers bedroeg 23 dagen

Daarnaast zijn er nog kosten voor:

- Oplossen incident (communicatie, reputatieschade, etc.)
- Investeringen heropbouw en beveiligen netwerk
- Doorbetalen mensen en apparatuur
- Etc.

Bij bedrijven ligt de losgeldeis vaak tussen de 0,4% en 2% van de jaaromzet

Draagkracht is een belangrijk criterium voor de hoogte van de losgeldeis

Gevolgen zijn steeds vaker merkbaar in de maatschappij (Kaas-hack, Colonial Pipeline-hack)

Een aanval zorgt in het klein ook voor grote persoonlijke schade voor betrokkenen (baanverlies, privéproblemen, etc.)

[1]https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

We willen natuurlijk allemaal graag het liefste een ransomware aanval voorkomen…

	IN	DOOR	UIT
MENS	Awareness training	Positieve security cultuur	Training crisis-scenario's
ORGANISATIE	Wachtwoordbeleid Patch management	Kritieke processen beheren	Incident response plan
TECHNIEK	End point detection & response	Netwerksegmentatie Access control Network monitoring	Offline back-up (3-2-1 principe) Log retentie

Er zijn veel informatieve kennisproducten (zie bijv. https://www.ncsc.nl/documenten)
Cybersecuritybedrijven kunnen passend advies geven over benodigde maatregelen

Meer details staan in de whitepapers ransomware en data exfiltratie

https://cyberveilignederland.nl/actueel/cyberveilig-nederland-publiceert-whitepaper-ransomware-en-ncsc
https://cyberveilignederland.nl/upload/userfiles/files/VCNL_Whitepaper_Exfiltratie_v3_0_Web.pdf

Tenslotte: deel ervaringen!

CYBERVEILIG NEDERLAND

Liesbeth Holterman

info@cyberveilignederland.nl

www.cyberveilignederland.nl