RANSOMWARE BACK-UP
PATCH TRIPLE EXTORTION
MALWARE PENTEST
BULLETPROOF ANGEL
AIR GAP ASSURANCE
KLIKFRAUDE HOSTING
WACHTWOORDKLUIS

Cybersecurity Woordenboek 2024

Van **Cybersecurity**
naar **Nederlands**

Voorwoord Cybersecurity Woordenboek

Recente cyberincidenten hebben laten zien wat de mogelijke gevolgen van digitale uitval zijn. Digitale uitval heeft bij deze incidenten impactvolle fysieke gevolgen: vertraging op vliegvelden, ziekenhuizen konden de zorg niet plannen en haperende communicatiesystemen van onze hulpdiensten. Door de huidige geopolitieke spanningen neemt de kans op digitale uitval en verstoring nog steeds toe. Statelijke actoren voeren cyberaanvallen uit om politieke, economische en militaire doelen te bereiken. Ook zien we wereldwijd opererende en steeds geavanceerdere criminelen die grof geld verdienen aan digitale criminaliteit. Maar, ook menselijke fouten in complexe en sterk verwerven netwerk- en informatiesystemen kunnen leiden tot brede en onvoorspelbare uitval. In een tijd waarin digitale dreigingen en de afhankelijkheid van onze samenleving en economie van digitale processen steeds verder toenemen, is het belang van cybersecurity nog nooit zo groot geweest. De dreigingen waar we als samenleving mee te maken krijgen, nemen zowel in complexiteit als in frequentie toe. Daarmee wordt de woordenschat ook steeds verder uitgebreid. Dit vraagt om een woordenboek dat continu in ontwikkeling blijft. Als coördinerend minister op cybersecurity presenteer ik u daarom met veel enthousiasme en trots alweer de vierde editie van het Cybersecurity Woordenboek.

Dit woordenboek legt zo'n 780 cybersecuritytermen uit in begrijpelijke taal. Het is een waardevolle gids voor iedereen die werkt aan de digitale weerbaarheid van Nederland, of er meer over te weten wil komen. Het woordenboek is een initiatief van Cyberveilig Nederland in samenwerking met ruim 90 organisaties en vele Nederlandse cybersecurity professionals, en tevens in samenwerking met het ECP, Platform voor de Informatiesamenleving. Deze gezamenlijke inspanning maakt het mogelijk om gebruikers van cybersecuritydiensten beter te ondersteunen of als specialist de directie beter te informeren. Met het woordenboek kunnen zij eenvoudiger het gesprek aangaan.

De voortdurende ontwikkeling van cyberdreigingen vraagt om actuele en toegankelijke kennis. Dit woordenboek helpt u om een beter inzicht te krijgen in de complexe wereld van cybersecurity en stelt u in staat om effectiever te communiceren met experts in het veld. Want pas wanneer we de taal van de digitale wereld begrijpen, kunnen we beter inspelen op de dreigingen die ermee gepaard gaan. In het kader van Nederlandse Cybersecurity Strategie werken we met de overheid, het bedrijfsleven en de wetenschap samen aan een veiligere digitale toekomst. De uitdagingen zijn groot, maar met de juiste kennis en een gemeenschappelijke taal kunnen we de digitale weerbaarheid van onze samenleving verder versterken.

David van Weel
Minister van Justitie en Veiligheid

Inleiding Cybersecurity Woordenboek

Dit is alweer de vierde uitgave van het Cybersecurity Woordenboek! In 2019 zijn we hiermee begonnen vanuit Cyberveilig Nederland omdat we vonden dat cybersecurity begint bij de basis: elkaar kunnen begrijpen in een gemeenschappelijke taal. Mooi om te zien hoe we als specialisten in het vakgebied hierin zijn gegroeid: waar we in 2019 nog in ons eigen ‘ jargon’ dachten, proberen we anno 2024 bij een cybersecurity woord deze meteen deze in begrijpelijke taal aan de ander uit te leggen. Het Cybersecurity Woordenboek heeft in onze ogen sterk bijgedragen aan deze ontwikkeling.

Al meteen bleek het woordenboek in 2019 een succes: veel organisaties gebruiken de termen in het woordenboek om hun diensten begrijpelijk uit te leggen of om als CISO moeilijke onderwerpen op gebied van cybersecurity uit te leggen in de boardroom.

Ons vakgebied is volop in beweging, ook vanwege nieuwe wet- en regelgeving zoals de Cyberbeveiligingswet. Datis terug te zien in het aantal termen, inmiddels gegroeid tot bijna 800. Met trots presenteren we daarom de herziene versie: het Cybersecurity Woordenboek 2024. Een initiatief van Cyberveilig Nederland in samenwerking met ECP, het Platform voor de Informatiesamenleving.

Het Cybersecurity Woordenboek is het resultaat van een samenwerking met ruim 100 cybersecurity experts vanuit de Nederlandse overheid, wetenschap en private organisaties. Leuk om bij elke nieuwe uitgave weer de organisaties te zien die er in 2019 al bij waren, maar ook om nieuwe enthousiastelingen te mogen verwelkomen bij de doorontwikkeling.

Het woordenboek is gemaakt met de volgende uitgangspunten:

1. De opgenomen termen worden veel gebruikt bij de afnemers van cybersecuritydiensten en door CISO’s. Het woordenboek is daarom geschreven op een wijze dat niet-vakspecialisten de betekenissen goed kunnen begrijpen.

2. We hebben vooral uitleg gegeven aan de termen (verklarend). We zijn minder bezig geweest om de exacte definities te bepalen waar iedereen zich aan moet houden (definiërend).

3. De termen in het woordenboek gaan uit van de context van cybersecurity. Daarom hebben we zoveel mogelijk de toevoeging ‘cyber’ weggelaten bij zowel de uitleg als de opgenomen vaktermen. Daar waar de term met het voorvoegsel cyber- is ingeburgerd, hebben we deze wel zo opgenomen.

4. Algemene IT-termen die niet specifiek voor cybersecurity zijn of geen sterke link ermee hebben zijn weggelaten. Zo zijn bijvoorbeeld router, switch en browser niet opgenomen, maar wel cloud computing, cookie en domeinnaam.

5. Overheidsorganisaties die als wettelijke (dienstverlenende) taak een sterke link hebben met cybersecurity zijn opgenomen. Bijvoorbeeld: Het Nationaal Cyber Security Centrum (NCSC), de Rijksinspectie Digitale Infrastructuur. het Digital Trust Center (DTC) en de Autoriteit Persoonsgegevens. Niet opgenomen zijn bijvoorbeeld: Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en toezichthouders als de Inspectie Leefomgeving en Transport (ILT)

6. Certificeringen op het gebied van cybersecurity die vaak worden gebruikt in offerteaanvragen en aanbestedingen hebben we opgenomen. De certificerende instanties die deze certificering bekrachtigen zoals SANS, ISACA, ISC2, EC-Council, IAPP zijn niet opgenomen.

7. Begrippen die ook in de begrippenlijst van het Cybersecurity Beeld Nederland (CSBN) 2024 zijn opgenomen, hebben we in de meeste gevallen integraal overgenomen. Waar we de uitleg in het CSBN te beperkt vonden door haar scope hebben we voor enkele begrippen (zoals dreiging en gevaar) gekozen voor een andere invulling.

8. Voorbeelden van kwetsbaarheden zijn niet allemaal opgenomen, wel de vaktermen die voorkomen in de uitleg van de OWASP top 10.

9. Namen van aanvallen en malware zijn niet opgenomen in de lijst. Ook niet wanneer deze veel media-aandacht hebben gekregen.

10. Niet alle securityprotocollen zijn opgenomen. We hebben ons beperkt tot de protocollen op internet.nl en de protocollen die vaak in gesprekken tussen aanbieders en afnemers van cybersecurydiensten worden besproken. Voorbeelden zijn: TLS, SPF, DKIM, SSL.

11. Niet alle normenkaders zijn opgenomen. We hebben ons beperkt tot de ISO/IEC 27000 serie. Specifieke normen die alleen in bepaalde sectoren worden gebruikt, zoals NEN 7510 (zorg) en BIO (overheid) zijn daarom niet opgenomen. In samenwerking met de NEN zijn de termen die worden gehanteerd in de herziening van de ISO 27002 opgenomen in dit woordenboek.

12. Er is een fopwoord opgenomen in het woordenboek, vergelijkbaar met de fopwoorden uit vroegere woordenboeklijsten. Het is een woord zonder verdere betekenis.

13. Als in de uitleg van de termen een “hij” staat wordt niet een man bedoeld, maar een persoon in het algemeen.

14. We gebruiken bij de uitleg van de termen “digitaal systeem”als verzamelnaam voor woorden als computer, computersysteem, computer-netwerk. Dit hebben we besloten omdat bijna alle digitale systemen onderling verbonden zijn. In de meeste gevallen kan “digitaal systeem” dus ook gelezen worden als “digitaal genetwerkt systeem”.

Tot slot wil ik zeggen dat de inhoud van dit woordenboek met de grootste zorg en een enorme inzet van veel experts uit het werkveld is samengesteld. Ik wil iedereen heel hartelijk bedanken voor hun inzet die vaak tot in de nachtelijke uren doorging! We streven ernaar om elke drie jaar het woordenboek te herzien. Waarschijnlijk valt er ook nog veel te verbeteren aan de woordenlijst. Dat zullen we gaan doen in de vijfde druk. Alle feedback is daarom zeer welkom via het mailadres woordenboek@cyberveilignederland.nl.

Petra Oldengarm
Directeur Cyberveilig Nederland
November 2024

BEGRIP	BETEKENIS	ZIE OOK
0-day	...	*Zie zero-day*
2-stapsverificatie	Tweefactorauthenticatie	*Meerfactor authenticatie*
2-trapsverificatie	Tweefactorauthenticatie	*“”*
2FA	Tweefactorauthenticatie	*“”*
AAA	Authenticatie, autorisatie en accounting	*Authenticatie, autorisatie en accounting*
Aanbieder van essentiële diensten	Een aanbieder die vanuit de Wet beveiliging netwerk en informatiesystemen en straks de Cyberbeveiligingswet rechten en plichten heeft op het gebied van cybersecurity.	*Wet beveiliging netwerk- en informatie systemen*
Aanval	...	*Cyberaanval*
Aanvaller	Iemand die met opzet de beveiliging probeert uit te schakelen of omzeilen om in een digitaal systeem te komen.	
Aanvalsfacilitator	Persoon of entiteit met kwaadaardige intenties die software, computers en netwerken ontwikkelt en verkoopt zodat anderen hiermee digitale aanvallen kunnen uitvoeren.	
Aanvalsoppervlak	Het gedeelte van digitale systemen dat een aanvaller kan bereiken om zijn aanvallen op te richten.	*Aanvalsvector*
Aanvalspad	Route die een aanvaller gebruikt in een digitale omgeving om van de initieel verkregen toegang bij zijn doel te komen. Een dergelijk pad kan worden gemodelleerd aan de hand van bijvoorbeeld de Unified Kill Chain of de cyber kill chain.	*Aanvalsvector , Cyber kill chain*
Aanvalsvector	Manier die een aanvaller kan gebruiken om een digitaal systeem binnen te dringen.	*Aanvalsoppervlak, Aanvalspad*

BEGRIP	BETEKENIS	ZIE OOK
Acceptable risk level	...	*Risico acceptatie*
Acceptable Use Policy	Beleid van de aanbieder/eigenaar van een systeem of dienst voor aanvaardbaar gebruik. Dit beleid bepaalt welke handelingen/ activiteiten de gebruikers/klanten mogen verrichten. Bij het gebruik van een systeem buiten de acceptable use policy (AUP) kunnen veiligheidsoverwegingen en juridische gevolgen een rol spelen en niet geaccepteerde veiligheidsrisico’s ontstaan.	*AUP*
Access Control	...	*Toegangsbeheer*
Access Control List	Een lijst waarop staat welke gebruiker of systeem welke toegang heeft in een idigitaal systeem of onderdeel ervan.	*ACL*
Access Point	Een apparaat waarmee een gebruiker of systeem verbinding maakt om met een netwerk te verbinden.	
Account	Element van een digitaal systeem dat een gebruiker representeert. Bij een account hoort informatie over de gebruiker, zoals persoonlijke gegevens, inloggegevens en informatie waar de gebruiker bij mag. Er bestaan verschillende soorten accounts, zoals een gebruikersaccount of een administratoraccount voor beheerders. In het spraakgebruik wordt deze term vaak gebruikt om lidmaatschap bij een dienst aan te duiden - “Ik heb een account bij ...”.	*Inlogcode, Wachtwoord, Meerfactor-authenticatie*
Account hijacking	Het overnemen van een account met bijbehorende rechten. Wordt gebruikt bij onder andere identiteitsdiefstal.	*Identity theft*
Account niet persoonsgebonden	Account niet aan een specifieke natuurlijke persoon gebonden (bijvoorbeeld adminstator accounts en service accounts).	
Accountability	Verantwoordelijk worden gehouden voor het eindresultaat.	

BEGRIP	BETEKENIS	ZIE OOK
Accreditatie	Verklaring van een toezichthouder dat een getoetste organisatie geschikt is om haar werk te doen en dat haar diensten voldoen aan bepaalde eisen.	
Achterdeur	...	*Backdoor*
ACL	Access Control List	*Access Control List*
Actor	Een persoon of samenstelling van personen die een cyberaanval uitvoert of de intentie daartoe heeft. Voorbeelden zijn: a) staten/ staatsgelieerde actoren, b) criminelen, c) terroristen, d) hacktivisten, e) cybervandalen en scriptkiddies en f) insiders.	
Admin	...	*Administrator*
Administrator	Beheerder van een digitaal systeem of computernetwerk. Deze persoon heeft meer rechten dan een gewone gebruiker. Zo kan hij bijvoorbeeld instellingen aanpassen. En hij bepaalt wat gebruikers in een computernetwerk mogen doen en wat niet.	
Advanced Red Teaming	Dit is een grote oefening (adversary simulation) onder toezicht van een toezichthouder, zoals de Nederlandsche Bank (DNB). Het verschil met een TIBER oefening is dat in een Advanced Red Teaming slechts één scenario wordt uitgevoerd, en gebaseerd op generieke threat intelligence (in plaats van specifieke threat intelligence).	*Adversary simulation*
Adversary simulation	Oefening waarbij een organisatie aanvallen simuleert om te ontdekken hoe goed ze is beschermd tegen aanvallen. Het Red team speelt aanvallen en aanvalsmethodes na van een gekozen tegenstander. Het Blue team probeert aanvallen van het Red team op te sporen en vervolgens tegen te gaan. Als ze een echte aanval tegenkomen, pakken ze die ook aan. Soms is er ook een White team. Dit team zorgt dat de oefening haar doel bereikt.	*Red team, Blue team, White team, Purple team, Crisisoefening, Penetratietest*

BEGRIP	BETEKENIS	ZIE OOK
““	Bijvoorbeeld door te bepalen welke informatie beide teams krijgen. De gecombineerde oefening met een Red team en een Blue team heet ook wel Purple teaming. Bij dit soort oefeningen ligt de nadruk op samenwerking tussen teams, en op het nadoen van tegenstanders en aanvallen. Bij een penetratietest probeert men zo diep mogelijk in een systeem binnen te dringen.	*””*
Adware	Software die onbewust op een digitaal systeem van een gebruiker wordt geplaatst. De software verzamelt informatie uit het systeem. Die informatie wordt gebruikt om bijvoorbeeld via advertenties doelgerichte reclame naar de gebruiker te sturen of profielen van gebruikers te verzamelen.	
AED	...	*Aanbieder van Essentiele Diensten*
Agent	Computerprogramma dat op de achtergrond draait om bepaalde processen te ondersteunen of uit te voeren.	
AI	Artificial Intelligence.	*Artificial Intelligence*
AI-verordening	Europese verordening die de regels bevat voor het verantwoord ontwikkelen en gebruik van kunstmatige intelligentie door bedrijven, overheden en andere organisaties.	*Europese wet- en regelgeving*
Air gap	Maatregel die ervoor zorgt dat een component of computer of netwerk niet verbonden is met een ander netwerk of het Internet. Fysieke isolatie van netwerken en/of systemen.	

BEGRIP	BETEKENIS	ZIE OOK
Algemene Verordening Gegevensbescherming	In Europa wordt dit geregeld in de GDPR. De AVG is de Nederlandse uitwerking van de Europese GDPR. De GDPR zorgt ervoor dat er in de gehele EU dezelfde basis/ minimum regels voor de bescherming van persoonsgegevens zijn. De AVG is in Nederland de opvolger van de Wet Bescherming persoonsgegevens.	*Europese wet- en regelgeving, Autoriteit Persoonsgegevens*
Algoritme	Set van regels en instructies die een digitaal systeem uitvoert.	*AI*
Allow listing	Actie waarmee men in een lijst vastlegt welke applicaties, gebruikers en acties men toestaat. Alles wat niet op de lijst staat wordt automatisch geblokkeerd. Het tegenovergestelde is blacklisting.	*Allow listing, Blacklisting, Blocklisting, Denylisting, Whitelisting*
Anomaly	Iets wat afwijkt van het normale gedrag van een gebruiker, netwerk, computer, laptop, smartphone of ander digitaal systeem, vaak veroorzaakt door malware of een kwaadaardige aanvaller.	*Anomaly detection*
Anomaly detection	Een afwijking ontdekken in het gedrag van een digitaal systeem. Bijvoorbeeld een netwerk, computer, laptop, smartphone of ander digitaal apparaat. Dit doet men om daarna te onderzoeken of het gaat om een ongewenste of zelfs kwaadaardige afwijking.	
Anomaly-based detection	...	*Anomaly detection*
Anonimiseren	Maskeren, wijzigen of verwijderen van gegevens zodat deze niet meer herleidbaar zijn tot een persoon. Door persoonsgegevens te pseudonimiseren is het moeilijker om deze gegevens te herleiden naar personen. En dat maakt bijvoorbeeld de impact kleiner bij een datalek. Een methode om persoonsgegevens te pseudonimiseren is hashing.	

BEGRIP	BETEKENIS	ZIE OOK
Anonymity	Door de opzet van het Internet is het mogelijk om anoniem te blijven als je op Internet iets doet. Er is dan niet te achterhalen welke persoon of machine iets doet. Dit draagt weliswaar bij aan de vrijheid van meningsuiting, maar maakt het ook moeilijker om kwaadwillenden op te sporen.	
Anonymizing Proxy	Een proxy-server of proxydienst die gebruikt wordt om de oorsprong van netwerkverkeer mee te verbergen.	*Proxy*
Anonymizing VPN	Een VPN-server of VPN-dienst die gebruikt wordt om de oorsprong van netwerkverkeer mee te verbergen.	*VPN*
Antivirus software	Beveiligingssoftware die schadelijke software of schadelijke code herkent.	
AP	Autoriteit Persoonsgegevens, Access Point.	*Autoriteit Persoons-gegevens, Access Point*
API	Application Programming Interface. Een programma waarmee applicaties onderling communiceren zonder dat mensen dit aansturen.	
APT	Advanced Persistent Threat. Voortdurende dreiging van een geavanceerde tegenstander, zoals statelijke actoren of cybercriminelen, tegen een specifiek slachtoffer of instantie. Er wordt gebruik gemaakt van cyberaanvallen waarbij de aanvaller langere tijd in een digitaal systeem zit, zonder te worden opgemerkt. Of hij probeert langere tijd op allerlei manieren bij bepaalde informatie in het systeem te komen. Vaak wil de aanvaller hiermee blijvende toegang creëren in een digitaal systeem. Het doel is om schade toe te brengen. Een APT verschilt van een gewone dreiging door de (lange) tijdsinvestering,	*Statelijke actor, Cybercrimineel*

BEGRIP	BETEKENIS	ZIE OOK
““	het motief, de vasthoudendheid en soms ook de gekozen methoden van de aanvaller.	*““*
Architectuur	Het ontwerp en de opbouw van een digitaal systeem en netwerk. Het ontwerp regelt hoe businessprocessen, applicaties, data en technologie samenhangen.	
ART	Advanced Red Teaming.	*Advanced Red Teaming*
Artificial Intelligence	Technologie waarbij digitale systemen reageren op data, bijvoorbeeld afkomstig uit sensoren, en op basis daarvan zelfstandig acties ondernemen. Er us een streven naar lerend vermogen in de gebruikte technologie. Toepassing van dit soort technologie wordt steeds belangrijker binnen cybersecurity.	*Kunstmatige Intelligentie, AI*
Assessment	Onderzoek naar de verschillende soorten risico's die kunnen leiden tot een dreiging in één of meerdere digitale systemen. Voorbeelden van onderzoeken zijn penetratietesten, vulnerability assessments, red teaming en risico assessments.	*Audit, Risk assessment, Vulnerability Assessment, Red teaming, Penetratietest*
Asset	Informatie of digitale systemen die van waarde zijn voor een organisatie. Voorbeelden zijn: intellectueel eigendom, een klantendatabase, personeelsinformatie, etc.	
Asset Management	Complete inventarisatie van de digitale systeen en hoe deze structureel te beheren.	*Risk management, Aanvalsoppervlak*
Assurance	Zekerheid dat je kunt vertrouwen op de kwaliteit van een bepaalde dienst of een bepaald proces.	

BEGRIP	BETEKENIS	ZIE OOK
Assurance level	Mate van zekerheid waarin je kunt vertrouwen op de kwaliteit van een bepaalde dienst of een bepaald proces.	
Asymmetrische encryptie	Versleuteling is het onbegrijpelijk maken van informatie voor anderen zoals een tekstbestand of netwerkverkeer. Dit wordt gedaan met twee sleutels, in tegenstelling tot symmetrische versleuteling waarbij één sleutel wordt gebruikt. De ontvanger heeft een eigen persoonlijke sleutel die de verzender niet kent. De informatie wordt onleesbaar gemaakt met een openbare sleutel van de ontvanger en de ontvanger gebruikt vervolgens zijn persoonlijke sleutel om de informatie weer leesbaar te maken. Een andere functie is om met de persoonlijke sleutel een digitale handtekening te zetten onder data en met de openbare sleutel te controleren of de digitale handtekening met iemands persoonlijke sleutel is gemaakt en dus waarheidsgetrouw is voor deze data.	*Public Key Infrastructure, Encryptie*
ATT&CK framework	Gecategoriseerde verzameling van aanvalstechnieken onder beheer van MITRE (zie mitre.org) Het MITRE ATT&CK framework wordt bijvoorbeeld gebruikt om inzichtelijk te maken welke aanvalstechnieken een organisatie tegen beschermd is en waar nog maatregelen getroffen moeten worden, of om inzichtelijk te maken op welke aanvalstechnieken een bepaalde technologie of maatregel impact heeft.	
Attack surface	...	*Aanvalsoppervlak*
Attributie	Duiden dat een bepaalde organisatie of groep aanvallers een aanval heeft uitgevoerd of dat heeft proberen te doen.	

BEGRIP	BETEKENIS	ZIE OOK
Audit	1. Onderzoek waarmee men beoordeelt hoe de werkelijkheid binnen een afgekaderd gebied zich verhoudt tot een bepaalde (vastgestelde) norm. Kan getoetst worden aan de opzet, bestaan en werking van de norm. 2. Systematisch, onafhankelijk en gedocumenteerd proces voor het verkrijgen van auditbewijsmateriaal, en het objectief beoordelen daarvan om vast te stellen in welke mate aan de auditcriteria is voldaan.	
Audit log	1. Bestand waarin is vastgelegd wanneer, wie, wat heeft gedaan in het digitale systeem. Dit wordt veelvuldig gebruikt om na te gaan wie bijvoorbeeld toegang heeft gehad tot digitale systemen, informatie of onderdelen daarvan en welke wijzigingen zijn aangebracht. 2. Bestand waarin staat in welke volgorde men de onderdelen van een audit heeft uitgevoerd. Een audit is een onderzoek waarin men beoordeelt hoe een organisatie functioneert.	*Audit*
Auditor	(Gekwalificeerd) persoon of instantie die een audit uitvoert.	*Audit*
Audit log	...	*Audit trail*
AUP	...	*Acceptable Use Policy*
Authenticatie	Het vaststellen van de identiteit van een gebruiker, computer of applicatie.	*Identity en access management*
Autorisatie	De bevoegdheden die een gebruiker van een digitaal systeem en/of het digitale systeem, heeft gekregen om toegang te krijgen tot gegevens of handelingen te mogen uitvoeren. Bijvoorbeeld het opstarten van programma's of het inzien, wijzigen of wissen van informatie.	

BEGRIP	BETEKENIS	ZIE OOK
Autorisatiematrix	Tabel met uitgegeven rechten binnen een organisatie.	*Authorisatie*
Autoriteit Persoonsgegevens	Nederlandse overheidsorganisatie die toezicht houdt op de manier waarop organisaties persoonsgegevens verwerken. Ze doen dit zodat de privacy van personen goed beschermd wordt. Het toezicht is in de wet geregeld.	*Algemene Verordening Gegevensbescherming*
Availability	...	*Beschikbaarheid*
AVG	...	*Algemene Verordening Gegevensbescherming*
Awareness	...	*Bewustwording*
Back-up	Een reservekopie van gegevens of digitale systemen. Hiermee kan men gegevens of systemen herstellen als het origineel beschadigd of weg is.	
Backdoor	Een manier om via een omweg in een digitaal systeem te komen. Iemand heeft die omweg vaak met opzet gemaakt, en op zo'n manier dat anderen die niet kunnen zien.	
Backup	...	*Back-up*
Baseline	Pakket maatregelen dat ervoor moet zorgen dat de beveiliging van een netwerk een basisniveau heeft. Een voorbeeld van een baseline is de Baseline Informatie Overheid (BIO).	
Basismaatregelen	Activiteiten die zijn gericht op realisatie van minimaal noodzakelijke fysieke, procedurele, gedragsmatige en technische waarborgen opdat cyberincidenten kunnen worden voorkomen en wanneer cyberincidenten zich toch hebben voorgedaan deze kunnen worden ontdekt, schade kan worden...	*Basisprincipes*

BEGRIP	BETEKENIS	ZIE OOK
“”	... beperkt en herstel eenvoudiger kan worden gemaakt. Dit wordt ook wel cyberhygiëne genoemd. Het gaat bijvoorbeeld (maar niet alleen) om het maken van (online en offline) back-ups.	
Basisprincipes van digitale weerbaarheid	Door de Rijksoverheid geformuleerde basisprincipes: 1. Breng je risico’s in kaart 2. Bevorder veilig gedrag 3. Bescherm systemen, applicaties en apparaten 4. Beheer toegang tot data en diensten 5. Bereid je voor op incidenten	
BCI	Business Continuity Impact	*Business continuity impact*
Bedrijfsrisico	Risico dat er iets gebeurt wat negatieve gevolgen heeft voor de doelstellingen en resultaten van een bedrijf.	*Risico*
Behavioral targeting	...	*Profilering*
Beheersmaatregel	Een activiteit met als doel om de oorzaak of het gevolg van een ongewenste gebeurtenis te voorkomen, weg te nemen, of te verkleinen.	
Belang(en)	Waarden, verworvenheden, materiële en immateriële zaken waaraan schade kan ontstaan als een cyberincident zich voordoet en het gewicht dat de maatschappij of een partij aan de verdediging ervan toekent.	
Beschikbaarheid	De zekerheid dat gebruikers in een digitaal systeem of bij informatie kunnen of gebruik kunnen maken van digitale diensten of processen wanneer zij dat willen of zouden moeten kunnen. Gepland onderhoud telt niet mee.	
Best practice	Een techniek, werkmethode of activiteit die in de in de praktijk heeft bewezen effectief te zijn.	

BEGRIP	BETEKENIS	ZIE OOK
Bestuurs-aansprakelijkheid	De verantwoordelijkheid die bestuurders dragen voor hun eigen handelingen en beslissingen en die van hun verantwoordelijke medewerkers. Bestuurders kunnen persoonlijk aansprakelijk worden gesteld voor het niet actief naleven van wet- en regelgeving. Voor de Cyberbeveiligingswet geldt deze aansprakelijkheid.	*Cyberbeveiligingswet, DORA, Europese wet- en regelgeving*
Betrouwbaarheid	Mate waarin digitale (genetwerkte) systemen beschikbaar zijn voor gebruik. Cyberaanvallen, uitval en storingen kunnen de betrouwbaarheid beïnvloeden.	
Beveiliging	Alle maatregelen die nodig zijn om een digitaal systeem te beschermen tegen schadelijke invloeden.	*Risico, Threat, Kwetsbaarheid*
Beveiligingsbewustzijn	De mate waarin mensen risico’s herkennen en zich ervan bewust zijn dat deze de veiligheid van informatie in gevaar kunnen brengen.	
Cyberincident	...	*Cyberincident*
Beveiligingslek	...	*Kwetsbaarheid*
Beveiligingsmaatregel	Iets wat men doet om risico’s voor de veiligheid van informatie te verkleinen of weg te nemen.	*Business impact analyse*
BIA	Business Impact Analyse of Business Impact Assessment.	*Business Impact Analyse, Business Impact Assessment*
Biometrie	Methode om vast te stellen wie iemand is. Men gebruikt hiervoor unieke kenmerken van het lichaam. Denk aan een vingerafdruk of irisscan.	
Bitcoin	Digitale munteenheid.	*Cryptovaluta*

BEGRIP	BETEKENIS	ZIE OOK
BIV	Model om drie verschillende kenmerken van informatiebeveiliging aan te duiden: beschikbaarheid, integriteit en vertrouwelijkheid van informatie en informatiesystemen. Met andere woorden: is de informatie en het systeem op het gewenste moment te zien en te gebruiken? Klopt de informatie? En wie mag de informatie zien en het systeem gebruiken?	*Beschikbaarheid, Integriteit, Vertrouwelijkheid, CIA*
Blackbox test	Veiligheidstest die aangeeft dat de tester geen voorkennis van het systeem heeft. Je kunt ook op andere manieren testen: - Heeft de tester een beetje kennis? Dan heet het greybox test. - Bij veel voorkennis, zoals bijvoorbeeld toegang to de broncode, is het een whitebox test of crystalbox test.	*Greybox test, Whitebox test, Crystalbox test*
Blackhat hacker	Iemand die met kwade bedoelingen inbreekt in een digitaal systeem. De naam 'blackhat' komt uit cowboyfilms waarin slechteriken altijd een zwarte hoed dragen.	*Hacker, Greyhat hacker, Whitehat hacker*
Blacklisting	Actie waarmee men in een lijst vastlegt welke applicaties, gebruikers en acties men blokkeert. Al het andere dat niet op de lijst staat is dus wel toegestaan.Er wordt naar gestreefd om deze term te vervangen voor het meer neutrale allow/deny listing.	*Allow listing, Blacklisting, Blocklisting, Denylisting, Whitelisting*
Blockchain	Een digitaal overzicht waarin transacties worden gecontroleerd en opgeslagen als ze in orde zijn. Dat gebeurt via een netwerk van computers. Iedere nieuwe waarde die in het overzicht komt te staan, wordt berekend op basis van de vorige waarde. Vandaar de naam 'chain' (ketting). Het voordeel van een blockchain is dat er geen onafhankelijke persoon bij nodig is voor het valideren van de transacties, zoals een notaris. Men gebruikt blockchain voor verschillende doelen. Onder meer voor cryptovaluta, zoals de bitcoin.	*Cryptovaluta*

BEGRIP	BETEKENIS	ZIE OOK
Blocklisting	Lijst waarop zaken worden bijgehouden die geblokkeerd worden. Een dergelijke lijst wordt gebruikt door een software die bijvoorbeeld gebruikers, IP-adressen of applicaties toegang ontzegt op basis van de lijst.	*Allow listing, Blacklisting, Blocklisting, Denylisting, Whitelisting*
Blokkeren & filteren	Techniek waarmee op geautomatiseerde wijze domeinen of websites ontoegankelijk worden gemaakt. Of waarbij het onmogelijk wordt gemaakt specifieke informatie te delen. Blokkeren betekent dat een eindgebruiker geen toegang heeft tot een website op basis van de URL van die website. Bij filteren heeft de eindgebruiker geen toegang door bepaalde inhoud op de website.	*Filteren & blokkeren*
Blue team	Oefening waarbij een organisatie aanvallen simuleert om te ontdekken hoe goed ze is beschermd tegen aanvallen. Het Red team speelt aanvallen en aanvalsmethodes na van een gekozen tegenstander. Het Blue team probeert aanvallen van het Red team op te sporen en vervolgens tegen te gaan. Als ze een echte aanval tegenkomen, pakken ze die ook aan.	*Adversary simulation*
Booter	Een dienst van criminelen om een DDoS-aanval mee uit te voeren.	
Bot	Een computerprogramma dat zelfstandig taken kan uitvoeren. Bot is een afkorting van robot. Een bot kan onschuldig zijn, bijvoorbeeld als zoekmachines bots gebruiken om websites te vinden. Maar iemand kan een bot ook gebruiken om in te breken in een computer. Of om de computer zo klaar te maken dat een ander kan inbreken. Een computer die besmet is met een bot, noemt men ook wel een zombie. De gebruiker van een computer merkt vaak niets van een bot.	*Botnet, Command-and-control server*

BEGRIP	BETEKENIS	ZIE OOK
Bot herder	Iemand die een botnet beheert.	*Bot, Botnet, Command-and-control server*
Botnet	Een verzameling van besmette systemen die door actoren centraal bestuurd kan worden. Botnets vormen de infrastructuur voor veel vormen van Internetcriminaliteit.	*Bot, Command-and- control server*
Bounty program	...	*Bug bounty program*
Breach Counsel	Advocaat gespecialiseerd in het ondersteunen bij een cyberincident.	
Broncode	De leesbare tekst die een programmeur heeft geschreven in een programmeertaal. Er bestaan verschillende programmeertalen, zoals C, C++, Pascal. De broncode wordt door een compiler omgezet naar een voor computer uitvoerbare machine code.	*Escrow*
Brute force aanval	Een aanvalsmethode waarbij iemand met een hulpmiddel alle mogelijkheden uitprobeert om een geheime code te achterhalen. Bijvoorbeeld een wachtwoord.	
Bruto risico	Risico-inschatting waarbij niet wordt gekeken of men het risico kan verkleinen of wegnemen.	
Buffer overflow	Situatie waarin een programma of besturingssysteem problemen krijgt doordat het meer data moet opslaan dan past in het stuk geheugen dat hiervoor beschikbaar is. Gevolg is dat het programma of systeem onvoorspelbaar wordt. Soms crasht een digitaal systeem hierdoor. Of het voert commando's uit die het normaal niet had mogen uitvoeren.	*Kwetsbaarheid, Bug*
Bug	Een fout in de hardware of software van een digitaal systeem.	

BEGRIP	BETEKENIS	ZIE OOK
Bug bounty	Beloning die iemand krijgt als hij een beveiligingslek in een digitaal systeem heeft gevonden en gemeld. Men krijgt de beloning van de eigenaar van het digitale systeem.	
Bulletproof hosting	Een hostingdienst (zoals cloud-hosting, dedicated servers of webhosting) die zeer tolerant is in het type materiaal dat opgeslagen is op de afgenomen server en/ of de activiteiten die verricht worden via de afgenomen server. Dit uit zich doordat deze hosters geen maatregelen nemen als gevolg van abusemeldingen of andere klachten of notificaties over de afgenomen servers. Deze hosting is populair bij spammers, cybercriminelen en aanbieders van illegaal materiaal, omdat de servers langer in de lucht blijven dan bij andere hosters.	
Business continuity	Vermogen van een organisatie om tijdens een verstoring producten en diensten met een vooraf vastgestelde capaciteit binnen aanvaardbare tijdskaders te blijven leveren. Zelfs bij een incident of crisis.	
Business continuity impact	Hoe ernstig de gevolgen zijn van een groot cyberincident, als belangrijke ICT-bedrijfsprocessen en applicaties uitvallen.	
Business continuity plan (BCP)	Gedocumenteerde informatie die een organisatie richting geeft om te reageren op een verstoring en de levering van producten en diensten conform haar doelstellingen voor bedrijfscontinuïteit te hervatten en herstellen.	
Business e-mail compromise (BEC)	Een incident waarbij de aanvaller is doorgedrongen tot de mailomgeving van een organisatie. De aanvaller kan deze toegang gebruiken om vertrouwelijke informatie te stelen of om nieuwe aanvallen mee uit te voeren. Bijvoorbeeld CxO-fraude.	*CEO/CFO/CxO fraude*

BEGRIP	BETEKENIS	ZIE OOK
Business Impact Analyse	Proces voor het analyseren van de impact in de tijd gemeten van een verstoring op de organisatie. Deze analyse is onderdeel van een Business Continuity Plan en kan men gebruiken om zich voor te bereiden op grote storingen.	
BYOD	Bring Your Own Device. Situatie waarbij personen hun eigen apparaten, zoals een privételefoon of -laptop, mogen gebruiken in een zakelijk computernetwerk van een organisatie. Vaak mag dit alleen onder bepaalde voorwaarden.	
C&C server	Command-and-control server.	*Comand-and-control server*
C2 server	Command-and-control server.	*Comand-and-control server*
CA	Certificate Authority.	*Certificate authority*
CAAS	Cybercrime-as-a-service.	*Cybercri-me-as-a-service*
Capacity building	Een netwerk opzetten van verantwoordelijke organisaties om de weerbaarheid van een land te vergroten op het vlak van cybersecurity en cybercrime.	
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart. Functie van een informatiesysteem om te controleren of de gebruiker een mens is. Bekende voorbeelden van CAPTCHA zijn dat de gebruiker een tekst op het scherm moet overtypen of kenmerken in foto's moet herkennen.	
Cbw	Cyberbeveiligingswet.	*Cyberbeveiligings-wet*
CASB	Cloud Access Security Broker.	

BEGRIP	BETEKENIS	ZIE OOK
Catfishing	Een social engineering techniek. Hierbij proberen oplichters persoonlijke gegevens van iemand te stelen via nagemaakte sociale netwerksites en datingsites. Bij die gegevens gaat het meestal om persoonlijke informatie, creditcardnummers of geld.	*Phishing*
CEH	Certified Ethical Hacker. Dit is een certificering voor professionals op gebied van cybersecurity, specifiek voor ethisch hacken.	
Censorship	Censuur. Informatie ontoegankelijk maken, of het onmogelijk maken om informatie te delen.	
CEO/CFO/CxO fraude	Vorm van fraude waarbij een aanvaller e-mails verstuurt aan een financiële afdeling zogenaamd uit naam van de CEO of CFO van een bedrijf. De aanvaller wil hiermee een medewerker van een financiële afdeling overtuigen of onder druk zetten om geld over te maken.	*Spear phishing*
CERT	Beschermde term (afkorting voor Computer Emergency Response Team) van Carnegie Mellon voor het eerste Computer Security Incident Response Team (CSIRT) ter wereld. Deze term mag onder bepaalde voorwaarden ook door andere CSIRT's worden gebruikt. Voorbeelden van CERT's in Nederland zijn het NCSC, Z-CERT en CERT-WM die verschillende sectoren ondersteunen.	*CSIRT*
Certificaat	1. Digitaal document dat aantoont dat een product, digitaal systeem of persoon is wie hij zegt dat hij is. Dit kan bijvoorbeeld worden gebruikt om een beveiligde verbinding tot stand te brengen. Een erkende instantie (Certificate Authority) geeft het document uit. 2. Een verklaring van een onafhankelijke instantie waarin staat dat een product, proces of persoon voldoet aan de eisen in het certificaat.	

BEGRIP	BETEKENIS	ZIE OOK
Certificate authority	Erkende instantie die digitale certificaten uitgeeft. Daarvoor stelt ze eerst vast dat de aanvrager is wie hij zegt te zijn.	
Certificatie schema	Systeem om een bepaald type producten, processen of diensten te beoordelen. Deze moeten voldoen aan bepaalde eisen, regels en procedures. Een certificeringssysteem staat in ISO/IEC 17000: 2004.	
Certificerende instelling	Instantie of instelling die zogeheten certificaten onder accreditatie mag uitgeven. Voorbeeld van zo'n certificaat is ISO 27001. De instelling moet voldoen aan internationale eisen. In Nederland beoordeelt de Raad voor Accreditatie of de instelling onafhankelijk en deskundig is.	
Certificering	Het proces waarbij een erkende instantie of persoon met een schriftelijk bewijs verklaart dat een persoon, product, systeem of dienst voldoet aan bepaalde eisen, zoals bijvoorbeeld beschreven in een internationale standaard.	
Chatham House Rule	Afspraak dat deelnemers de informatie die ze in een bijeenkomst delen bekend mogen maken aan anderen, zonder vermelding van de bron. De deelnemers mogen de informatie dus vrij gebruiken, maar ze mogen niet zeggen van wie de informatie komt.	
Chief Information Security Officer	De medewerker die verantwoordelijk is voor cybersecurity binnen een organisatie. Rol op strategisch niveau.	
CIA	Confidentiality, Integrity en Availability. De Nederlandse afkorting is BIV: Beschikbaarheid, Integriteit en Vertrouwelijkheid, waarbij de termen in een andere volgorde worden genoemd.	*Beschikbaarheid, Integriteit, Vertrouwelijkheid, BIV*

BEGRIP	BETEKENIS	ZIE OOK
CIEM	Cloud Infrastructuur Entitlement Management.	*Cloud Infrastructuur Entitlement Management*
CISM	Certified Information Security Manager. Dit is een certificering voor professionals in informatiebeveiliging.	
CISO	Chief Information Security Officer.	*Chief Information Security Officer*
CISSP	Certified Information System Security Professional. Dit is een certificering voor professionals in informatiebeveiliging.	
Classificatie	Beoordeling hoe gevoelig of belangrijk informatie of een systeem is. Dit is nodig om de juiste maatregelen te kunnen nemen om de informatie of het systeem te beschermen en ook het systematisch indelen in groepen of categorieën, volgens vastgestelde criteria. Bij security classificatie wordt vaak gebruik gemaakt van BIV: Beschikbaarheid, Integriteit en Vertrouwelijkheid.	
Click fraud	...	*Adware*
Closed source	Software waarvan de broncode door de auteurs niet wordt vrijgegeven.	
Cloud	Het toegankelijk maken van IT-diensten, zoals bijvoorbeeld hardware en software via een netwerk, meestal het Internet. Voorbeelden van Clouddiensten zijn Software-as-a-Service (SAAS), Platform-as-a-Service (PAAS) en Infrastructure-as-a-Service (IAAS).	

BEGRIP	BETEKENIS	ZIE OOK
Cloud access security broker	Een beveiligingsoplossing voor toepassingen in de cloud. Daarbij plaatst men een schakel tussen het bedrijfsnetwerk en de cloud. Dat levert de volgende voordelen op: - Men verkleint het aanvalsoppervlak - Men heeft een overzicht van welke applicaties men in de cloud men gebruikt. - Men beschermt de bedrijfsgegevens die worden uitgewisseld met de cloud - Men krijgt controle vanuit één centraal punt.	
Cloud based security	...	*Cloud security*
Cloud Detection and Response	Oplossing om beveiligingsrisico's in cloudomgevingen te kunnen signaleren, identificeren, analyseren en aan te pakken.	
Cloud computing	Een model waarbij op aanvraag computercapaciteit van anderen wordt gebruikt. De capaciteit deelt men bijvoorbeeld voor servers, opslag, applicaties en diensten.	
Clouddienst	IT-diensten die via het Internet worden aangeboden. De gebruiker schaft geen hardware en software aan, maar betaalt voor het daadwerkelijke gebruik van één of meerdere diensten die op de infrastructuur van een cloudaanbieder draaien. Clouddiensten worden vaak in drie categorieën verdeeld: Software as a Service (SaaS), Platform as a Service (PaaS) en Infrastructure as a Service (IaaS). De scheidslijnen tussen die drie zijn niet altijd even scherp te trekken. De grootste cloudaanbieders zijn actief op de drie genoemde lagen en zijn dus verticaal geïntegreerd.	
Cloud security	1. De beveiliging van alle data, applicaties en het netwerk van apparaten in een cloudtoepassing. 2. Cybersecuritydiensten die een aanbieder vanuit de cloud aan een klant levert.	

BEGRIP	BETEKENIS	ZIE OOK
Code assessment	...	*Code audit*
Code audit	Een analyse van de broncode van een programma, met als doel om zwakke plekken te vinden. Dit gebeurt volgens een norm die men vooraf objectief heeft vastgesteld. Een code audit voert men voor een groot deel handmatig uit.	
Code execution	Actie waarbij iemand ongewild programmacode laat uitvoeren door een computer of programma. Doet iemand dat op afstand, dan heet dat remote code execution.	
Code injection	Aanval op een onveilige plek in een applicatie. Daarbij verandert de aanvaller iets in de code van het systeem waardoor het programma anders werkt dan voorheen. Voorbeeld van een code injection is SQL-injection.	
Code review	Analyse van de broncode van een programma. Het doel is onder meer om zwakke plekken te vinden. Men zoekt voor een groot deel handmatig en niet aan de hand van een uitputtende lijst van kwetsbaarheden. De aanpak berust meer op expertise van de uitvoerder.	
Command execution	Aanval waarbij men door zwakheden in een website direct opdrachten kan geven aan het systeem waar de website op draait. Met die opdrachten kan een aanvaller het systeem dingen laten doen die niet de bedoeling zijn.	
Command-and- control server	De machine die een aanvaller gebruikt om commando's te sturen naar systemen waarin hij heeft ingebroken. Bijvoorbeeld als hij een DDoS-aanval wil doen of een bot in een botnet wil aansturen.	
Compartimentering	...	*Segmentering*

BEGRIP	BETEKENIS	ZIE OOK
Compliance	De activiteiten die men uitvoert om als persoon of organisatie te voldoen aan bepaalde eisen. Dat kan een wet zijn, maar ook eisen uit de branche of regels van de eigen organisatie.	
Compromitteren	Een woord dat vaak wordt gebruikt in combinatie met de woorden netwerken of systemen. Met compromitteren wordt een succesvolle aanval op een netwerk of systeem bedoeld.	
Computervredebreuk	Met opzet inbreken in een digitaal systeem, terwijl dat van de wet niet mag.	
Confidentiality	Vertrouwelijkheid, vooral van data en informatie. Data en informatie zijn alleen bedoeld voor specifieke ontvanger(s).	
Configuratie	De manier waarop hardware en software is ingesteld voor het gewenste doel.	
Consent	Toestemming. Eén van de peilers van het dataprotectierecht en privacyrecht. Data mogen niet verwerkt worden, tenzij de persoon waarover de data gaan, toestemming heeft gegeven. Deze toestemming is expliciet, geïnformeerd, vrijwillig en ondubbelzinnig.	
Containeriseren	Een manier om applicaties los te laten werken van een besturingssysteem of andere applicaties. In een container zit de applicatie zelf en alles wat nodig is om de applicatie te laten werken. Het voordeel van containeriseren is dat men de applicatie makkelijk kan verplaatsen naar een andere omgeving. Net als met containers op een schip.	
Control	...	*Beheersmaatregel*

BEGRIP	BETEKENIS	ZIE OOK
Control framework	Principes, uitgangspunten, manieren van denken, processen en afspraken die een organisatie gebruikt voor het omgaan met veiligheidsrisico's.	
Convention on Cybercrime	Convention on Cybercrime van de Council of Europe. Internationaal verdrag dat tot doel heeft om de wetten van de aparte landen op het gebied van cybercrime op elkaar aan te laten sluiten. Het verdrag beoogt landen samen te laten werken op dit terrein en kennis uit te laten wisselen op het gebied van opsporingstechnieken. 63 landen hebben dit verdrag geratificeerd, en nog eens 4 landen hebben het getekend.	
Cookie	Een klein bestand dat door een website op de harde schijf van een computer van een bezoeker wordt gezet. In een cookie staat informatie over het bezoek aan de website, zoals de naam, datum en tijd. De website bewaart de informatie om die later te kunnen gebruiken voor andere doeleinden zoals analyses en marketing.	
Coordinated vulnerability disclosure	Coordinated vulnerability disclosure is de praktijk van het gecoördineerd melden van aangetroffen beveiligingslekken. Hierbij worden afspraken gehanteerd die doorgaans neerkomen op dat de melder de ontdekking niet deelt met derden totdat het lek verholpen is, en de getroffen partij geen juridische stappen tegen de melder zal ondernemen. Voorheen werd dit responsible disclosure genoemd.	*Responsible disclosure*
COSO	1. Chief Operational Security Officer. Equivalent van de Chief Information Security Officer binnen een operationele productie omgeving. 2. Een managementmodel dat is ontwikkeld door Committee of Sponsoring Organizations of the Treadway Commission (COSO).	

BEGRIP	BETEKENIS	ZIE OOK
CRA	Cyber Resilience Act.	*Cyber Resilience Act, Verordening Cyber-weerbaarheid*
Cracker	Een aanvaller die met kwade bedoelingen in een computernetwerk inbreekt, bijvoorbeeld omdat hij gegevens wil stelen of een netwerk wil beschadigen.	*Hacker*
Cracking	Met kwade bedoelingen in een computernetwerk inbreken, bijvoorbeeld om gegevens te stelen of een netwerk te beschadigen.	*Hacken*
Credential harvesting	Het aanvallen van een organisatie om op illegale wijze inloggegevens (van werknemers) te verkrijgen.	
Credentials	De gegevens waarmee een gebruiker of ander digitaal systeem bij een digitaal systeem kan aantonen dat hij is wie hij zegt dat hij is. Bijvoorbeeld een gebruikersnaam in combinatie met een wachtwoord of een via SMS opgestuurde code.	
Credential Stuffing	Een methode waarbij aanvallers lijsten met gecompromitteerde gebruikersnamen en/ of wachtwoorden gebruiken om een systeem binnen te dringen.	
Criminele actor	Crimineel die aanvallen pleegt met economische of financiële motieven.	
Crisismanagement	Gecoördineerde activiteiten om een organisatie te leiden, te sturen en te controleren met betrekking tot crises. Een crisis is een abnormale of buitengewone gebeurtenis of situatie die een organisatie of gemeenschap bedreigt en een strategische, adaptieve en tijdige reactie vereist om de levensvatbaarheid en integriteit te behouden.	

BEGRIP	BETEKENIS	ZIE OOK
Crisisoefening	Het oefenen van het reactievermogen van een organisatie bij een groot cyberincident.	
Cristalbox Test	...	*Whitebox test*
Critical infrastructure	...	*Kritieke infrastructuur*
Cross site request forgery	Als een aanvaller een gebruiker naar een andere webpagina lokt, kan hij namens die gebruiker iets doen op die webpagina of in het account op die website. Bijvoorbeeld het wijzigen van een wachtwoord of een e-mailadres.	
Cross site scripting	Veel voorkomende fout in een website waardoor een aanvaller toegang kan krijgen tot gegevens of functionaliteit die niet voor hem bedoeld is.	
Crypto	1. Cryptografie 2. Cryptosleutels	*Cryptografie, cryptovaluta*
Crypto mule/Crypto-ezel	Iemand die zijn account van een online cryptovaluta portemonnee beschikbaar stelt aan criminelen. Criminelen gebruiken dit soort accounts om er geld op te laten storten dat ze hebben gestolen en deze vervolgens om te wisselen naar cryptovaluta.	
Cryptografie	Informatie omzetten in een code zodat een ander het niet kan lezen. Dit doet men als men gevoelige informatie veilig wil bewaren of versturen. Meestal bestaat cryptografie uit een algoritme voor versleutelen en ontsleutelen en één of meerdere sleutels.	
Cryptojacking	De rekenkracht van een computer van iemand anders gebruiken om er cryptovaluta mee te maken. Die ander weet hier niets van. Het maken van cryptovaluta wordt ook ‘minen’ genoemd.	

BEGRIP	BETEKENIS	ZIE OOK
Cryptomining	Alle transacties in een blockchain verzamelen, controleren en verwerken. Dit gebeurt om dubbele uitgaves op te sporen.	
Cryptovaluta	Verzamelnaam voor digitale munteenheden die cryptografische berekeningen gebruiken als echtheidskenmerk en voor transacties.	
Crystal box test	...	*Black box test*
CSIRT	Computer Security Incident Response Team. Een team van deskundigen dat cyberincidenten oplost. Dit kan een intern team zijn, maar ook een extern ingehuurd team.	*CERT*
CSMS	Cyber Security Management System. Dit systeem houdt bij of de maatregelen voor cybersecurity goed werken.	*ISMS*
CSRF	Cross Site Request Forgery.	*Cross Site Request Forgery*
CVD	Coordinated Vulnerability Disclosure.	*Coordinated vulnerability disclosure*
CVE	Common Vulnerabilities and Exposures. Een openbare lijst van bekende zwakke plekken in software. De lijst is te vinden via https://cve.mitre.org.	
CVSS	Common Vulnerability Scoring System. Systeem om een score te geven aan een zwakke plek in software. Hoe hoger de score, hoe zwakker de plek. Een organisatie kan deze score gebruiken om te bepalen welke zwakke plekken ze als eerste gaat oplossen. Meer informatie over het scoresysteem is te vinden via https://www.first.org/cvss/.	

BEGRIP	BETEKENIS	ZIE OOK
CWE	Common Weakness Enumeration. Een openbare lijst met bekende soorten zwakke plekken in software. De lijst is te vinden via https://cwe.mitre.org/.	
Cyber	Iets wat te maken heeft met digitale informatie en systemen die verbonden zijn met het Internet.	
Cyberaanval	Moedwillige activiteit van een actor die is gericht op het met digitale middelen verstoren van één of meer digitale processen.	
Cyberaanval	Een gerichte aanval in of via cyberspace. Doelwitten kunnen zijn: personen, groepen, bedrijven en organisaties, overheden, andere landen.	
Cyberbeveiligingswet	De Cyberbeveiligingswet is de Nederlandse uitwerking van de Europese NIS2-richtlijn. De NIS2-richtlijn beoogt de cyberveiligheid in de Europese Unie naar een hoger gemeenschappelijk niveau te brengen door de digitale weerbaarheid van essentiële en belangrijke entiteiten in de lidstaten te versterken. Risicomanagement en incidentmanagement zijn belangrijke onderwerpen in de Cbw.	*NIS2, Wbni, Incident-management, Risicomanagement*
Cyberattack	...	*Cyberaanval*
Cyberbullying	Pesten op Internet.	

BEGRIP	BETEKENIS	ZIE OOK
Cybercrime	Hierbij kan onderscheid worden gemaakt tussen cybercrime in enge zin (computer-focused) en cybercrime in ruime zin (computer-assisted en computer-enabled). • Computer-focused crime: ICT is hierbij het doelwit van aanvallen met behulp van ICT. Voorbeelden zijn hacking, DDoS-aanvallen en ransomware. • Computer-assisted crime: criminaliteit die voorheen analoog, maar nu hoofdzakelijk digitaal wordt gepleegd. Bijvoorbeeld CEO-fraude. • Computer-enabled crime: analoge criminaliteit die alleen maar in de fysieke wereld kan bestaan, maar waarvan delen van de modus operandi ondersteund worden door ICT. Zo kunnen drugs wel digitaal verhandeld worden, maar niet digitaal gesmokkeld of geconsumeerd. In toenemende mate zijn zo alle vormen van criminaliteit in zekere zin computer-enabled. Alle vormen van cybercrime kunnen een meer of minder geavanceerd karakter hebben.	*Cybercriminaliteit, Cybercrime-as-a-service*
Cybercrime-as-a-service	Een omvangrijke online cybercriminele dienstverlening waarbij vrijwel elke stap voor het plegen en het beschermen van cybercrime verhandeld wordt.	
Cybercriminaliteit	...	*Cybercrime, Cybercrime-as-a-service*
Cyber defense	Het hebben van middelen om cyberaanvallen af te slaan. Bijvoorbeeld strategische of militaire middelen. Term wordt met name gebruikt in de context van nationale veiligheid.	

BEGRIP	BETEKENIS	ZIE OOK
Cyberdiplomatie	Het onderhouden van geopolitieke relaties met andere staten en hun representanten ten aanzien van statelijk gedrag in cyberspace.	
Cyberhygiene	Wat minimaal nodig is om een digitaal systeem te beveiligen. Bijvoorbeeld het automatisch vergrendelen van een digitaal systeem als het een bepaalde tijd niet gebruikt wordt, meerfactorauthenticatie, het maken van back-ups, het gebruik van anti-virus software, het aansturen op veilig gedrag van personeel en deze trainen.	
Cyberincident	Verstoring van één of meer (digitale) processen. Verzamelbegrip voor cyberaanval en uitval.	
Cyber kill chain	Een model waarin staat welke stappen een aanvaller zet bij een cyberaanval. Het bekendste voorbeeld van een cyber kill chain is de Lockheed Martin Kill Chain.	
Cyber norms	Internationale afspraken op het terrein van gedrag van landen in cyberspace. Bijvoorbeeld over het gebruik van cyber defense, cyber offense of capacity building.	
Cyber offense	Het hebben van middelen om cyberaanvallen uit te voeren. Bijvoorbeeld strategische of militaire middelen. Deze term wordt met name gebruikt in de context van nationale veiligheid.	
Cyber-physical system	Digitaal systeem dat niet enkel data verwerkt maar ook een interactie heeft met de fysieke wereld.	
Cyber resilience	...	*Cyber-weerbaarheid*

BEGRIP	BETEKENIS	ZIE OOK
Cyber Resilience Act	Europese wet die tot doel heeft om consumenten en bedrijven te beschermen die producten of software met een digitale document kopen of gebruiken. Deze wet legt verplichte beveiliging op aan dit soort producten en of software en legt de plicht bij fabrikanten om veilige producten te garanderen gedurende de levensduur van een apparaat of software. De CRA treedt in 2025 in werking. De wet dwingt bedrijven om cybersecurity niet langer als bijzaak, maar als kernonderdeel van hun productontwikkeling te beschouwen. Er is een overgangsperiode van 24 maanden ingevoerd zodat producten en processen kunnen worden aangepast aan de nieuwe eisen.	*Europese wet- en regelgeving, Verordening Cyber-weerbaarheid*
Cybersabotage	Een actor tast opzettelijk en langdurig de beschikbaarheid van digitale diensten, processen of systemen aan (door in extreme gevallen de vernietiging daarvan). Dit is mogelijk door voorbereidingshandelingen daartoe, door zich toegang te verschaffen tot en zich in te nestelen in ICT- en/of OT-systemen. Voorbereidingshandelingen kunnen lang duren (maanden of jaren), vereisen specifieke technische kennis en zijn voornamelijk afkomstig vanuit statelijke actoren. Digitale sabotage kan ingrijpende gevolgen hebben.	
Cyberschaamte	Cyberwoord van 2022. Het lijkt logisch dat je een incident meteen meldt en hulp zoekt, maar dat blijkt in de praktijk vaak niet het geval. Vaak schamen mensen zich voor hun fout en dan maakt het niet uit of ze werken in de boardroom of in de kantine, of het politici zijn of ambtenaren. Iedereen kan slachtoffer worden van een cybersecurity incident. Daarover hoef je je dus niet te schamen! Niet omdat je niet oplette, bang bent voor imagoschade of gewoonweg de kennis niet had.	

BEGRIP	BETEKENIS	ZIE OOK
Cybersecurity	Het geheel aan maatregelen om relevante risico's tot een aanvaardbaar niveau te reduceren. De maatregelen kunnen zijn gericht op het voorkomen van cyberincidenten en - wanneer cyberincidenten zich hebben voorgedaan - deze te ontdekken, schade te beperken en herstel eenvoudiger te maken. Wat een aanvaardbaar niveau is, is de uitkomst van een risico-afweging.	
Cyberspace	Een ecosysteem van digitale (genetwerkte) technologieën, waarbinnen allerlei verschillende actoren informatie creëren, opslaan, uitwisselen, gebruiken en delen.	
Cyberspionage	Een actor tast de vertrouwelijkheid aan van informatie door die te kopiëren of weg te nemen. De onderliggende motivatie is het verkrijgen van gevoelige of geclassificeerde gegevens of intellectueel eigendom. Digitale spionage vindt primair plaats door statelijke actoren.	
Cyberterrorisme	Terroristische activiteiten die men digitaal uitvoert. Bijvoorbeeld het beschadigen of uitschakelen van belangrijke informatienetwerken via Internet.	
Cybervandaal	...	*Scriptkiddie*
Cyberveilig	...	*Cyber-weerbaarheid*

BEGRIP	BETEKENIS	ZIE OOK
Cyberverzekering	Een verzekering die uitkeert bij financiële schade die ontstaat als gevolg van een datalek, virus, hack of andere cyberaanval. De verzekering keert uit voor schade bij de organisatie zelf, maar ook voor schade die ze aan anderen moeten vergoeden. Daarnaast bieden de meeste verzekeraars ook dekking aan in de vorm van diensten, zoals assistentie, forensische expertise, herstel, juridische ondersteuning en/of communicatie. De uitkering hangt af van de dekking en polisvoorwaarden.	*Europese wet- en regelgeving*
Cyberwarfare	Digitale (genetwerkte) technieken die staten gebruiken om de systemen van andere staten of organisaties aan te vallen. Vaak met een militair of strategisch doel.	
Cyberweerbaarheid	Het vermogen om (relevante) risico's tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen om cyberincidenten te voorkomen en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken. Wat een aanvaardbaar niveau van weerbaarheid is, is de uitkomst van een risico-afweging en daarop gebaseerde politieke en/of bestuurlijke keuzen als het gaat om (onder andere) de juiste technische, procedurele of organisatorische maatregelen te kiezen. Andere manieren zijn bijvoorbeeld wetgeving, subsidieverlening, scholing om gebruikers te bekwamen in veilig gedrag, voorlichtings- en bewustwordingscampagnes, samenwerking tussen partijen en normerende kaders voor digitalisering van diensten en processen en ontwerp van systemen.	
DANE	Op DNS gebaseerde authenticatie van entiteiten.	

BEGRIP	BETEKENIS	ZIE OOK
Dark net	...	*Dark web*
Dark web	Een besloten deel van het Internet dat men niet vindt met normale browsers en zoekmachines. Het staat vooral bekend als een plek waar criminelen hun zaken doen.	
DAST	Dynamic Application Security Testing. Categorie van software-tools die een applicatie testen op kwetsbaarheden, terwijl deze in werking is.	
Data breach	Engelse term voor datalek.	*Datalek*
Data leak prevention	Een tool die mogelijke datalekken/data-exfiltratie detecteert en voorkomt deze door gevoelige gegevens te bewaken, te detecteren en te blokkeren terwijl ze in gebruik zijn op het endpoint van de gebruiker (Data in use), over het netwerk wordt getransporteerd (Data in motion) en in opslag is (Data at rest).	*Data loss prevention, Data exfiltratie*
Data loss prevention	Voorkomen dat specifieke informatie ongeoorloofd wordt verzonden.	
Data protection	Gegevensbescherming. Het geheel van wettelijke rechten en plichten over het opslaan, gebruiken en delen van (persoonlijke) data.	
Data Protection Impact Assessment	Engelse benaming voor de gegevensbeschermingseffectbeoordeling. Een analyse van de impact van een (voorgenomen) verwerkingsactiviteit op de privacy en persoonlijke levenssfeer personen. Voor specifieke gevallen is deze verplicht.	*Gegevens-beschermings-effectbeoordeling*

BEGRIP	BETEKENIS	ZIE OOK
Datadiode	Netwerkapparaat dat ervoor zorgt dat netwerkverkeer tussen interfaces maar in één richting geïnitieerd en verzonden kan worden. De datadiode kan voor verschillende toepassingen gebruikt worden zoals het scheiden van (geclassificeerde)netwerken om datalekken tegen te gaan maar ook om data uit vanuit een industriële omgeving (OT) te sturen naar IT-omgevingen.	
Datalek	Een gangbare term voor een cyberincident, veelal gebruikt in relatie tot persoonsgegevens. In de context van de Algemene Verordening Gegevensbescherming is een datalek een leken-term voor 'inbreuk in verband met persoonsgegevens', inhoudende een incident waardoor de integriteit, beschikbaarheid en/of vertrouwelijkheid van persoonsgegevens worden aangetast. Voorbeelden zijn ransomware aanvallen, of een e-mail met alle geadresseerden in het "To" – veld.	*Algemene Verordening Gegevens-bescherming*
Dataleverancier	Een dataleverancier levert gegevens van slachtoffers aan fraudeurs. Deze gegevens kunnen verkregen zijn uit bestaande en nieuwe datalekken of de dataleverancier steelt zelf gegevens. De gegevens worden voornamelijk verhandeld via het Darkweb en via (veelal besloten) sociale media groepen binnen Facebook en Telegram.	
DDoS	Distributed Denial of Service aanval.	*Distributed Denial of Service aanval*
Deception technology	Technologie voor het ontdekken van aanvallers in digitale systemen. Bijvoorbeeld door aanvallers te lokken en misleiden met nepinformatie en het gebruiken van die informatie om hen te ontdekken.	
Decryptie	...	*Ontsleutelen, Cryptografie*

BEGRIP	BETEKENIS	ZIE OOK
Deep fake	Synthetische media waarbij de beeltenis of de stem van een persoon in een bestaand audiobestand, beeld of video wordt vervangen door de beeltenis van iemand anders.	
Deep fake defence	Technologien en technieken die worden ingezet om deep-fake video's en audio's te detecteren en tegen te gaan.	
Deep learning	Een toepassing van machine-learning waarbij meerdere lagen neurale netwerken gebruikt worden om machines (computers) te ontwerpen die kunnen leren van patronen in data.	
Deep packet inspection	Algemene naam voor technieken waarmee men in detail gegevens analyseert die via netwerken verspreid worden. Men onderzoekt hierbij meer dan alleen het adres van de afzender en de ontvanger. Doel is om zo meer bedreigingen te kunnen opsporen.	
Deep web	Het deel van Internet waar geen rechtstreekse verwijzingen naar toe zijn vanaf websites.	
Defacement	Digitale bekladding. Een actor verandert de inhoud op de webpagina's of voegt nieuwe webpagina's toe. Soms laat de actor bij de uitvoering van een defacement malware achter, waardoor bezoekers van de website besmet kunnen raken. Een defacement tast dus de integriteit van webpagina's aan door foutieve informatie te verstrekken of kan, in het geval van de plaatsing van malware, leiden tot een vervolgaanval bij bezoekers. Defacements worden veelal uitgevoerd door hacktivisten, waarbij zij de inhoud van websites veranderen in overeenstemming met de boodschap van de betreffende groep.	

BEGRIP	BETEKENIS	ZIE OOK
Defense-in-Depth	Meerlaagse/gelaagde beveiliging: achter elkaar schakelen van beveiligingsmaatregelen, zodat als er één faalt, de anderen een aanval alsnog tegenhouden.	
Defensive capabilities	...	*Cyber defense*
Denial of Service aanval	De benaming voor een type aanval die een bepaalde dienst (bijvoorbeeld een website) niet beschikbaar maakt voor de gebruikelijke afnemers. Bij websites wordt meestal een Distributed Denial of Service (DDoS) aanval uitgevoerd.	*Distributed Denial of Service aanval*
Denylisting	...	*Blacklisting*
Desinformatie	Misleidende of afleidende informatie die men met opzet verspreidt.	*Nepnieuws*
DevSecOps	Een benadering van softwareontwikkeling die rekening houdt met de veiligheid vanaf het begin van het ontwikkelingsproces en tot het einde van de levenscyclus van een product. Het is een combinatie van de woorden ontwikkeling, beveiliging en operaties.	*Shift-left*
Digitaal proces	Een proces dat geheel of gedeeltelijk wordt uitgevoerd door de complexe en onderling samenhangende interactie tussen mensen en vele componenten van hardware, software en/of netwerken. Volledig geautomatiseerde processen, zoals procesbesturingssystemen, vallen ook onder het begrip.	
Digitaal risico	De kans dat een cyberincident zich voordoet en de impact daarvan, beide in relatie tot het actuele niveau van weerbaarheid.	
Digital domain	...	*Cyberspace*
Digitale aanval	...	*Cyberaanval*

BEGRIP	BETEKENIS	ZIE OOK
Digitale handtekening	Een elektronische variant van de handgeschreven handtekening. De digitale handtekening bestaat uit elektronische gegevens en hoort bij een digitaal document. Zo kan men met cryptografische technieken vaststellen of het document niet aangepast is, en waar het vandaan komt.	*Hashing, PKI, certificaat*
Digitale ruimte	...	*Cyberspace*
Digitale sabotage	...	*Cybersabotage*
Digitale soevereiniteit	De mate waarin landen en staten in staat zijn om hun eigen data, informatiesystemen en technologische infrastructuur onder controle te hebben en te houden.	
Digitale spionage	...	*Cyberspionage*
Digitale veiligheid	Het ongestoord functioneren van informatie- en procesbesturingssystemen, daardoor verwerkte en opgeslagen informatie en daarvan afhankelijke diensten en processen. De focus in het CSBN ligt op digitale veiligheid van de digitale ruimte, vitale processen en andere voor het functioneren van de (Nederlandse) maatschappij cruciale sectoren, digitale diensten en processen.	

BEGRIP	BETEKENIS	ZIE OOK
Digitalisering	Een breed begrip dat duidt op een veelheid van (nieuwe) digitale technologieën en de impact daarvan op onze wereld. Een voorbeeld van een digitale technologie is kunstmatige intelligentie, dat duidt op machines of systemen die zichzelf steeds intelligenter maken door voortdurend hun omgeving te analyseren en actie te ondernemen om specifieke doelen te bereiken. Digitalisering gaat over de impact die deze en andere technologieën hebben op bestaande processen, ons gedrag, organisaties en instituties. Digitalisering drijft op drie kurken: steeds meer data, een steeds grotere rekenkracht en steeds sterkere onderlinge verbondenheid van apparaten.	
Digital Trust Center	Onderdeel van het ministerie van Economische Zaken dat als doel heeft om ondernemers te helpen om veilig digitaal te ondernemen. De wettelijke basis is de Wet bevordering digitale weerbaarheid bedrijven (Wbdwb).	*DTC, Wet bevordering digitale weerbaarheid bedrijven*
Disaster recovery plan (DRP)	Plan waarin staat hoe een digitaal systeem moet herstellen na een grote storing.	*Business continuity plan*
Disk image	...	*Forensic image*
Distributed Denial of Service aanval	Een aanval op de capaciteit van onlinediensten of de ondersteunende servers en netwerkapparatuur. Het resultaat van deze aanval is dat digitale diensten slecht of helemaal niet meer bereikbaar zijn voor medewerkers of klanten.	

BEGRIP	BETEKENIS	ZIE OOK
DIVD	Dutch Institute for Vulnerability Disclosure.	*Dutch Institute for Vulnerability Disclosure*
DKIM	Domain Keys Identified Mail. DKIM is een techniek waarmee e-mailberichten kunnen worden gewaarmerkt. Het gebruik van DKIM verkleint de kans op misbruik van e-mailadressen doordat ontvangers betrouwbaar echte e-mails van phishingmails of spam kunnen onderscheiden. Ook kunnen ontvangers controleren of de inhoud van de e-mail door derden is gemanipuleerd.	
DLP	Data Loss Prevention.	*Data loss prevention*
DMARC	Domain-based Message Authentication, Reporting and Conformance. Techniek om valse e-mails of SPAM tegen te gaan. DMARC geeft de verzendende partij de mogelijkheid om beleid te formuleren over wat er met e-mails moet gebeuren wanneer de echtheidswaarmerken niet kloppen. Het geeft ook rapportagemogelijkheden voor legitieme en niet-legitieme uitgaande e-mailstromen.	
DMZ	Demilitarized Zone. Een apart gebied in een computernetwerk dat het interne netwerk scheidt van het Internet. Alle onderdelen van het netwerk die contact hebben met externe netwerken, zitten bij elkaar in dit gebied.	*Zero trust*
DNS	Het Domain Name System is het systeem dat Internetdomeinnamen koppelt aan IP-adressen en omgekeerd. Verder vermeldt een DNS-record onder meer hoe e-mails aan dat domein afgehandeld moeten worden.	*Domeinnaam, IP-adres*

BEGRIP	BETEKENIS	ZIE OOK
DNSSEC	Domain Name System Security Extensions. Beveiligingsoplossing om een aanval op een domeinnaam tegen te gaan. In vaktaal heet dit DNS-spoofing. Bij zo'n aanval stuurt men bijvoorbeeld een bezoeker van een bepaalde website door naar een valse website. Een domeinnaamhouder kan met DNSSEC een digitale handtekening toevoegen aan DNS-informatie. Met deze handtekening kan een Internetgebruiker onzichtbaar en volledig automatisch de inhoud en de ontvangen DNS-informatie valideren. Hierdoor is met grote waarschijnlijkheid vast te stellen dat het antwoord van de DNS onderweg niet is gemanipuleerd door derden.	
Doelwit	De digitale dienst of organisatie of het digitale proces of systeem waar een actor zich op richt met een cyberaanval.	
Domeinnaam	Een unieke naam op Internet. Meestal geldt een domeinnaam voor websites, maar men kan ook een domeinnaam aanvragen voor een persoonlijk mailadres.	*IP-adres*
Domotica	Technologie en diensten die processen in en rond een gebouw automatiseren.	*Internet of Things, Toezichthoudende domotica*
DORA	Operations Resilience Act. Sinds januari 2023 is de DORA van kracht. Dit is een Europese verordening die tot doel heeft dat financiële organisaties hun IT-risico's beter gaan beheersen en daarmee weerbaarder worden tegen cyberdreigingen.	*Europese wet- en regelgeving, NIS2*
DoS	Denial of Service.	*Denial of Service aanval*

BEGRIP	BETEKENIS	ZIE OOK
Double Extortion	Bestanden of systemen van het slachtoffer zijn versleuteld: de sleutel wordt tegen betaling aangeboden. Naast versleuteling worden gevoelige gegevens van het slachtoffer buitgemaakt, betaling moet voorkomen dat ze gelekt worden.	*Single Extortion, Triple Extortion, Quadruppel Extortion*
Doxing/Doxxing	Het proces waarbij vertrouwelijke informatie over een persoon of organisatie publiek wordt gemaakt. Dit gebeurt doorgaans via het Internet. Deze informatie wordt verkregen via open bronnen, social engineering of via (vaak ongeautoriseerde) toegang tot gesloten systemen. De doeleinden waarvoor doxing kan worden toegepast zijn: shaming, afpersing of als ongevraagde hulp aan de opsporing.	
DPA	Afkorting voor Data Protection Authority. 1.De toezichthouder in een land die toeziet op naleving en handhaving van wet- en regelgeving op het terrein van privacy en gegevensbescherming. In Nederland is dit de Autoriteit Persoonsgegevens. Afkorting voor Data Processing Agreement, de Engelse term voor Verwerkersovereenkomst	*Autoriteit Persoons-gegevens, Verwerkers-overeenkomst*
DPI	Deep Packet Inspection.	*Deep packet inspection*
DPIA	Afkorting van Data Protection Impact Assessment, de Engelse benaming voor de gegevensbeschermingseffectbeoordeling.	*Privacy impact assessment*
DPO	Afkorting voor Data Protection Officer, de Engelse term voor Functionaris Gegevensbescherming.	*Functionaris Gegevens-beschermer, AVG*
Dreiging	Mogelijke schade die intentioneel veroorzaakt is. Een dreiging betreft een bedoeling om schade aan te richten.	*Risico, Gevaar*

BEGRIP	BETEKENIS	ZIE OOK
Dreigingsinformatie	Technische informatie over kwaadwillende actoren inclusief mogelijke persoonsgegevens (bijvoorbeeld IP-adressen) ten behoeve van monitoring en detectie.	
Dreigingslandschap	Een overzicht van alle mogelijke dreigingen voor digitale systemen, organisaties of sectoren.	
Drive-by download	Wanneer een website kwaadaardige bestanden op je computer plaatst, automatisch en zonder dat je het doorhebt.	
DSP	Digitale Service Provider. Een aanbieder die clouddiensten, onlinezoekmachinies en/of onlinemarktplaatsen aanbiedt.	
DSPM	Data Security Posture Management.	*Data Security Posture Management*
DTC	Digital Trust Center.	*Digital Trust Center*
Dual control	Uitgangspunt waarbij meerdere personen nodig zijn om 1 specifieke activiteit uit te voeren. Bijvoorbeeld: als iemand een kamer in wil, zijn er vingerafdrukken van 2 personen nodig.	
Dual use	Het feit dat dezelfde digitale (genetwerkte) technologie gebruikt kan worden voor zowel militaire als civiele doelen.	
Dumpster-diver	Iemand die vertrouwelijke informatie probeert te vinden door het afval van iemand te doorzoeken.	
Dutch Institute for Vulnerability Disclosure	Vrijwilligersorganisatie die scans uitvoert op het Internet naar bekende kwetsbaarheden in digitale systemen. Als ze deze vinden, maken ze een melding bij de organisaties waar ze zijn aangetroffen. De organisatie werkt wereldwijd. Ook leiden ze hackers op.	

BEGRIP	BETEKENIS	ZIE OOK
E-discovery	Grote aantallen elektronische data doorzoeken voor een bepaald doel. Meestal voor een juridisch onderzoek of een rechtszaak.	
E-mailspoofing	...	*Spoofing*
Edge device	Digitaal apparaat dat zich aan de buitenrand van een netwerk bevindt. Routers en firewalls zijn hiervan voorbeelden.	
EDR	Endpoint Detection and Response.	*Endpoint detection and response*
Encryptie	...	*Versleutelen, Cryptografie*
End-of-life	Het moment dat een leverancier de software of hardware niet meer ondersteunt. Meestal voert hij dan geen updates of andere aanpassingen meer uit.	*Patch, Update*
Endpoint detection and response	Software die computers, laptops en vergelijkbare digitale apparaten beschermt tegen kwaadaardige software. Deze beschermende software zoekt naar deze software op basis van kenmerken van al bekende kwaadaardige software of van opvallend gedrag van nieuwe software in een digitaal systeem. Bij een incident gebruikt men deze software om specifieke zoekopdrachten uit te voeren op digitale systemen. Zo kan men dit incident helpen oplossen.	
Endpoint protection	Software die op een digitaal systeem (endpoint) draait en de bescherming van dat systeem voor z'n rekening neemt.	
ENISA	European Union Agency for Network and Information Security. Het Europees agentschap dat als doel heeft om netwerken en informatie binnen de EU beter te beveiligen.	

BEGRIP	BETEKENIS	ZIE OOK
EPP	Endpoint Protection Platform. Een verzameling van endpoint protection oplossingen die gezamenlijk de bescherming van een systeem voor hun rekening nemen.	*Endpoint protection*
Escrow	Een juridisch concept dat een overeenkomst beschrijft tussen een softwareleverancier en een onafhankelijk bedrijf om ervoor te zorgen dat de broncode van een computerprogramma vertrouwelijk wordt bewaard, bijvoorbeeld voor het geval dat de leverancier failliet gaat of bij een juridisch conflict.	
Ethical hacker	...	*Whitehat hacker*
Ethische hacker	...	*Whitehat hacker*
Europese richtlijnen	...	*Europese wet- en regelgeving*
Europese wet- en regelgeving	wet- en regelgeving in het digitale domein is afkomstig uit Europa. Veel van deze wetten en richtlijnen hebben een relatie met cybersecurity. Voorbeelden zijn de AVG, AI-ACT, DORA, NIS2, DMA en DSA. Zie ENISA.EU voor meer informatie.	*AVG, GDPR, NIS2, Cyberbeveiligings-wet, DORA*
Exfiltratie	Het naar buiten sluizen van vertrouwelijke informatie van een gehackte organisatie naar de systemen van de hacker of een ander gehackt systeem.	
Exfiltatration	...	*Exfiltratie*
Exploit	Software, gegevens of een opeenvolging van commando's die gebruikmaken van een kwetsbaarheid in software of hardware om ongewenste functies of gedrag te veroorzaken.	

BEGRIP	BETEKENIS	ZIE OOK
Exploitkit	Hulpmiddel om een aanval op te zetten door te kiezen uit kant-en-klare exploits, in combinatie met gewenste gevolgen en besmettingsmethode.	*Exploit*
Failsafe	Inrichting van een beveiligingssysteem die ervoor zorgt dat bij een storing of defect het beveiligde object in een veilige status blijft. Bijvoorbeeld: bij stroomuitval blijven alle buitendeuren gesloten.	
Fake news	...	*Nepnieuws*
False negative	De situatie dat een beveiligingssysteem iets hoort te zien en het niet opmerkt terwijl het wel gebeurt.	
False positive	De situatie dat een beveiligingssysteem iets opmerkt, bijvoorbeeld een aanval, terwijl er niets aan de hand is.	
FG	Functionaris Gegevensbescherming.	*Functionaris Gegevensbescherming*
Filteren & blokkeren	...	*Blokkeren & filteren*
Firewall	Hardware of software om computers en netwerken te beschermen tegen aanvallen. Een firewall bekijkt alles wat een netwerk in en uit gaat en blokkeert bepaald verkeer op het netwerk.	
Firmware	Software in een apparaat of onderdeel van hardware in een apparaat dat ervoor zorgt dat de hardware zijn werk doet. Vaak kan men firmware updaten.	

BEGRIP	BETEKENIS	ZIE OOK
Forensic image	Een exacte kopie van bijvoorbeeld een harde schijf, een USB-stick of het geheugen van een digitaal systeem. In de kopie staat alle informatie die nodig is om te achterhalen wat er op het origineel staat en heeft gestaan. Denk aan bestanden en mappen, soms ook als ze al verwijderd zijn. Beveiligingsbedrijven gebruiken deze kopie vaak voor onderzoek, en politie en openbaar ministerie gebruiken deze kopie vaak voor onderzoek in relatie tot een strafzaak.	
Forensisch onderzoek	Technisch sporenonderzoek op (forensische kopieën van) digitale systemen tijdens of na een aanval. De onderzoekers verzamelen en analyseren bewijsmateriaal en proberen zo vragen te beantwoorden over de aanval. Bijvoorbeeld wanneer en hoe de aanval heeft plaatsgevonden, welke informatie er is gestolen en wie er achter de aanval zat.	*Incident response*
Forward Proxy	...	*Proxy*
Functiescheiding	Uitgangspunt dat er verschillende personen nodig zijn om een serie van kwetsbare activiteiten uit te voeren. Dit zijn activiteiten die men eenvoudig kan misbruiken of een hoge mate van beveiliging vereisen. Bijvoorbeeld, een persoon geeft toestemming voor een nieuw account. Een ander maakt het account aan en weer een ander bepaalt de rechten die iemand krijgt. Zo kan niet één persoon alles zelf uitvoeren waardoor het risico op misbruik afneemt.	
Functionaris Gegevensbescherming	Een medewerker of externe persoon, die is aangewezen om de organisatie te adviseren over en toe te zien op de naleving van de AVG en dient als contactpunt voor de toezichthouder.	*AVG*

BEGRIP	BETEKENIS	ZIE OOK
Fysieke beveiliging	Maatregelen om te voorkomen of ontdekken dat iemand zich toegang kan verschaffen tot fysieke locaties en/of zich in de nabijheid van specifieke personen begeven waarbij deze toegang of nabijheid niet gewenst of toegestaan is.	*Cyberbeveiligings-wet*
Gap analyse	Analyse om te bepalen in hoeverre een systeem of organisatie voldoet aan de veiligheidseisen. En wat de organisatie eventueel nog moet regelen om aan alle eisen te voldoen.	
GDPR	General Data Protection Regulation.	*General Data Protection Regulation*
Gebruikersnaam	Naam waarmee een gebruiker op een digitaal systeem kan inloggen.	*Inlogcode*
Geheimhoudings-verklaring	Overeenkomst waarbij twee of meer partijen met elkaar afspreken om informatie geheim te houden. Ze delen die dus niet met anderen.	
Gegevensbescherming-seffectbeoordeling	Een analyse van de impact van een (voorgenomen) verwerkingsactiviteit op de privacy en persoonlijke levenssfeer van personen. Voor specifieke gevallen is deze verplicht.	*DPIA*
General Data Protection Regulation	General Data Protection Regulation. Algemene Verordening Gegevensbescherming (AVG) is de Nederlandse uitwerking van deze Europese regelgevingie die in Europa zorgt voor een geharmoniseerde bescherming van persoonsgegevens.	*AVG*
Gevaar	Mogelijke schade die veroorzaakt is zonder bedoeling.	*Risico, Dreiging*
Gijzelsoftware	...	*Ransomware*

BEGRIP	BETEKENIS	ZIE OOK
Gold team	Combinatie van een Red Team oefening, waarbij een aanval door een geselecterde threat actor realistisch wordt geëmuleerd, met een crisisoefening die voortbouwt op de crisis die door de Red Team oefening geënsceneerd is.	*Red team*
GRC	Governance, Risk and Compliance.	
Greybox test	Een penetratietest waarbij de tester al beperkte toegang heeft tot een computersysteem om de test mee te starten, bijvoorbeeld de inloggegevens van een gebruikersaccount op het systeem. Hiermee wordt een scenario gesimuleerd waarbij een aanvaller via social engineering technieken zich toegang heeft weten te verschaffen tot een account van een medewerker van de organisatie, bijvoorbeeld via phishing.	*Blackbox test*
Greyhat hacker	Iemand die met zijn handelen weliswaar soms ethische of juridische grenzen over gaat, maar geen kwade of criminele bedoelingen heeft, zoals een blackhat hacker.	*Hacker, Blackhat hacker, Whitehat hacker*
Grooming	Het proces waarbij een dader het vertrouwen wint van een ander (het slachtoffer) met het doel deze persoon seksueel te misbruiken door aanranding, verkrachting, seksuele uitbuiting, het produceren van kinderporno, ontvoering of mensenhandel.	
Hack	...	*Hacken*
Hacken	1. Actie om in of bij een computer, netwerk, hardware of software te komen. Als men dat ongevraagd of zonder geldige reden doet, is zo'n actie illegaal. 2. Het vinden van nieuwe toepassingen. Bijvoorbeeld tijdens hackathons, workshops waarin men met kleine groepjes creatieve oplossingen probeert te vinden voor diverse problemen.	

BEGRIP	BETEKENIS	ZIE OOK
Hacker	Iemand die systemen wil proberen te doorgronden puur en alleen om zijn of haar nieuwsgierigheid te bevredigen. Hackers willen graag weten hoe bepaalde zaken werken. Soms is het twijfelachtig hoe legaal bepaalde zaken zijn die een hacker uitvoert, zoals het inbreken in een digitaal systeem. Hacker is van oorsprong een neutrale term maar veel mensen gebruiken het woord hacker tegenwoordig om iemand mee aan te duiden die kwade bedoelingen heeft, zoals een crimineel.	*Hacken, Whitehat hacker, Blackhat hacker, Greyhat hacker*
Hacktivist	Samentrekking van de woorden hacker en activist: actor die uit ideologische motieven digitale aanvallen van activistische aard pleegt.	
Hall of Fame/Wall of Fame	Een lijst met namen van hackers die hebben meegeholpen om een computersysteem te beveiligen. Bijvoorbeeld door zwakke plekken in de beveiliging te vinden en die te melden bij de leverancier via coordinated vulnerability disclosure.	
Hardening	Niet gebruikte functies in hardware en software uitzetten of weghalen en de rechten van andere functies waar mogelijk beperken. Zo verkleint men het aanvalsoppervlak en daarmee het risico van aanvallen.	
Hash/Hashwaarde	...	*Hashing*
Hashing	Een methode om met een speciaal algoritme een unieke code te berekenen voor een bestand of een stuk tekst of andere informatie. Deze unieke code heet hash of hashwaarde en is een soort digitale vingerafdruk. SHA-2 en Bcrypt zijn veelgebruikte algoritmes. Men gebruikt bijvoorbeeld SHA-2 om te controleren of een bestand, tekst of informatie niet is aangepast.	

BEGRIP	BETEKENIS	ZIE OOK
Hertest	Vervolgtest om na te gaan of de zwakke plekken die men eerder bij een penetratietest heeft gevonden, inderdaad weg zijn.	
Heuristic detection	...	*Machine learning*
Honey token	Gegevens die een speciaal kenmerk hebben, zodat men kan nagaan wat ermee gebeurt als ze worden gestolen. Zo kan men bijvoorbeeld bij een datalek zien waar de gegevens naar toe zijn gegaan en wie daarbij betrokken waren.	
Honeypot	Een digitaal systeem dat met opzet niet goed beveiligd is. Het doel van dit systeem is om het te laten besmetten met software die een digitaal systeem wil aanvallen. Daarna kan men deze software analyseren.	*Deception technology*
Host	Een apparaat dat via Internet kan communiceren met een ander apparaat. Een host heeft een eigen hostnaam en IP-adres.	*Hostnaam, IP-adres*
Hostnaam	Een hostnaam is de naam van een digitaal systeem. Samen met het domein waar het systeem bij hoort vormt de hostnaam de unieke Fully Qualified Domain Name (FQDN). Beheerders kiezen voor veelgebruikte servers zoals websites of servers die mail versturen vaak hostnamen die gemakkelijk te onthouden zijn, zoals www of smtp. De FQDN is dan bijvoorbeeld www.google.nl of smtp.google.nl.	

BEGRIP	BETEKENIS	ZIE OOK
HTTPS	HyperText Transfer Protocol Secure. Beheerders van websites kunnen HTTPS gebruiken om bezoekers van hun website beter te beschermen. Het zorgt ervoor dat informatie die de bezoekers op de website opzoeken of invullen en die verstuurd moet worden over Internet, niet onderweg afgeluisterd kan worden. Bezoekers van een website kunnen een beveiligde verbinding met een website herkennen aan HTTPS in de URL (HTTPS://). De website-identiteitsknop (het hangslot) wordt in de adresbalk weergegeven zodra een bezoeker een beveiligde website bezoekt. Om de echtheid van een website te controleren moet een gebruiker naast het hangslot in de adresbalk ook kijken naar de domeinnaam. HTTPS is een uitbreiding van het HTTP-protocol.	
Human error	Menselijke fout. Menselijke fouten zijn een veelvoorkomende (deel)oorzaak van cybersecurity-incidenten. Er bestaan veel verschillende soorten menselijke fouten. Denk bijvoorbeeld aan nalatigheid, iets niet of verkeerd begrijpen, iets vergeten te doen, of een verkeerde handeling uitvoeren.	
Human factor	Menselijke factor. Als er iets misgaat in de cybersecurity, komt dat regelmatig ook door een menselijke factor: iemand maakt een fout. Vaak heeft deze persoon zelf niet door dat hij een fout maakt.	
Human risk management	De evolutie van security awareness & training. HRM omvat ook security awareness en het trainen van medewerkers, maar legt de nadruk op evidence-based handelen, meetbaarheid, en cyberveiligheid in de cultuur.	
Hunting	Een veelal handmatig proces waarin men in netwerkverkeer of op digitale systemen zoekt naar sporen van aanvallen die bestaande beveiligingsmaatregelen hebben omzeild.	

BEGRIP	BETEKENIS	ZIE OOK
IaC	Infrastructure as Code.	*Infrastructure as Code*
IACS	Industrial and Automation Control Systems. Verzameling netwerken, control systemen, SCADA systemen en andere systemen die kwetsbaar zijn voor cyberaanvallen.	
IAM	Identity en Access Management.	*Identity en access management*
ICS	Industrial Control System.	*Industrial control system, Proces-besturingssysteem*
Identificatie	Herkennen wie iets of iemand is.	
Identiteit	1. Die eigenschappen of karakteristieken die mensen of objecten uniek maken. 2. Dat wat mensen of objecten uniek identificeerbaar maakt.	
Identiteitsfraude	Vorm van bedrog waarbij iets of iemand zich voordoet als iemand anders. Bijvoorbeeld spullen huren met de paspoortgegevens van iemand anders. Of iemands inloggegevens gebruiken om in te breken in een systeem.	
Identity broker	Bedrijf dat ervoor zorgt dat een programma of site verschillende manieren van aanmelden aanbiedt aan gebruikers. Bijvoorbeeld aanmelden met een Google-account of via Facebook.	
Identity en access management	Algemeen begrip voor twee systemen: - Identificatiesystemen: wie ben je? - Autorisatiesystemen: wat mag je?	

BEGRIP	BETEKENIS	ZIE OOK
Identity theft	Het stelen van persoonlijke data zodat men zich kan voordoen als de persoon waarop de data betrekking hebben. Zo kan een crimineel bijvoorbeeld iemands geld stelen, kan hij spullen kopen op iemands kosten, of criminele handelingen doen uit naam van die persoon.	*Identiteitsfraude*
IDS	Intrusion Detection System.	*Intrusion detection system*
Immutable	Back-up die niet overschreven kan worden.	*Back-up*
IIoT	Industrial Internet of Things. Internet of Things toegepast binnen een industriële omgeving.	*Internet of Things*
Incident	...	*Cyberincident*
Incident response	Het reageren op een cyberincident. Het is een (gestructureerde) aanpak op alle niveaus: operationeel, tactisch en strategisch. Incident response kan gezien worden als een soort brandweer bij een cyberincident.	
Indicator of compromise	Informatie die je kunt gebruiken om te kijken of iemand een aanval heeft uitgevoerd op één van je assets. De informatie bevat vaak kenmerken van een aanvaller, van een aanvalsmethode of van malware. Bijvoorbeeld, als men weet dat een bepaalde aanvaller zijn aanvallen vanuit een specifiek IP-adres uitvoert, dan kan je dat IP-adres gebruiken als indicator of compromise. Als je op je eigen digitale systemen sporen ziet van verbindingen met dat IP-adres, dan weet je dat die aanvaller misschien bij jou een aanval heeft proberen uit te voeren.	
Industrial control system	...	*Procesbesturings-systeem*

BEGRIP	BETEKENIS	ZIE OOK
Industriële controle systemen	...	*Industrial control system, Proces-besturingssysteem*
Informatiebeveiliging	Alles wat men doet om ervoor te zorgen dat men bij informatie kan komen wanneer men dat wil, dat de informatie klopt en dat de informatie niet bij anderen terecht komt. Het gaat daarbij vaak om een digitaal systeem, maar dat hoeft niet. Het gaat om maatregelen, procedures en processen die beveiligingsproblemen voorkomen, opsporen, onderdrukken en oplossen. Ontstaat er wel een probleem met de informatie? Dan zorgt informatiebeveiliging ervoor dat de gevolgen zoveel mogelijk beperkt worden.	*Cybersecurity*
Informatiebeveiligings-beleid	Algemene regels waarmee een organisatie beveiligingsrisico's zo klein mogelijk wil maken. Van tevoren spreekt men af hoe groot de beveiligingsrisico's mogen zijn.	
Informatiediefstal	Aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie.	
Informatiemanipulatie	Het opzettelijk wijzigen van informatie; aantasting van de integriteit van informatie.	
Information Security Officer	Persoon die verantwoordelijk is voor de uitwerking van de informatiebeveiliging van een organisatie. Er zijn verschillende niveau, zoals de CISO (strategisch) of de TISO (technisch).	
Info stealer	Een door de wetgever aangesteld, onafhankelijk en onpartijdig instituut dat toeziet op naleving van wet- en regelgeving door organisaties en (rechts)personen.	

BEGRIP	BETEKENIS	ZIE OOK
Initial access broker	Partij die illegaal toegang tot netwerken verkrijgt en deze toegang aan anderen verkoopt. Deze anderen gebruiken de gekochte toegang bijvoorbeeld voor de uitvoering van ransomware-aanvallen.	*Cybercrime-as-a-service*
Initieel risico	...	*Bruto risico*
Infrastructure as Code	Een benadering voor het beheren en inrichten van IT-infrastructuur door middel van machineleesbare configuratiebestanden in plaats van handmatige hardwareconfiguratie of interactieve configuratietools. IaC maakt het mogelijk om infrastructuur te definiëren en te beheren met dezelfde principes en processen die worden gebruikt voor softwareontwikkeling, zoals versiebeheer en testen.	
Inlogcode	Combinatie van gegevens die men nodig heeft om in een digitaal systeem of een ruimte te komen. Bijvoorbeeld een gebruikersnaam en wachtwoord.	*Wachtwoord, Gebruikersnaam*
Inlooptest	...	*Mystery guest bezoek*
Inputvalidatie	Geldigheidscontrole op invoergegevens. Een besturingstechniek bij het invoeren van gegevens, die wordt toegepast om invoergegevens, die onnauwkeurig, incompleet of onlogisch zijn, te herkennen.	
Insider	Een interne actor die met toegang tot systemen of netwerken van binnenuit een dreiging vormt, met als motief wraak, geldelijk gewin of ideologie. Een insider kan ook worden ingehuurd of opgedragen van buitenaf.	*Insider threat*

BEGRIP	BETEKENIS	ZIE OOK
Insider threat	Dreiging die zijn oorsprong heeft binnen de organisatie. Bijvoorbeeld doordat medewerkers, oud-medewerkers en leveranciers bij informatie kunnen komen. Of doordat zij weten hoe zaken zijn beveiligd. Er is sprake van een insider threat als zo'n medewerker, oud-medewerker of leverancier zijn positie misbruikt voor kwaadwillende activiteiten.	*Insider*
Integriteit	1. Bij data: juiste en volledige informatie, en verwerking van informatie. 2. Bij personen: de betrouwbaarheid van iemand. 3. Bij digitale diensten, processen of systemen: hun correcte werking.	
Intelligence	...	*Inlichtingen*
Internet of Things	Een netwerk van slimme apparaten, sensoren en andere objecten die (vaak verbonden met het Internet) gegevens verzamelen over hun omgeving, deze kunnen uitwisselen en op basis daarvan (semi-) autonome beslissingen of acties nemen die van invloed zijn op hun omgeving.	
Internet Protocol Security	Standaardafspraken over hoe men netwerkverkeer kan beveiligen. Hiermee kan worden gecontroleerd of informatie in het verkeer niet is aangepast en kunnen anderen de informatie onderweg niet afluisteren.	
Intrusion	In een informatiesysteem of computernetwerk gaan, terwijl men daar geen toestemming voor heeft.	
Intrusion detection	Alle data controleren die door een computer-netwerk gaan of die een digitaal systeem verstuurt en ontvangt en een waarschuwing geven als er iets niet in orde lijkt.	

BEGRIP	BETEKENIS	ZIE OOK
Intrusion prevention	Alle data controleren die door een computernetwerk gaan of die een digitaal systeem verstuurt en ontvangt en deze data tegenhouden als er iets niet in orde lijkt.	
IoC	Indicator of Compromise.	*Indicator of compromise*
IoT	Internet of Things.	*Internet of Things*
IP	Internet Protocol. Zorgt voor de adressering van Internetverkeer zodat het bij het beoogde doel aankomt.	*IP-adres*
IP-adres	Internet Protocol adres. Adres dat de bron of bestemming van verkeer op Internet aangeeft.	
IPS	Intrusion Prevention System. Een geautomatiseerd systeem dat intrusion prevention doet.	*Intrusion prevention*
IPSEC	Internet Protocol Security.	*Internet Protocol Security*
IPv4	Internet Protocol versie 4. IPv4 maakt communicatie van data tussen ICT-systemen binnen een netwerk, zoals Internet, mogelijk. De standaard bepaalt dat ieder ICT-systeem binnen het netwerk een uniek nummer (IPv4-adres zoals 192.168.1.2) heeft. Hierdoor kunnen ICT-systemen elkaar herkennen en onderling data uitwisselen. IPv4 heeft ongeveer 4 miljard unieke IP-adressen, die bijna allemaal in gebruik zijn. De opvolger van IPv4 is IPv6, maar IPv4 wordt op dit moment nog het meest gebruikt.	

BEGRIP	BETEKENIS	ZIE OOK
IPv6	Internet Protocol versie 6. IPv6 maakt communicatie van data tussen ICT-systemen binnen een netwerk, zoals Internet, mogelijk. De standaard bepaalt dat ieder ICT-systeem binnen het netwerk een uniek nummer (IPv6-adres zoals 2002:4aab:3490:0000:0000:b93f:0481:2289) heeft. Hierdoor kunnen ICT-systemen elkaar herkennen en onderling data uitwisselen. IPv6 heeft een veel grotere hoeveelheid beschikbare IP-adressen ten opzichte van de voorganger IPv4. Dit maakt verdere groei en innovatie van het Internet mogelijk. IPv4 wordt nog steeds meer gebruikt dan IPv6.	
ISAC	Information Sharing and Analysis Centre. Overleg over cybersecurity dat regelmatig plaatsvindt. Tijdens dit overleg delen organisaties uit dezelfde sector gevoelige informatie over cyberincidenten, dreigingen, zwakke plekken en maatregelen op het gebied van cybersecurity. Doel hiervan is dat de organisaties van elkaar leren.	
ISMS	Information Security Management System. Managementsysteem voor de beveiliging van informatie. Met dit systeem bewaakt men het proces van informatiebeveiliging.	
ISO	1. Internationale set afspraken waar iets aan moet voldoen. De internationake afspraken voor informaitiebeveiliging is de reeks ISO 2700x. 2. Information Security Officer.	*Chief Information Security Officer*
ISO/IEC 27000 serie	Aantal ISO-normen waarin staat hoe een organisatie informatie goed kan beveiligen. In de normen staat hoe een organisatie beveiligingsmaatregelen kan vaststellen, invoeren, uitvoeren, beoordelen en bijhouden. De bedrijfsrisico's bepalen aan welke normen een organisatie wil of moet voldoen. Voorbeelden: ISO 27001 en 27002.	*Informatie-beveiliging*

BEGRIP	BETEKENIS	ZIE OOK
Jamming	Het verstoren van draadloze signalen zoals bijvoorbeeld WiFi.	
Joint Sigint Cyber Unit (JSCU)	De Joint Sigint Cyber Unit is een gezamenlijk onderdeel van de Nederlandse geheime diensten AIVD en MIVD en is gericht op het afluisteren van radio- en satellietverkeer (sigint) en het verkrijgen van inlichten via cyberoperaties.	
Key risk	Belangrijkste risico. De Key risk stelt men vast als men alle risico's heeft geanalyseerd.	
Keylogger	Software die kan bijhouden en vastleggen wat iemand op een toetsenbord typt. Aanvallers gebruiken zo'n programma vaak om wachtwoorden of creditcardgegevens te stelen.	
Kill chain	Verschillende fases van een doelgerichte aanval. Vanaf het verkennen van een mogelijk doelwit, het daadwerkelijk binnendringen, het maskeren van de aanval en het realiseren van het uiteindelijke doel.	
Klikfraude	...	*Adware*
Known unknown	Een bekend risico, dat wil zeggen een risico waarvan men weet dat het bestaat. Er zijn grofweg twee typen bekende risico's. Van sommige bekende risco's weet men hoe vaak ze voorkomen en welke consequenties ze hebben. Deze risico's zijn goed te voorspellen en te behandelen. Van andere bekende risico's weten we alleen dat ze kunnen optreden, maar kunnen we niet goed voorzien hoe, en wanneer.	
Kritieke infrastructuur	Die diensten, producten of onderdelen van de infrastructuur van een land die essentieel zijn. Worden deze onderdelen uitgeschakeld, of vallen ze uit? Dan is de kans op economische en/of maatschappelijke ontwrichting groot.	*Cyberbeveiligings-wet*

BEGRIP	BETEKENIS	ZIE OOK
Kroonjuwelen	Informatie en informatiesystemen die het allerbelangrijkst zijn voor een organisatie. Het heeft grote gevolgen voor de organisatie als men niet meer bij deze informatie kan komen wanneer men dat wil. Of als de informatie niet meer klopt, of als die ongewild bij anderen terechtkomt. Intelectueel eigendom is voorbeeld van een kroonjuweel.	
Kunstmatige intelligentie	...	*Artifical Intelligence*
Kwantum Computer	...	*Quantum computer*
Kwetsbaarhedenscan	...	*Vulnerability scan*
Kwetsbaarheid	Een eigenschap die een aanvaller de mogelijkheid biedt een cyberaanval uit te voeren of een eigenschap die kan leiden tot uitval. Dit kan zich voordoen in een digitale dienst, proces of systeem, maar ook in de samenleving als geheel of in een specifieke organisatie.	
Lateral Movement/ Laterale beweging	Technieken die aanvallers gebruiken om geleidelijk door een netwerk te bewegen. Terwijl ze door het netwerk bewegen, zoeken ze naar informatie met als doel hogere gebruikersrechten te verkrijgen.	
Lawful hacking	Het toestaan van hacken door politie en justitie voor opsporingsdoeleinden, onder strikte juridische voorwaarden. Dit kan gaan om het ontsleutelen van versleutelde informatie, het gebruiken van backdoors, het gebruiken van bekende vulnerabilities etc.	
Least Privilege	Uitgangspunt dat iemand zo min mogelijk bij informatie en systemen kan. Degene kan alleen bij informatie en systemen die hij of zij nodig heeft voor het werk.	

BEGRIP	BETEKENIS	ZIE OOK
Legacy	Verzamelnaam voor verouderde hardware en/ of software, die niet meer door leveranciers ondersteund wordt.	
Legacy systemen	Verouderde software of systemen die nog steeds gebruikt worden maar niet meer onderhouden worden door de leverancier of ontwikkelaar. De beveiliging van deze systemen is vaak verouderd en bevat regelmatig bekende gebreken.	
Lek	Aantasting van de vertrouwelijkheid als gevolg van natuurlijk, technisch of menselijk falen.	
Leveranciersketen	Een ecosysteem van dienstverleners die hard- en software, netwerken of diensten levert die door allerlei partijen worden gebruikt in hun netwerken en/of dienstverlening. Te denken valt aan cloudleveranciers.	
Living off the land	Living off the land (LOTL)-aanvallen gebruiken legitieme programma's en functies die al in het digitale domein aanwezig zijn, in plaats van malware van een externe bron binnen het domein te installeren. De heimelijke aard van deze aanvallen kan ze effectief maken, en lastig voor beveiligingsteams om te detecteren en voorkomen.	
Local privilege escalation	Zichzelf meer rechten geven op een digitaal systeem. Men doet dat via een hack of een bug in het systeem.	
Log	Een digitaal logboek. Bestand waarin een digitaal systeem automatisch veranderingen en gebeurtenissen bijhoudt.	*Auditlog*
LOTL	Living Off The Land.	*Living off the land*
LPE	Local Privilege Escalation.	*Local privilage escalation*

BEGRIP	BETEKENIS	ZIE OOK
Maatschappelijke ontwrichting	Er is sprake van een mogelijk ontwrichtend effect op de samenleving als één of meer van de zes nationale veiligheidsbelangen ernstig worden aangetast. (zie definitie nationale veiligheidsbelangen)	
M2M	Machine-to-machine. Uitwisseling van informatie tussen machines onderling.	
Machine Learning	Ontwikkeling van technieken waarmee computers kunnen leren.	
Malvertising	Het verspreiden van malware door die aan te bieden aan een een advertentiebemiddelaar. Zo worden grote groepen gebruikers besmet via een legitieme website.	
Malware	Samentrekking van malicious software. Malware is de term die als generieke aanduiding wordt gebruikt voor onder andere virussen, wormen en trojans.	
Managed detectie en respons	Bewaking van digitale infrastructuur middels een SOC/SIEM/XDR oplossing plus een (managed) dienst voor beheer van de oplossing en opvolging van de alarmsignalen die uit de oplossing resulteren.	*SOC, SIEM, XDR*
Man-in-the-middle aanval	Een aanval waarbij een aanvaller zich tussen twee partijen bevindt. De partijen denken direct met elkaar te communiceren. Echter de aanvaller is in staat informatie af te luisteren en/of te wijzigen en hier misbruik van te maken.	
Managed security	Continue beveiligingsdiensten die een managed security service provider levert aan een klant. Bijvoorbeeld managed firewalls, managed endpoint protection, etc.	
Managed security provider	...	*Managed security service provider*

BEGRIP	BETEKENIS	ZIE OOK
Managed security service provider	Gespecialiseerd bedrijf dat continue beveiligingsdiensten levert aan een klant. Bijvoorbeeld managed firewalls, managed endpoint protection, etc.	*Managed security*
MDM	Mobile Device Management.	*Mobile Device Management*
MDR	Managed Detectie en Respons.	*Managed detectie en respons*
Meerfactor authenticatie	Een manier van identiteit vaststellen waarvoor meerdere onafhankelijke bewijzen van identiteit zijn vereist.	
Meldplicht	Een wettelijke plicht om een incident te melden aan een toezichthouder of anderen. Verschillende wetten kennen een meldplicht, het meest bekend is de meldplicht in de AVG, die verplicht een datalek te melden aan de AP soms aan natuurlijke personen wiens persoonsgegevens zijn betrokken in het incident. Ook de Cyberbeveiligingswet kent een meldplicht.	*AVG, Cyberbeveiligingswet, Europese wet- en regelgeving*
Metadata	Gegevens die de eigenschappen van andere gegevens beschrijven. Bijvoorbeeld van wie de gegevens zijn, of wie ze verstuurd heeft, of wanneer ze voor het laatst gewijzigd zijn.	
MFA	Meer/Multi Factor Authenticatie	*Meerfactor authenticatie*
Middel	Aanvalstechniek(en), software en hardware die een actor gebruikt of kan gebruiken voor een cyberaanval. Een voorbeeld is ransomware of DDoS-aanval. De focus ligt hier op ‘de tool(box)’ zelf en bij Modus operandi op de inzet ervan door een actor.	

BEGRIP	BETEKENIS	ZIE OOK
Minimum viable product	Het minimaal levensvatbare vereistenpakket voor een product: het absolute minimum dat een digitaal systeem moet hebben om te werken. Alleen “need to have”, geen “could have” of “should have” of “nice to have”.	*MVP*
Mitigatie	Schade als gevolg van een incident verminderen. Of risico’s verkleinen om zo incidenten te voorkomen.	*Risico*
Mitigerende maatregel	Een activiteit met als doel om de oorzaak of het gevolg van een ongewenste gebeurtenis weg te nemen, of te verkleinen.	
MITRE Att&ck	Een samengestelde kennisbank en model voor het gedrag van cyberaanvallers, dat de verschillende fasen van de aanvalslevenscyclus van een tegenstander weerspiegelt en de platforms waarvan bekend is dat deze zich richten. De afkorting staat voor Adversarial Tactics, Techniques, and Common Knowledge.	
Mobile device management	Zorgen dat mobiele apparaten in een organisatie goed beheerd en beveiligd worden. Bijvoorbeeld smartphones en tablets. Beveiliging hoort daar ook bij, zoals een pincode instellen voor apparaten of zorgen dat men op afstand gegevens op deze apparaten kan wissen.	*MDM*
MO	Modus Operandi.	*Modus operandi*
Modus operandi	Een werkwijze die een actor gebruikt of kan gebruiken voor een cyberaanval. Denk aan voorbeelden zoals het combineren van middelen voor een aanval, het ongericht inzetten van het middel (schot hagel) of juist heel gericht inzetten e.d.. De focus ligt hier op de werkwijze en bij middel op ‘de tool(box)’ zelf.	*Middel*

BEGRIP	BETEKENIS	ZIE OOK
Money mule	Iemand die zijn bankrekening en/of pinpas uitleent aan criminelen. Criminelen gebruiken de bankrekening om er geld op te laten storten dat ze hebben gestolen door oplichting. Dit wordt ook wel geldezel of katvanger genoemd.	*Katvanger, cryptomule*
Monitoring	Continu bewaken van een computer of digitaal netwerk. Bijvoorbeeld of het nog helemaal goed werkt, of er fouten voorkomen, etc.	*Security monitoring*
MSP	Managed Security Provider.	*Managed security provider*
MSSP	Managed Security Service Provider.	*Managed security service provider*
Multifactor authenticatie	...	*Meerfactor authenticatie*
MVP	Minimium Viable Product.	*Minimium viable product*
Mystery guest bezoek	Beveiligingstest waarbij een daartoe aangewezen persoon op bezoek gaat bij een organisatie. Daar probeert hij in ruimtes te komen waar hij niet mag komen en hij probeert bij informatie te komen waar hij niet bij mag komen. Zo test de persoon deze organisatie. Men kan deze test combineren met een penetratietest. Bij zo’n gecombineerde test gaat de mystery guest een beveiligde technische ruimte in. Daar probeert hij in te breken op het lokale computernetwerk.	*Penetratietest*
NAT	Network Address Translation.	*Network Address Translation*

BEGRIP	BETEKENIS	ZIE OOK
Nationale Veiligheid	De nationale veiligheid is in het geding wanneer een of meerdere nationale veiligheidsbelangen ernstig worden bedreigd. Nationale veiligheid gaat over alle opzettelijke en niet-opzettelijke risico's (gevaren en dreigingen) die kunnen leiden tot maatschappelijke ontwrichting in Nederland. Van overstroming tot terrorisme en van een grieppandemie tot een cyberaanval.	
Nationale Veiligheidsbelangen	De zes nationale veiligheidsbelangen zijn: 1. Territoriale veiligheid: Het ongestoord functioneren van Nederland en haar EU en NAVO bondgenoten als onafhankelijke staten in brede zin, dan wel de territoriale veiligheid in enge zin. 2. Fysieke veiligheid: Het ongestoord functioneren van de mens in Nederland en zijn omgeving. 3. Economische veiligheid: Het ongestoord functioneren van Nederland als een effectieve en efficiënte economie. 4. Ecologische veiligheid: Het ongestoord blijven voortbestaan van de natuurlijke leefomgeving in en nabij Nederland. 5. Sociale en politieke stabiliteit: Het ongestoorde voortbestaan van een maatschappelijk klimaat waarin individuen ongestoord kunnen functioneren en groepen mensen goed met elkaar kunnen samenleven binnen de verworvenheden van de Nederlandse democratische rechtstaat en daarin gedeelde waarden. 6. Internationale rechtsorde: Het goed functioneren van het internationale stelsel van normen en afspraken, gericht op het bevorderen van de internationale vrede en veiligheid.	

BEGRIP	BETEKENIS	ZIE OOK
NCSC	Nationaal Cyber Security Centrum. Onderdeel van het ministerie van Justitie en Veiligheid. In dit centrum komt alle informatie over cyberveiligheid samen. Het centrum werkt voor de Rijksoverheid en voor processen die het belangrijkst zijn in Nederland. Bijvoorbeeld elektriciteit, toegang tot schoon drinkwater.	
N-day kwetsbaarheid	Een zwakke plek in de beveiliging waarvan een softwareontwikkelaar of hardwarefabrikant al op de hoogte is. Deze bedrijven hebben misschien al een patch uitgebracht voor dit soort zwakke software of hardware, of ze zijn er een aan het maken of uitrollen.	*Zero-day*
Nederlandse Cybersecurity Strategie 2022-2028	Strategiedocument uit 2022. De NLCS beschrijft de visie op een digitaal veilig Nederland waarin iedereen ten volle kan profiteren van deelname aan de digitale samenleving. Om deze visie te realiseren zijn er doelen geformuleerd langs vier pijlers: 1. Digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties 2. Veilige en innovatieve digitale producten en diensten 3. Tegengaan van digitale dreigingen van staten en criminelen 4. Cybersecurity-arbeidsmarkt, onderwijs en digitale weerbaarheid van burgers	
Need-to-know principe	Uitgangspunt dat iemand alleen de informatie krijgt die nodig is om een bepaalde taak of opdracht uit te voeren. Ook als degene vanuit zijn functie eigenlijk meer informatie zou mogen zien. Dit wordt vaak toegepast bij erg gevoelige informatie.	

BEGRIP	BETEKENIS	ZIE OOK
Negligible risk	Verwaarloosbaar risico. Risico waarvan de kans, de consequenties, of beiden zo klein is/zijn, dat het verwaarloosd kan worden. De kosten van mitigatie wegen dan niet op tegen de baten.	
Nepnieuws	Nieuws dat niet waar is. Het doel van nepnieuws is dat men de mening van de ontvangers ervan beïnvloedt.	
Netto risico	Beveiligingsrisico van een systeem. Men kijkt hierbij ook naar de beveiligingsmaatregelen die er nu al zijn.	*Bruto risico*
Netwerk probe	...	*Netwerksensor*
Netwerkbeveiliging	De set van technische maatregelen die wordt genomen om een computernetwerk zo goed mogelijk te beveiligen. Voorbeelden zijn: firewalls, endpoint protectie, IDS, IPS, etc.	
Netwerksegmentatie	Het onderverdelen van een fysiek computernetwerk in verschillende logische onderdelen die van elkaar afgeschermd kunnen worden. Op elk netwerksegment kunnen verschillende beveiligingsmaatregelen worden toegepast. Zo krijgt een aanvaller die in een bepaald netwerksegment is gekomen, niet automatisch toegang tot andere (kwetsbare) delen in het computernetwerk.	
Netwerksensor	Systeem dat precies kan aflezen welke informatie over een netwerk gaat. Het systeem kan deze informatie onderzoeken, en uitzoeken of er een probleem is met de beveiliging.	
Netwerktoegangsbeheer	Manier om het een netwerk beter te beveiligen. Dit gebeurt door alleen bekende en geautoriseerde apparaten op het netwerk toe te laten.	

BEGRIP	BETEKENIS	ZIE OOK
Network access control	...	*Netwerktoegangs-beheer*
Network Operations Center	Een of meer plekken vanwaar men een netwerk bewaakt en eventueel beheert. Men bewaakt een netwerk door te controleren hoe stabiel netwerkverbindingen en servers zijn en hoeveel data er doorheen gaan. Men beheert een netwerk door in te loggen op servers en andere onderdelen van het netwerk. Zo nodig doet men dat op afstand.	
Network security	...	*Netwerkbeveiliging*
NIB-richtlijn	...	*WBNI, Cyber-beveiligingswet*
Niet persoonsgebonden account	Account dat niet bij een bepaalde persoon hoort. Er zijn 2 soorten: 1. Een non-interactive NPA wordt gebruikt door systeemfuncties en kan niet gebruikt worden door een eindgebruiker om in te loggen. 2. interactieve NPA. Dit is vaak een gedeeld account voor bepaalde beheertaken. Meerdere personen kunnen dit account gebruiken.	
Niet-statelijke actor	Woord dat wordt gebruikt om actoren aan te duiden die niet optreden voor of namens een staat. Term wordt veel gebruikt in geopolitieke discussies over cybersecurity, en in debatten rondom nationale veiligheid.	
NIS-directive	...	*WBNI, Cyber-beveiligingswet*

BEGRIP	BETEKENIS	ZIE OOK
NIST Cybersecurity Framework	Algemene regels van het National Institute for Standards and Technology (NIST) uit de Verenigde Staten. De regels geven aan wat organisaties beter kunnen doen om cyberaanvallen te voorkomen en op te sporen. En hoe ze er beter op kunnen reageren.	
NLCS	Nederlandse Cybersecurity Strategie.	*Nederlandse Cybersecurity Strategie*
No-log VPN	...	*Anonymizing VPN*
NOC	Network Operations Center.	*Network Operations Center*
Non-repudiation	...	*Onweerleg-baarheid*
Non-state actor	...	*Niet-statelijke actor*
Notice and take-down	Procedure voor website-eigenaren en netwerkbeheerders. Ze verwijderen content van Internet wanneer die door een rechtbank als illegaal is bestempeld, of wanneer daar een verdenking van is. Dit wordt veel gebruikt in het licht van schendingen van het auteursrecht.	
NPA	Niet Persoonsgebonden Account.	*Niet persoonsge-bonden account*
NPG-account	Account niet persoonsgebonden.	*Niet persoonsge-bonden account*
Nummerspoofing	Spoofing via SMS of spraakoproep waarbij een ander nummer dan het eigen nummer wordt gebruikt.	

BEGRIP	BETEKENIS	ZIE OOK
Obfuscation	Iets verhullen om het anderen moeilijk te maken. Beveiligers kunnen bijvoorbeeld systemen of informatie verhullen om het aanvallers moeilijk te maken. Aanvallers verhullen bijvoorbeeld vaak de broncode in hun malware om het beveiligers moeilijk te maken.	
Offensieve capaciteiten	Digitale middelen die tot doel hebben het handelen van de tegenstander te beïnvloeden of onmogelijk te maken. Deze capaciteiten kunnen bijvoorbeeld in een militaire operatie worden ingezet ter ondersteuning van conventionele militaire capaciteiten.	
One-day vulnerability	Een one-day vulnerability is een bekende kwetsbaarheid in software of hardware waarvoor een patch of oplossing beschikbaar is, maar die nog niet is toegepast.	
Ontsleutelen	Versleutelde informatie leesbaar maken. Bijvoorbeeld een versleuteld tekstbestand of netwerkverkeer. Dit wordt gedaan met één of twee sleutels: symmetrische of asymmetrische versleuteling. De informatie die onleesbaar is gemaakt door de zender, maakt de ontvanger weer leesbaar met behulp van de sleutel(s). Men versleutelt informatie bijvoorbeeld om deze veilig te versturen of om vast te stellen dat een bericht ook echt komt van degene die zegt dat hij het heeft verstuurd.	*Cryptografie, Versleutelen*
Onweerlegbaarheid	Een bericht is onweerlegbaar als de verzender niet kan ontkennen dat hij het bericht heeft verstuurd. De ontvanger kan niet ontkennen dat hij het bericht heeft ontvangen.	*Cryptografie*

BEGRIP	BETEKENIS	ZIE OOK
Open source	Een kenmerk van software dat aangeeft dat de broncode van de software publiek beschikbaar is, in tegenstelling tot software die alleen in binaire vorm wordt verspreidt. Het open source maken van software stelt anderen in staat werking te verifiëren en aanpassingen aan de software aan te brengen of voor te stellen. Open source maakt het ook makkelijker om kwetsbaarheden in software te vinden, omdat de broncode hiervoor gelezen kan worden. Nadeel kan zijn dat hierdoor ook kwetsbaarheden ontstaan die niet snel opgemerkt worden.	*Broncode*
Open source intelligence (OSINT)	Inlichtingen verzamelen over een onderwerp door bronnen te gebruiken die voor iedereen toegankelijk zijn.	
Operational Technology	Een verzamelnaam voor verschillende systemen die worden gebruikt voor het beheer van operationele processen in de fysieke wereld zoals het aansturen en monitoren van (industriële) apparatuur. Voorbeelden zijn sluizen en medische apparatuur.	
OSCP	Offensive Security Certified Professional. Diploma voor pentesters. Het praktijkexamen duurt ongeveer 24 uur. In deze tijd moet de tester verschillende soorten systemen hacken.	
OSI model	Open Systems Interconnection model. Referentiemodel dat is ontwikkeld vanuit ISO. Het doel van dit model is een open communicatie tussen verschillende technische systemen.	

BEGRIP	BETEKENIS	ZIE OOK
OSINT	Open Source INTelligence.	*Open source intelligence*
OT	Operational Technology.	*Operational Technology*
OTP	One Time Password. Een wachtwoord dat geldig is voor de duur van één login-sessie.	
OWASP top 10	Project van Open Web Application Security Project (OWASP). In de OWASP top 10 staan de 10 grootste risico's op het gebied van beveiliging van webapplicaties. De OWASP top 10 wordt periodiek herzien.	
P2P	Een logisch (peer-to-peer) netwerk van computers die in dit netwerk gelijkwaardig zijn, en diensten aan elkaar kunnen aanbieden.	*Peer-to-peer*
PaC	Policy as Code.	*Policy as code*
Packet capture	Bestand met een exacte kopie van gegevens die door een netwerk zijn gegaan.	
Parameter	Een parameter is een variable van een bepaald type die kan worden veranderd of worden gebruikt in bewerkingen en berichten, zoals x in een formule. Als de parameter een waarde krijgt, krijgt ook de uitkomst van de formule een waarde.	
Partij	Verzamelbegrip voor organisaties, bedrijven, overheden en burgers.	
Password	...	*Wachtwoord*
Patch	Nieuwe versie van software. In deze nieuwe versie heeft de leverancier kwetsbaarheden in het systeem hersteld. Hij heeft geen nieuwe functies toegevoegd.	*Update*

BEGRIP	BETEKENIS	ZIE OOK
Patch management	Proces waarbij men indien mogelijk patches installeert op een digitaal systeem. Het proces dat zorgt voor het verwerven, testen en installeren van patches (wijzigingen ter opheffing van bekende beveiligingsproblemen in de code) op (verschillende softwarecomponenten van) een digitaal systeem.	
Path traversal	Aanval via een website, met als doel om bij bestanden en mappen te komen waar men niet bij mag. De aanvaller kan de website manipuleren door bepaalde invoer te sturen. Zo kan hij een pad volgen naar een bestand of map waar hij niet bij mag.	*Directory traversal*
Payload	Het onderdeel van malware dat de echte kwaadaardige actie uitvoert, zoals het stelen van gegevens of het vernielen van een systeem.	*Malware*
PCAP	Packet CAPture.	*Packet capture*
PCI	Payment Card Industry. De branche die ervoor zorgt dat men geld kan pinnen en elektronisch kan betalen. Bijvoorbeeld door pinautomaten, kassasystemen en creditcards te leveren. Het betreft ook de elektronische verbindingen tussen deze systemen.	*PCI-DSS*
PCI-DSS	Payment Card Industry Data Security Standard. Standaardregels voor de betaalindustrie, met als doel om gegevens van bankpassen en creditcards te beschermen. De regels gelden voor alle organisaties die gegevens van kaarthouders opslaan, verwerken of versturen. De regels gaan over eisen voor het technische systeem waarin men gegevens van de kaarthouder opslaat. En over eisen voor het verwerken en versturen van deze gegevens.	

BEGRIP	BETEKENIS	ZIE OOK
Penetratietest	Handmatige controle waarbij men zo diep mogelijk wil binnendringen in een digitaal systeem om zwakke plekken te vinden en de gevolgen hiervan te kennen. Men gebruikt de zwakke plekken om nog wat dieper in het systeem te komen. Doel van de test is niet om zoveel mogelijk zwakke plekken te vinden, maar om te onderzoeken of een systeem zwakke plekken kent. Het zoeken naar zoveel mogelijk zwakke plekken gebeurt wel bij een vulnerability scan.	*Securitytest , Vulnerability scan*
Pentest	...	*Penetratietest*
Persistence	Langdurige aanwezigheid.	
Persoonsgegevens	Informatie waarmee een persoon direct of indirect geïdentificeerd kan worden, zoals naam, adres, BSN-nummer. Om van persoonsgegevens te kunnen spreken is het niet perse nodig dat iemands naam kan worden achterhaald. Voldoende is dat duidelijk is dat de informatie naar een specifiek persoon herleidbaar is.	*AVG, GDPR*
PGP	Pretty Good Privacy. Een standaardmanier om informatie onleesbaar voor anderen te maken met gebruik van zowel symmetrische als asymmetrische versleuteling. Men gebruikt hierbij 2 verschillende formules: 1. Eén om de tekst om te zetten in een code. 2. Eén om de code weer terug te zetten in tekst.	*Cryptografie*
Phishing	Verzamelnaam voor digitale activiteiten die tot doel hebben informatie aan mensen te ontfutselen. Deze informatie kan worden misbruikt voor bijvoorbeeld toegang tot systemen.	*Smishing, Vishing*

BEGRIP	BETEKENIS	ZIE OOK
Phishingkit/phishing-panel	Software om phishing-websites op te zetten en te beheren. De phishingkit biedt doorgaans de kwaadwillende mogelijkheden omverschillende neppagina's te beheren en via een beheerderspagina de bezoekers van de phishing-website te instrueren. Phishingkits worden tegenwoordig ook aangeboden als een dienst, een vorm van cybercrime-as-a-service.	*Cyber-crime-as-a-service*
PIA	Privacy Impact Assessment.	*Privacy Impact Assessment*
PII	Personally Identifiable Information.	*Persoonsgegevens*
PKI	Public Key Infrastructure.	*Public Key Infrastructure, Certificate*
Policy as Code	Het ervoor zorgen dat bepaalde regels en procedures automatisch binnen een digitaal netwerk worden toegepast.	
Poortscan	...	*Port scan*
Port scan	Scan van openstaande poorten op een digitaal systeem waarmee inzichtelijk wordt gemaakt welke poorten openstaan. Een poort is een ingang om via een netwerk te communiceren met een digitaal systeem. Aanvallers gebruiken de informatie uit de poortscan om te beslissen hoe zij het systeem kunnen binnendringen of beschadigen.	
Post-quantum key exchange	Afspraken over hoe je in het kader van versleuteling (cryprografie) de sleutels uitwisselt. Het gaat om sleutels die niet te kraken zijn met kwantumcomputers.	*Cryptografie, Quantum computing*
Pretexting	Manier die gebruikt wordt bij social engineering: het inzetten van psychologische trucs om iemand persoonlijke, gevoelige informatie te ontfutselen en/of om diegene er op manipulatieve wijze toe te bewegen om bepaalde handelingen te verrichten.	

BEGRIP	BETEKENIS	ZIE OOK
Privacy by Default	Standaardinstellingen van een product, dienst of systeem zodanig maken, dat ze een zo groot mogelijke privacy garanderen.	*AVG*
Privacy by Design	Eigenschap van een product, dienst of systeem. Bij de ontwikkeling en het ontwerp ervan heeft men zoveel mogelijk rekening gehouden met privacy.	*AVG*
Privacy Impact Assessment	Onderzoek waarmee een organisatie inzicht krijgt in de privacyrisico's. De Algemene Verordening Gegevensbescherming verplicht organisaties soms om dit onderzoek uit te voeren. Die heet dan een Data Privacy Assessment of een gegevensbeschermingseffectbeoordeling.	*AVG*
Privacybeleid	Met een privacybeleid brengt een organisatie in kaart welke maatregelen zij heeft genomen om de persoonsgegevens van bijvoorbeeld klanten, patiënten en cliënten te beschermen. Daarnaast is het een manier om als organisatie aan zowel de doelgroep als aan de Autoriteit Persoonsgegevens te laten zien dat ze voldoet aan de AVG.	*Gegevens-bescherming*
Privacy Officer	De Privacy Officer (PO) is verantwoordelijk voor de ontwikkeling en implementatie van het privacybeleid van een organisatie.	
Private key	Daarnaast is de PO tweede lijn voor privacy-gerelateerde vragen vanuit de organisatie. Sleutel die men gebruikt om te versleutelen en ontsleutelen wanneer er gebruik gemaakt wordt gemaakt van asymmetrische versleuteling. Het is van belang dat deze sleutel geheim wordt gehouden.	*Public key, Versleutelen, Assymetrische cryptografie*
Privilege escalation	Aanvalsmethode waarbij men zwakke plekken in een digitaal systeem gebruikt. Zo zorgt de aanvaller dat hij rechten krijgt om op plekken in het digitale systeem te komen, waar hij niet zou mogen komen.	

BEGRIP	BETEKENIS	ZIE OOK
Privileged account	Account op een digitaal systeem dat meer rechten geeft om bepaalde dingen te doen. Bijvoorbeeld bestanden en instellingen veranderen. In Windowssystemen heet dit account de administrator. In Unix en Linuxsystemen de root.	
Procesbesturings-systeem	Algemene naam voor verschillende typen systemen die fysieke processen aansturen zoals SCADA, DCS's, PLC's. Deze systemen openen bijvoorbeeld een sluis of zetten een windmolen uit. Ook wel aangeduid als industriële controlesystemen (ICS).	*ICS, industriële controlesystemen, industral control system*
Profilering	Techniek waarbij men op basis van het profiel van een persoon gepersonaliseerde diensten of informatie aanbiedt. Het profiel wordt gebaseerd op de sites die iemand bezoekt en de links waar hij op klikt. Zowel bedrijven als overheidsdiensten gebruiken deze techniek.	
Proxies	Alle niet-statelijke actoren (non-state actors) die namens een staat cyberaanvallen uitvoeren op of via het Internet. Soms erkent een staat deze proxies, maar vaak ook niet.	*Niet-statelijke actor*
Proxy	Digitaal systeem dat als (beschermend) tussenstation dient tussen een gebruiker en het Internet.	
Pseudonimisering	Methode om gegevens niet meteen te kunnen verbinden met een persoon. De persoonsgegevens vervangt men via een formule door een code. De formule en de persoonsgegevens bewaart men op een andere plek. Zo kan men altijd nagaan om welke persoon het gaat.	
Public Key	Sleutel die men gebruikt om te versleutelen en ontsleutelen wanneer er gebruik gemaakt wordt gemaakt van asymmetrische versleuteling. Deze sleutel is openbaar, in tegenstelling tot de private key.	*Private key, Versleutelen, Assymetrische cryptografie*

BEGRIP	BETEKENIS	ZIE OOK
Public Key Infrastructure	Alle rollen, regels en procedures die nodig zijn om verantwoord om te gaan met digitale certificaten. Men gebruikt de certificaten bijvoorbeeld om teksten via asymmetrische versleuteling onleesbaar te maken voor anderen of bij authenticatie.	*Public key, Private key, Versleutelen*
Purple teaming	Gecombineerde oefening voor het testen van de beveiliging van een digitaal systeem waarbij een Red Team en een Blue Team worden ingezet.	*Adversary simulation, Blue Team, Red Team*
Quadrupel Extortion	Situatie waarbij de bestanden of systemen van het slachtoffer zijn versleuteld en de sleutel tegen betaling wordt aangeboden. Voor extra druk op het slachtoffer wordt gedreigd om gestolen informatie te openbaren.	
Quantum Computer	Computer die informatie opslaat en bewerkt door de eigenschappen te gebruiken van deeltjes die nog kleiner zijn dan een atoom. De kwantumcomputer kan heel veel sneller rekenen dan gewone computers. Hierdoor kan een kwantumcomputer bijvoorbeeld gemakkelijk beveiligingscodes kraken en zijn er in de toekomst daardoor nieuwe manieren van beveiliging nodig. Deze soort computer is voorlopig nog toekomstmuziek.	
Quarantaine	Situatie waarin een apparaat of documenten worden geïsoleerd van andere apparaten of documenten. Dit kan bijvoorbeeld doordat een firewall een apparaat netwerktoegang ontzegt, of doordat security tooling op een apparaat geïnstrueerd wordt om de netwerktoegang van dat apparaat uit te schakelen of te beperken. Quarantaine wordt toegepast wanneer bijvoorbeeld een malware-dreiging met risico op verspreiding wordt aangetroffen op een apparaat: in afwachting van onderzoek wordt het apparaat in quarantaine geplaatst om verspreiding van de dreiging te voorkomen.	

BEGRIP	BETEKENIS	ZIE OOK
Quishing	Een vorm van phishing door het gebruiken van valse QR codes om gegevens of geld te stelen.	*Phishing*
Radio Equipment Directive 2 (RED2)	Ook wel Radioapparatenrichtlijn genoemd. Europese richtlijn waar fabrikanten, importeurs en verkopers van radioapparaten zich aan moeten houden. Daar komen vanaf augustus 2025 ook eisen voor de cyberveiligheid bij.	*Europese wet- en regelgeving*
Rainbow table	Tabel met mogelijke wachtwoorden en de versleutelde versies van deze wachtwoorden. Men gebruikt de tabel om te testen of wachtwoorden veilig zijn, of om ze te kraken. Deze techniek is veel efficiënter dan een brute force-aanval.	*Brute force*
Random	Iets wat niet te voorspellen is.	
Ransomware	Kwaadaardige software waarbij eenslachtoffer 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. Ransomware is een samenvoeging van de woorden ransom (losgeld) en software. Tegenwoordig is de daadwerkelijke software maar een kleine stap in de totale aanval die plaatsvindt. Alle stappen samen vormen de Ransomware Killchain.	*Ransomware Killchain, Ransomware aanval*

BEGRIP	BETEKENIS	ZIE OOK
Ransomware aanval	Een actor versleutelt bestanden van gebruikers met behulp van ransomware (software), met als doel om deze later te ontsleutelen in ruil voor losgeld. In extreme gevallen blokkeert de ransomware de toegang tot het systeem door ook systeembestanden te versleutelen die essentieel zijn voor de goede werking van het systeem. Een actor kan met behulp van geavanceerde soorten ransomware naast lokale systemen ook harde schijven, databases, back-ups, USB-sticks en gegevens in de cloud versleutelen. Een ransomware aanval tast in ieder geval de beschikbaarheid van systemen en data aan. Bij een gerichte ransomware-aanvallen heeft de actor toegang tot de systemen en dat brengt mogelijk de integriteit en de vertrouwelijkheid van data in gevaar. Met name cybercriminelen voeren ransomware-aanvallen uit.	
Ransomware affiliate	Partij die ransomware-aanvallen uitvoert met ransomware-tooling die wordt gehuurd van een ransomware operator, waar de affiliate een partnerrelatie mee heeft. Ransomware affiliates maken vaak gebruik van toegang tot netwerken die wordt gekocht bij initial access brokers.	*Ransomware operator, Initial access broker*
Ransomware-as-a-Service	Een dienst waarbij cybercriminelen ransomware aanbieden als een comerciele dienst, waardoor ook minder technische criminelen ransomware aanvallen kunnen uitvoeren.	
Ransomware Killchain	De verschillende stappen in de keten die gezamenlijk een ranssomware aanval vormen. Deze stappen zijn: 1. Initiële toegang 2. Consolidatie 3. Data exfiltratie 4. Ransomware uitrol 5. Afpersing	*Ransomware*

BEGRIP	BETEKENIS	ZIE OOK
Ransomware operator	Partij die ransomware ontwikkelt, en vaak ook een platform onderhoudt waarop gecommuniceerd kan worden tussen slachtoffer en operator voor onderhandelingen en betalingen. Ransomware operators maken vaak gebruik van een “affiliate program” waardoor andere groepen de daadwerkelijke aanvallen uitvoeren, en de ransomware operator zich beperkt tot het ontwikkelen van de tooling en het platform, en een percentage van de winst opstrijkt.	
Ransomware simulation	Gespecialiseerde en gecontroleerde ransomware oefening.	
RASP	Runtime Application Self-Protection. Een beveiligingstechnologie die zich richt op het beschermen van applicaties tijdens hun uitvoering (runtime) door real-time monitoring en bescherming te bieden tegen aanvallen.	
RAT	Remote Access Trojan. Kwaadaardige software waarmee een aanvaller een digitaal systeem kan besturen. Bijvoorbeeld vastleggen wat iemand typt, de webcam aanzetten, gegevens op een digitaal systeem wissen, of contact maken met Internet.	
Rate-limiting	Methode om netwerkverkeer te beperken of om te beperken hoe vaak een actie mag worden uitgevoerd binnen een bepaalde tijd. Bijvoorbeeld beperking van het aantal inlogpogingen dat een gebruiker binnen korte tijd kan doen.	
RBAC	Role Based Access Control.	*Role based access control*
RDI	...	*Rijksinspectie Digitale Infrastructuur*

BEGRIP	BETEKENIS	ZIE OOK
Recovery	...	*Disaster recovery*
RED	...	*Radio Equipment Directive (RED)*
Red team	Oefening waarbij een organisatie aanvallen simuleert om te ontdekken hoe goed ze is beschermd tegen aanvallen. Het Red team speelt aanvallen en aanvalsmethodes na van een gekozen tegenstander.	*Adversary simulation*
Reliability	...	*Betrouwbaarheid*
Remote access	Mogelijkheid om van buitenaf in een computernetwerk te komen. Bijvoorbeeld in een bedrijfsnetwerk, zodat je thuis kunt werken.	
Resilience	...	*Cyber-weerbaarheid*
Responsible disclosure	Actie waarbij men gevonden beveiligingslekken op een verantwoorde manier bekend maakt. Meestal meldt men het lek eerst bij de eigenaar van het systeem waar het is gevonden. De eigenaar heeft regels over wat er daarna gebeurt. Wordt het systeem meteen aangevallen via dit lek? Dan meldt de onderzoeker het lek bij de maker van het systeem of de software. Als het lek gedicht is, krijgt de bredere security community dit te horen. Melders van een lek krijgen meestal geen geld. Maar vaak krijgen ze wel een cadeautje. Of hun naam komt in een Hall of Fame.	*Coordinated vulnerability disclosure*
Restrisico	...	*Netto risico*
Reverse engineering	Hardware of software onderzoeken om te snappen hoe deze precies werkt. De onderzoeker weet van tevoren niet hoe de software of hardware ontworpen is.	

BEGRIP	BETEKENIS	ZIE OOK
Rijksinpectie Digitale Infrastructuur	Toezichthouder die toeziet op de beschikbaarheid, continuïteit en betrouwbaarheid van de digitale infrastructuur.	*Cyberbeveiligingswet, RED2, Europese wet- en regelgeving*
Risico	Kans op schade of verlies in een digitaal systeem, gecombineerd met de gevolgen die deze schade heeft voor de organisatie. Een voorbeeld van schade kan bijvoorbeeld zijn dat mensen informatie zien die ze niet hadden mogen zien. Of dat men niet meer zeker weet of gegevens nog kloppen. Bij gevolgen voor de organisatie kan men denken aan financiële schade of het verlies van de goede naam van de organisatie.	*Dreiging, threat*
Risico acceptatie	Het besluit om bepaalde risico's te nemen en hier tegenmaatregelen op te nemen.	*Risico, Bestuursaansprakelijkheid*
Risico identificatie	Het in kaart brengen van de mogelijke risico's waaraan een organisatie of systeem is blootgesteld.	
Risico inventarisatie	Systematische beschrijving van alle risico's die een organisatie loopt. Vaak doet men dit als onderdeel van risicomanagement of voordat men een verzekering afsluit.	*Bedrijfsrisico*
Risicoanalyse	Methode om inzicht te krijgen in de risico's die je loopt. De onderzoeker kijkt daarbij onder andere naar het volgende: - Hoe groot is de kans dat iets gebeurt? - Hoe groot zijn de gevolgen als dat gebeurt?	
Risicobeheersing	...	*Risicomanagement*
Risicobereidheid	De hoeveelheid en het soort risico dat een organisatie bereid is na te streven, te behouden of te nemen.	*Mitigatie*

BEGRIP	BETEKENIS	ZIE OOK
Risicofactor	Al die dingen die de kans vergroten op schade aan mensen, organisaties, staten of digitale (genetwerkte) systemen. Of die de gevolgen van schade daarvan verergeren.	
Risicoinformatie	Technische informatie over mogelijk kwetsbare systemen. Bijvoorbeeld informatie over kwetsbare Citrix of Exchange servers die gelokaliseerd kan worden op basis van bekende IP-adressen en assets.	
Risicomanagement	Een continu proces waarbij bedrijfsrisico's voortdurend worden bewaakt. Onderdelen van dit proces zijn bijvoorbeeld het identificeren, evalueren, prioriteren van risico's en het nemen van maatregelen (accepteren, mitigeren, overdragen of vermijden).	*Bedrijfsrisico, risicoanalyse, mitigerende maatregelen*
Risicomitigatie	Alle dingen die een organisatie doet om risico's te verkleinen of helemaal te laten verdwijnen. Grijpt een organisatie in, dan kan dat twee doelen hebben: 1. De kans op een incident verkleinen. 2. De gevolgen verkleinen als dat incident toch plaatsvindt.	
Risiconiveau	...	*Risicoprofiel*
Risicoperceptie	De manier waarop risico's worden geïnterpreteerd en gewaardeerd. Vaak hebben experts een heel andere risicoperceptie dan leken ten aanzien van hetzelfde risico. Beslissers moeten zich bewust zijn van de beleving van risico's bij het nemen van beslissingen.	
Risicoprofiel	Overzicht van alle risico's van een organisatie, project, proces of programma. Een risicoprofiel laat zien welke risico's er zijn, inclusief kans van optreden en de gevolgen.	

BEGRIP	BETEKENIS	ZIE OOK
Risk appetite	...	*Risicobereidheid*
Role based access control	Bepalen of een gebruiker bij een digitaal systeem mag komen. Men kijkt daarbij naar de rol die de gebruiker of een groep gebruikers heeft. Voorbeelden van rollen zijn viewer, editor en manager.	
Root cause analyse	Onderzoek naar de belangrijkste oorzaken van een cyberincident, zoals een datalek.	
Rootkit	Malware die een aanvaller gebruikt als hij eenmaal toegang heeft tot een digitaal systeem. De rootkit zit zo diep in het systeem dat het lange tijd ongemerkt in het digitaal systeem kan blijven zitten. De rootkit kan ook een geheime toegang tot het systeem maken.	*Malware*
Rule based detection	Methode om een cyberaanval te ontdekken. Van tevoren bepaalt men welke patronen of tekens in data op een netwerk verdacht kunnen zijn. Daarna zoekt het systeem naar deze patronen of tekens.	
S/MIME	Secure/Multipurpose Internet Mail Extensions. Techniek waarbij men e-mails omzet in code met een openbare sleutel en een privésleutel. De openbare sleutel deelt men met elkaar via een certificaat.	

BEGRIP	BETEKENIS	ZIE OOK
Sandbox	Afgeschermd deel in een digitaal systeem. Software die op deze plek werkt, kan geen andere processen in de computer verstoren. Sandboxen kennen verschillende implementaties: - Gebruik als software om applicaties binnen deze sandbox te beschermen tegen aanvallen (wordt vaak toegepast binnen MDM oplossingen). - Een systeem in het netwerk dat ingezet wordt om te onderzoeken op onbekende content (zoals gedownload vanaf het Internet) ongewenst gedrag vertoont.	
SAST	Static Application Security Testing. Techniek waarmee men automatisch zwakke plekken in een broncode kan controleren.	
SBoM	Software Bill of Materials. Lijst van welke versie van componenten in de software zit.	
SCA	Software Composition Analysis. Doorontwikkeling van SAST.	*SAST*
SCADA	Supervisory Control and Data Acquisition. Meetsignalen en regelsignalen van machines in grote industriële systemen verzamelen, doorsturen, verwerken en zichtbaar maken. Bijvoorbeeld van windturbines.	*SCADA*
Screening	De integriteit van een persoon onderzoeken. Een werkgever kan dit doen als hij iemand wil aannemen voor een functie waarin integriteit extra belangrijk is. De werkgever vraagt informatie op over de persoon. Daarmee schat de werkgever in hoe integer deze persoon is. Screening mag alleen als je voldoet aan voorwaarden die staan in de wet: de Algemene Verordening Gegevensbescherming, de Uitvoeringswet Algemene Verordening Gegevensbescherming en de Wet veiligheidsonderzoeken.	

BEGRIP	BETEKENIS	ZIE OOK
Script	Computerprogramma met instructies die voor mensen leesbaar zijn. Men gebruikt vaak scripts als men webapplicaties wil bouwen en beheren. Aanvallers gebruiken onder andere scripts om onderdelen van een cyberaanval te automatiseren.	
Scriptkiddie	Actor met beperkte kennis die hulpmiddelen gebruikt die door anderen zijn bedacht en ontwikkeld, voor digitale aanvallen, om kwetsbaarheden aan te tonen of voor de eigen uitdaging.	
Scrubbing	Gegevens filteren die naar een systeem gaan. Doel is onder andere om te zorgen dat DDoS-aanvallen niet succesvol kunnen zijn of om DDoS-aanvallen onschadelijk te maken.	
Secure coding	Een gestructureerde aanpak om software te ontwikkelen. Doel is om software te maken die minder beveiligingslekken bevat.	
Secure development lifecycle	Een door Microsoft ontwikkeld proces waarin men kijkt wat de beste beveiligingsmethode is voor een reeks producten of toepassingen. Daarna wordt deze methode de standaardmethode. Het doel is in iedere fase van de ontwikkeling van een product te kijken naar de veiligheid.	
Secure Sockets Layer	Verouderd model om communicatie tussen computers onleesbaar te maken voor anderen. In 2014 werd bekend dat er een beveiligingslek in dit model zit. Nu vindt men dit model niet meer veilig. De opvolger is TLS: Transport Layer Security.	*Transport Layer Security*

BEGRIP	BETEKENIS	ZIE OOK
Secure web gateway	Een oplossing die ongewenste software en malware wegfiltert uit door de gebruiker geïnitieerd web- en Internetverkeer en die compliance met bedrijfsbeleid en regelgeving afdwingt. Een secure web gateway bevat vaak de volgende functionaliteiten: - URL-filtering (om minimaal malicious websites te blokkeren, maar eventueel ook andere categorieën als drugs, pornografie, peer-to-peer filesharing, etc) - Data Loss Prevention (DLP), - Anti-Malware - Authenticatie (om te bepalen welke gebruiker(sgroep) welke delen van het Internet mag benaderen) Een secure web gateway wordt ook wel forward proxy genoemd.	
Security	...	*Beveiliging*
Security advisory	1. Berichten van onderzoekers of leveranciers van software, waarin zij beschrijven waar zwakke plekken in software zitten. Gebruikers of beheerders kunnen dan het probleem oplossen of verkleinen. Men maakt vaak zo'n bericht als deze zwakke plekken staan in de lijst met Common Vulnerabilities and Exposures (CVE). 2. Adviesdiensten op het gebied van informatiebeveiliging en cybersecurity.	*CVE*
Security awareness	...	*Beveiligings-bewustzijn*
Security awareness training	Training gericht op het beveiligingsbewustzijn van medewerkers te vergroten. Een voorbeeld is een phishing-test.	

BEGRIP	BETEKENIS	ZIE OOK
Security by default	Aanduiding dat de maker of leverancier van een product ervoor zorgt het dat product standaard veilig is ingesteld. Degene die het product koopt of in gebruik neemt kan daar zelf wijzigingen in aanbrengen. Dit is in tegenstelling tot de situatie waarin een maker of leverancier van een product weinig of niks aan beveiliging doet. Degene die het product koopt of in gebruikt neemt is er dan helemaal zelf verantwoordelijk voor om het veilig in te stellen.	
Security by design	Een product, dienst of systeem ontwerpen en vanaf het begin ook de beveiliging mee ontwikkelen en testen.	
Security Information and Event Management	SIEM. Systeem waarin men informatie uit computersystemen verzamelt en analyseert. Het doel is om verdacht gedrag te ontdekken of zien dat iemand dingen in het systeem heeft veranderd, terwijl hij dat niet mocht.	*SIEM*
Security monitoring	Continu bewaken van een computer of digitaal netwerk met als doel om verdacht gedrag op te sporen.	
Security Operations Center	Afdeling, team of dienst dat digitale systemen en/of indentity's controleert en/of bewaakt en soms ook afhandelt.	*Security monitoring*
Security rating	Score die aangeeft hoe goed een persoon, netwerk of computer beveiligd is. Deze score wordt vaak automatisch berekend. Het helpt organisaties om te weten waar er risico's zijn.	
Security scan	...	*Vulnerability scan*
Security standaarden	Standaarden voor veiligheid die belangrijk zijn binnen de cybersecurity. Bijvoorbeeld over wat te doen om informatie te beveiligen. Voorbeelden zijn: ISO 2700x, NEN 7510, BIO, SOC1-2-3, ISAE3402, NIST-CSF en PCI-DSS.	

BEGRIP	BETEKENIS	ZIE OOK
Securitytest	Algemene naam voor testen die zijn bedoeld om zwakke plekken in een systeem te vinden. Geautomatiseerde scans horen hier niet bij.	
Security through obscurity	Digitaal systeem beveiligen door de beveiligingsmaatregelen geheim te houden. Het idee is dat iemand van buiten de organisatie moeilijker kan inbreken als hij niet weet hoe het systeem is beveiligd. Dit wordt over het algemeen niet gezien als een goede beveiligingsmethodiek.	*Obfuscation*
Security.txt	Een standaard die beschrijft hoe je een tekstbestand met contactinformatie kunt publiceren op je webserver. Hierin kunnen ethische hackers of cyberonderzoekers lezen met welke afdeling of persoon zij contact kunnen opnemen als zij een kwetsbaarheid vinden.	
Segregation of duties	...	*Functiescheiding*
Shift-left	Een benadering in softwareontwikkeling waarbij beveiliging zo vroeg mogelijk in het ontwikkelproces wordt geïntegreerd, zodat problemen vroegtijdig worden geïdentificeerd en kunnen worden voorkomen.	*DevSecOps*
Shift-right	Een woord zonder specifieke betekenis. Een stroming in risicomanagement en filosofie in cybersecurity die gebaseerd is op het uitgangspunt dat het goed gaat zo lang het niet fout gaat. Op basis hiervan worden alle beveiligingsmaatregelen en bijbehorende kosten uitgesteld (naar rechts op de tijdlijn) totdat ze absoluut onvermijdelijk zijn als gevolg van een incident, wetgeving of regulering.	
Service account	...	*Niet persoons-gebonden account*

BEGRIP	BETEKENIS	ZIE OOK
Severity	Hoe ernstig een zwakke plek van een digitaal systeem is.	
Sextortion	Sextortion maakt gebruik van niet-fysieke vormen van dwang om seksuele gunsten van een slachtoffer te krijgen. Sextortion is een vorm van seksuele uitbuiting waarin machtsmisbruik het dwangmiddel is, of het dreigen met vrijgeven van seksuele afbeeldingen of informatie.	
Shadow IT	Shadow IT is hardware of software binnen een organisatie die niet ondersteund wordt en opgezet is door de IT afdeling, maar wel een rol speelt in de bedrijfsvoering.	
Shell	Computerprogramma waarmee een gebruiker met een commandoregel opdrachten kan geven aan het besturingssysteem van een computer.	
Shodan	Zoekmachine voor alle systemen die op het Internet zijn aangesloten.	
Shoulder surfing	Meekijken over de schouder van een gebruiker van een digitaal systeem om informatie te verkrijgen, met het doel om de gegevens te misbruiken.	*Social engineering*
Side channel attack	Aanval die iemand uitvoert met informatie over de werking van een digitaal systeem. Denk aan timing, stroomverbruik of elektromagnetische lekken en niet aan normale beveiligingslekken. Het is informatie die in eerste instantie misschien niet nuttig lijkt maar die toch gebruikt kan worden om bijvoorbeeld informatie uit het systeem te stelen.	
SIEM	Security Information and Event Management.	*Security Information and Event Management*

BEGRIP	BETEKENIS	ZIE OOK
SIGINT	SIGnal INTelligence. Informatie verzamelen door signalen van elektronische communicatiekanalen op te vangen.	
Signature	1. Een specifiek patroon waaraan of waarmee men een cyberaanval kan herkennen. 2. Digitale handtekening.	
Signature based detection	Een techniek waarmee men aanvallen opspoort met hulp van vooraf afgesproken patronen, instructieregels of tekens.	
Signing	...	*Digitale handtekening*
SIM swapping	Het proces waarbij een kwaadwillende de telecomprovider van het slachtoffer overtuigt om het 06-nummer over te zetten naar een simkaart die in zijn bezit is.	
Single extortion	Situatie waarbij de bestanden of systemen van het slachtoffer zijn versleuteld en de sleutel tegen betaling wordt aangeboden.	*Triple en double extortion*
Single sign-on	Eindgebruikers loggen één keer in en kunnen daarna in verschillende applicaties en onderdelen van het netwerk werken. Ze hoeven dus niet meer elke keer opnieuw inloggegevens in te voeren. Bij single sign-on vertrouwt het systeem erop dat een ander systeem de identiteit van de gebruiker juist heeft vastgesteld en dat dit dus niet steeds opnieuw nodig is.	
Situational awareness	Het hebben van een overzicht van de (relevante) informatie en elementen binnen een ecosysteem, zodat goede voorspellingen kunnen worden gemaakt over risico's en dreigingen.	

BEGRIP	BETEKENIS	ZIE OOK
Skimmen	De gegevens van een bankpas of creditcard illegaal kopiëren. Als de eigenaar met de pas betaalt of geld pint, kopieert de crimineel de magneetstrip.	
Smishing	Vorm van phishing waarbij het phisingbericht per SMS-tekstbericht verstuurd wordt.	*Phishing*
Sniffen	De informatie die in een computernetwerk rondgaat, afluisteren en analyseren.	
SOAR	Security Orchestration, Automation and Response. Methode waarbij gecoördineerd en geautomatiseerd beveiligingstaken worden afgehandeld.	
SOC	Security Operations Center.	*Security Operations Center*
SOCaaS	SOC as a Service.	*SOC as a Service* *Security Operations Center*
SOC as a Service	Een Security Operations Center die als dienst aan klanten wordt aangeboden.	
Social engineering	Situatie als een aanvaller iemand misleidt door bijvoorbeeld in te spelen op nieuwsgierigheid of behulpzaamheid. Op deze manier probeert de aanvaller bijvoorbeeld aan informatie te komen om in een digitaal systeem in te breken.	
Software Defined Wide Area Network	De mogelijkheid om een Wide Area Netwerkverbinding centraal te beheren.	*SD-WAN*
Source code	...	*Broncode*
SPAM	Ongewenste e-mail, doorgaans commercieel van aard.	

BEGRIP	BETEKENIS	ZIE OOK
Spear phishing	Een variant van phishing die zich richt op één persoon of beperkte groep mensen, die specifiek wordt uitgekozen op basis van hun toegangspositie, om een zo groot mogelijk effect te sorteren zonder al te veel op te vallen.	*Phishing*
SPF	Sender Policy Framework. SPF is een techniek waarmee een domeinhouder de IP-adressen van verzendende mailservers kan publiceren in de Domain Name Server. Een ontvangende mailserver kan deze IP-adressen gebruiken om te controleren of een e-mail daadwerkelijk afkomstig is van een verzendende mailserver van de betreffende domeinhouder. Het gebruik van SPF verkleint de kans op misbruik van e-mailadressen doordat ontvangers betrouwbaar echte e-mails van phishingmails of spam kunnen onderscheiden.	*Domain Name Server*
Spionage	Aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie door statelijke of staatsgelieerde actoren.	*Cyberspionage*
Spoofing	Iemand misleiden door te doen alsof je iemand anders bent. Er zijn veel soorten spoofing. Een aanvaller kan zich in een email voordoen als een ander door het afzendadres te vervalsen.	
Spyware	Vorm van malware. Spyware is software waarmee men ongemerkt informatie verzamelt en doorstuurt naar een ander. Bij de informatie gaat het om toetsaanslagen, screenshots, e-mailadressen, surfgedrag of persoonlijke informatie zoals inloggegevens of een creditcardnummer.	
SQL injection	Een soort aanval op webapplicaties waarbij een aanvaller kwaadaardige SQL-code invoert in een invoerveld met als doel toegang te krijgen tot de database van de applicatie, deze te wijzigen of te vernietigen.	

BEGRIP	BETEKENIS	ZIE OOK
SSE	Secure Service Edge.	*Secure Service Edge*
SSL	Secure Sockets Layer.	*Secure Sockets Layer*
SSO	Single Sign On.	*Single sign on*
Staatsgelieerde actor	Actor gelieerd aan een statelijke actor.	*Statelijke actor*
State actor	...	*Statelijke actor*
Statelijke actor	Staten voeren digitale aanvallen uit op andere landen, organisaties of individuen uit primair geopolitieke motieven. Zij hebben als doel de verwerving van strategische informatie (spionage), beïnvloeding van de publieke opinie of democratische processen (beïnvloeding) of verstoring van vitale systemen (verstoring) of zelfs de vernietiging daarvan (sabotage).	
State-sponsored attack	Cyberaanval die een staat financiert of op een andere manier ondersteunt.	
Static Application Security Testing	Analyseert broncode in ontwikkeling om beveiligingszwakheden te identificeren.	
Stepping stone server	Beveiligde manier om in een digitaal netwerk te komen. Dit wordt ook wel een jumpserver genoemd.	
STIX	STIX is een op XML-gebaseerde gestructureerde taal om cyberdreigingsinformatie te beschrijven zodat deze op een consistente manier kan worden gedeeld, opgeslagen en geanalyseerd.	*TAXII*
Storing	...	*Uitval*

BEGRIP	BETEKENIS	ZIE OOK
Supply chain-aanval	Een actor tast doelbewust de vertrouwelijkheid, integriteit of beschikbaarheid aan van één of meer onderdelen binnen een supply chain (toeleveringsketen) om zo een springplank te krijgen voor aanvallen op andere organisaties, die veelal het primaire doelwit zijn. Actoren kunnen door middel van een supply chain-aanval bijvoorbeeld toegang verkrijgen tot beveiligde ICT-systemen van organisaties en daarmee onder andere tot diens gevoelige gegevens, processen en financiën. De aanval heeft een gelaagd karakter (minstens twee aanvallen) en is gericht, complex, duur en vereist daardoor vergaande capaciteit en planning van de actor. Het motief voor de aanval is meestal spionage, maar kan ook gericht zijn op sabotage of financieel gewin.	
Swag	Goodies die hackers krijgen om ze te bedanken voor hun gratis hulp om een informatiesysteem te beveiligen. Een bekend voorbeeld is een T-shirt met de tekst “I hacked…. and all I got was this lousy t-shirt”.	
Symmetrische versleuteling	Informatie onbegrijpelijk maken voor anderen. Bijvoorbeeld een tekstbestand of netwerkverkeer. Dit wordt gedaan met één sleutel, in tegenstelling tot asymmetrische versleuteling waarbij twee sleutels worden gebruikt. De ontvanger en verzender hebben dus allebei dezelfde sleutel. De informatie wordt onleesbaar gemaakt door de zender waarna de ontvanger deze weer leesbaar maakt, beide dus met dezelfde sleutel. Ze moeten deze sleutel op een vertrouwelijke manier met elkaar delen (bijvoorbeeld met behulp van asymmetrische versleuteling).	*Versleutelen*
Systeemmanipulatie	Het aantasten van de integriteit van digitale diensten, processen of systemen.	

BEGRIP	BETEKENIS	ZIE OOK
Tabletop exercise	Oefening waarbij een groep mensen in een kamer een bepaald incident naspeelt. De deelnemers zoeken samen naar een oplossing.	
Tailgating	Een techniek gebruikt door social engineers om ongeautoriseerd toegang te krijgen tot een beveiligde ruimte.	*Social engineering*
Tampering	Een digitaal systeem of informatie beschadigen door met opzet informatie, hardware en software te veranderen. Bijvoorbeeld een mail veranderen en versturen.	
TAXII	TAXII is een protocol voor het geautomatiseerd en in real-time uitwisselen van cyberdreigingsinformatie in STIX-formaat.	*STIX*
Terrorist	Actor met ideologische motieven die maatschappelijke veranderingen probeert te bewerkstelligen, bevolkingsgroepen angst wil aanjagen of politieke besluitvorming probeert te beïnvloeden, door geweld tegen mensen te gebruiken of ontwrichtende schade aan te richten.	
Testbed	Nagemaakte situatie waarin men testen kan doen.	
TIBER	Threat Intell Based Ethical Redteaming. Programma waarin (financiële) instellingen testen hoe weerbaar ze zijn tegen geavanceerde cyberaanvallen. Dit gebeurt met testaanvallen, die zijn gebaseerd op realistische dreiging.	
Threat	...	*Dreiging*
Threat actor	...	*Actor*
Threat hunting	...	*Hunting*

BEGRIP	BETEKENIS	ZIE OOK
Threat intell	...	*Threat Intelligence*
Threat intelligence	Inlichtingen en analyses over dreigingen.	
Threat management	Aanpak om bekende en onbekende dreigingen op te sporen en tegen te gaan. Men gebruikt hiervoor een combinatie van opsporingstechnieken.	
Threat Modeling	Een methode om zwakheden in computersystemen snel te herkennen zodat hierop kan worden ingespeeld.	
Time box	Vaste tijd waarin men bepaalde geplande activiteiten uitvoert. Is de tijd om, dan stopt het. Ook als de activiteiten nog niet klaar zijn.	
TLP	Traffic Light Protocol. Een methode, ontwikkeld door first.org, om data of informatie in te delen in klasses. Hoe men dit indeelt, hangt af van met wie men de informatie mag delen. De klasses zijn RED, AMBER, GREEN en WHITE. RED: de ontvanger of de ontvangers mogen de informatie alleen delen met de informatieverstrekker en met de mede ontvangers. AMBER: informatie mag alleen gedeeld worden binnen de ontvangende organisatie of met diens klanten op ‘‘need to know’-principe. GREEN: geeft aan dat de informatie uitsluitend onder gelijksoortige organisaties binnen de brede gemeenschap of sector gedeeld mag worden, dus wel op een gesloten Internetforum, maar niet op een openbaar toegankelijke website. WHITE: geeft aan dat er geen beperkingen aan de verspreiding zitten, informatie mag publiekelijk worden gedeeld.	

BEGRIP	BETEKENIS	ZIE OOK
TLS	Transport Layer Security.	*Transport Layer Security*
Toegangsbeheer	Controle om te bepalen wie naar binnen mag in een ruimte of digitaal systeem.	
Toezichthoudende domotica	Technologie en diensten in en om de woning met als doel het toezien op cliënten voor hun veiligheid, zoals uitluistersystemen, sensoren, camerabewaking en GPS-technologie.	*Domotica*
Toezichthouder	Een door de wetgever aangesteld, onafhankelijk en onpartijdig instituut dat toeziet op naleving van wet- en regelgeving door organisaties en (rechts)personen.	*Cyberbeveiligingswet, DORA, Europese- wet en regelgeving, Rijksinspectie Digitale Infrastructuur*
Token	Een middel dat men gebruikt om ergens in te mogen. Dat kan bijvoorbeeld een ruimte in een gebouw zijn of een digitaal systeem.	
TOTP	Time-based One Time Password.	*OTP*
Tokenisatie	Proces waarbij men een document met kwetsbare gegevens vervangt door andere gegevens die minder kwetsbaar zijn. Zo kan men bijvoorbeeld privacy beter garanderen.	
TOR	The Onion Router. Een methode om anoniemer op het Internet te kunnen surfen. TOR biedt ook toegang tot het Dark web.	*Dark web*

BEGRIP	BETEKENIS	ZIE OOK
TPM	1. Third Party Memorandum/Mededeling. Verklaring van een onafhankelijk onderzoeksbureau waarin staat hoe goed de ICT-dienstverlening en ICT-kennis van een organisatie zijn. 2. Trusted Platform Module. Internationale standaardeisen voor een veilige cryptoprocessor. De TPM is ontworpen om hardware te gebruiken in het beveiligen van sleutels en cijfercodes. Dit security model zorgt ervoor dat de sleutels niet gestolen kunnen worden.	
Traceback	Proces om iets terug te voeren naar de bron.	
Transport Layer Security	Standaard die zorgt voor beveiligde Internetverbindingen, met als doel de veilige uitwisseling van gegevens tussen Internetsystemen. Bijvoorbeeeld websites of mailservers. Dit maakt het voor cybercriminelen moeilijker om Internetverkeer te onderscheppen of te manipuleren. TLS is de opvolger van SSL.	*Cryptografie, authenticatie, SSL*
Triple extortion	Afpersing door middel van een combinatie van (1) bestanden of systemen van het slachtoffer versleutelen, (2) dreiging met openbaar maken van geëxfiltreerde informatie en (3) dreigen met uitvoeren van DDOS aanvallen op (herstelde) systemen.	*Ransomware, Single extortion, Double extortion*
Trojan	Type kwaadaardige software waarmee een aanvaller via een geheime ingang in een systeem kan komen. Vaak is deze verhuld in software die een gebruiker graag wil hebben en zelf installeert, zonder dat hij er zeker van is dat deze betrouwbaar is.	*Malware*
True negative	Niets doen zolang een digitaal systeem normaal werkt.	
True positive	Een aanval herkennen die ook echt een aanval is.	

BEGRIP	BETEKENIS	ZIE OOK
Trusted Third Party	Een entiteit die interacties tussen andere entiteiten faciliteert en door hen vertrouwd wordt.	*TPM*
TTP	Tactics, techniques and procedures. Tactieken, technieken en processen die een aanvaller gebruikt.	
Tweefactor authenticatie	...	*Meerfactor authenticatie*
Tweestapsauthenticatie	...	*Meerfactor authenticatie*
Two-factor authenticatie	...	*Meerfactor authenticatie*
Typosquatting	Een vorm van misbruik waarbij kwaadwillenden domeinnamen registreren met bewuste spelfouten om daarmee anderen te misleiden.	
Uitval	Een situatie waarin één of meer digitale processen zijn verstoord als gevolg van natuurlijke of technische oorzaken, of als gevolg van menselijke fouten.	
Uitvoeringswet AVG	De Nederlandse implementatiewet van de AVG (afgekort: UAVG). In de UAVG worden onderdelen van de AVG waarvoor dat is toegestaan op nationaal niveau verder uitgewerkt.	*AVG*
Unknown unknown	Onbekend en onkenbaar risico. Een risico dat pas ontdekt wordt wanneer het zich voor de eerst tijdens een incident toont.	
Update	Aanpassing van een bestaande versie van hard- of software. Deze repareert bekende zwakke plekken, zorgt eventueel voor nieuwe beveiliging en extra functies.	*Patch*
Upgrade	Nieuwe (geactualiseerde) versie van software, hardware of firmware.	

BEGRIP	BETEKENIS	ZIE OOK
URL-Shortening	Verkorten van de URL-link om het makkelijker te gebruiken. Maar vaak misbruikt door criminelen om de werkelijke (kwaadaardige) link te verhullen.	
Username	...	*Gebruikersnaam*
UVAG	...	*Uitvoeringswet AVG*
Verordening Cyberweerbaarheid	Nederlandse naam van der Cyber Resilience Act. Deze Europese verordening heeft tot doel heeft om consumenten en bedrijven te beschermen die producten of software met een digitale component kopen of gebruiken. Deze verordening legt verplichte beveiliging op aan dit soort producten en of software en legt de plicht bij fabrikanten om veilige producten te garanderen gedurende de levensduur van een apparaat of software. De verordening treedt in 2025 in werking. De wet dwingt bedrijven om cybersecurity niet langer als bijzaak, maar als kernonderdeel van hun productontwikkeling te beschouwen. Er is een overgangsperiode van 24 maanden ingevoerd zodat producten en processen kunnen worden aangepast aan de nieuwe eisen.	*Cyber Resilience Act*
Versleutelen	Het versleutelen van informatie om deze onleesbaar te maken voor onbevoegden. Dit wordt gedaan met één of twee sleutels (symmetrische danwel asymmetrische versleuteling). De informatie wordt onleesbaar gemaakt door de zender waarna de ontvanger deze weer leesbaar maakt, met behulp van de sleutel(s). Men versleutelt informatie bijvoorbeeld om deze veilig te versturen of bijvoorbeeld om vast te stellen dat een bericht ook echt komt van degene die zegt dat hij het heeft verstuurd.	*Cryptografie, Ontsleutelen*
Verstoring	Een aantasting van de beschikbaarheid, integriteit of vertrouwelijkheid van informatie(verwerking).	*Uitval*

BEGRIP	BETEKENIS	ZIE OOK
Vertrouwelijkheid	De zekerheid dat informatie en/of digitale diensten, processen of systemen alleen toegankelijk zijn voor personen of software die hiertoe zijn geautoriseerd.	*AVG*
Verwerkers-overeenkomst	Een verplichte overeenkomst tussen de verwerkingsverantwoordelijke en verwerker die hun onderlinge afspraken over de verwerking van persoonsgegevens regelt.	
Verwerkings-verantwoordelijke (controller)	De partij die het doel en de middelen voor de verwerking van persoonsgegevens bepaalt. Een verwerkingsverantwoordelijke kan persoonsgegevens zelf verwerken, of bij de verwerking gebruik maken van een verwerker.	*AVG*
Virtual Machine (VM)	Een computerprogramma dat een computer nabootst waarop men andere programma's kan uitvoeren. Zo kan men op één echte computer meerdere virtuele computers laten draaien en hardware delen.	
Virtual private network	Uitbreiding van een computernetwerk over een openbaar netwerk. Via die uitbreiding kunnen gebruikers vanaf elke plek veilig gegevens delen met het computernetwerk. Voor de gebruikers is het alsof ze rechtstreeks op het netwerk zijn aangesloten. De veilige verbinding valt te omschrijven als een tunnel en wordt afgekort VPN genoemd.	
Virtual private server	Een virtuele machine die als dienst wordt verkocht door een hostingpartij. Dit wordt ook wel een virtual dedicated server genoemd. Een VPS wordt doorgaans aangeboden met een geïnstalleerde kopie van een besturingssysteem, zoals Windows of Linux. De klant krijgt daarbij een account met systeemrechten op de VPS, zodat de klant kan inloggen op de VPS. Een VPS vertoont veel overeenkomsten met een fysieke server met het belangrijkste verschil dat de onderdelen van de VPS virtueel (softwarematig) zijn en daardoor makkelijker aan te passen.	

BEGRIP	BETEKENIS	ZIE OOK
Virus	...	*Malware*
Vishing	Voice phishing.	*Voice phishing*
Vitale infrastructuur	...	
Vitale processen	Bepaalde processen zijn zo essentieel voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid. Deze processen vormen de Nederlandse vitale infrastructuur. Elektriciteit, toegang tot internet, drinkwater en betalingsverkeer zijn voorbeelden van vitale processen.	*Vitale processen*
Voice phishing	Vorm van phishing waarbij een aanvaller belt met een gebruiker en probeert om van hem of haar vertrouwelijke informatie te krijgen om met deze informatie te proberen in een digitaal systeem te komen.	*Phishing*
VPN	...	*Virtual private network*
Vrijwaringsverklaring	Verklaring waarin men toestemming geeft om een beveiligingsonderzoek te doen en om de onderzoeker te vrijwaren van schade die hij mogelijk door dit onderzoek veroorzaakt bij professionele uitvoering ervan. Ook staat erin waaraan het onderzoek moet voldoen. Deze verklaring gebruikt men bijvoorbeeld voor een penetratietest.	

BEGRIP	BETEKENIS	ZIE OOK
Vulnerability	...	*Kwetsbaarheid*
Vulnerability assessment	Uitputtend onderzoek bij een organisatie waarbij alle tot op dat moment bekende kwetsbaarheden worden onderzocht in een digitaal systeem. Een deel wordt handmatig uitgevoerd, waardoor dit een vergaander onderzoek is dan een vulnerability scan.	*Vulnerability scan*
Vulnerability management	Handmatige controle waarbij men zwakke plekken in een systeem opspoort. Men bepaalt vooraf hoe men dat doet. Bij een vulnerability assessment probeert men alle zwakke plekken te vinden in een klein gebied. Dat is anders dan bij een penetratietest waarbij men zo diep mogelijk in een systeem wil komen.	
Vulnerability scan	Geautomatiseerd onderzoek bij een organisatie waarbij kwetsbaarheden worden onderzocht in een digitaal systeem.	*Vulnerability assessment*
WAAP	Web Application & API Protection.	*Web Application & API Protection*
Wachtwoord	Reeks van letters, cijfers en of andere karakters waarmee een gebruiker in een digitaal systeem kan komen. Het is de bedoeling dat een gebruiker dit wachtwoord niet aan anderen geeft en een sterk wachtwoord kiest zodat dit moeilijk te kraken is door aanvallers.	*Inlogcode*
Wachtwoordkluis	...	*Wachtwoord-manager*
Wachtwoordmanager	Een tool die meerdere wachtwoorden opslaat in een veilige digitale kluis waardoor de gebruiker alleen nog maar het wachtwoord van de kluis hoeft te onthouden.	

BEGRIP	BETEKENIS	ZIE OOK
WAF	Web Application Firewall.	*Web Application Firewall*
Wbdwb	Wet bevordering digitale weerbaarheid bedrijven.	*Wet bevordering digitale weerbaarheid bedrijven*
Wbni	Wet beveiliging netwerk- en informatiesystemen.	*Wet beveiliging netwerk- en informatiesystemen*
Web Application Firewall	Een specifieke vorm van applicatie-firewall die digitaal verkeer van en naar een webservice filtert, bewaakt en blokkeert.	
Weerbaarheid	...	*Cyber-weerbaarheid*
Wet bevordering digitale weerbaarheid bedrijven	Een wet met als doel om het Nederlandse bedrijfsleven te voorzien van algemene informatie, het stimuleren van samenwerking tussen organisaties en het delen van specifeke (dreigings)informatie aan individuele bedrijven. Het Digital Trust Center voert deze wet uit.	*Digital Trust Center*
Wet beveiliging netwerk- en informatiesystemen	Wet beveiliging netwerk- en informatie-systemen (Wbni). Nederlandse wet die bepaalt aan welke eisen aanbieders van essentiële diensten (AED's) en digitale diensten (DSP's) moeten voldoen. Deze wet voert uit wat er staat in de Europese Netwerk- en Informatiebeveiligingsrichtlijn (NIB). De Wbni wordt vervangen door de Cyberbeveiligingswet.	*Cyber-beveiligingswet, NIS2, Europese wet- en regelgeving*
Whaling	Manier om vertrouwelijke informatie (zoals persoonlijke data van werknemers) of geld van een organisatie te stelen. Meestal gebeurt dit door een valse e-mail te sturen uit naam van iemand die de werknemer vertrouwt. Via deze e-mail wordt de werknemer verleid om bedrijfsgegevens te onthullen of een grote betaling te autoriseren.	*CEO-Fraude (BEC-Fraude)*

BEGRIP	BETEKENIS	ZIE OOK
Whatsapp fraude	Vorm van oplichting waarbij het slachtoffer denkt een bekende, vaak een zoon of dochter, te helpen met een betaling.	
White Team	Oefening waarbij een organisatie aanvallen simuleert om te ontdekken hoe goed ze is beschermd tegen aanvallen. Soms is er ook een White team. Dit team zorgt dat de oefening haar doel bereikt. Bijvoorbeeld door te bepalen welke informatie de beide (Blue en Red) teams krijgen.	*Red Team, Red teaming, Blue teaming, Purple teaming*
Whitebox test	Veiligheidstest die aangeeft dat de tester veel voorkennis van het te onderzoeken computersysteem heeft, zoals bijvoorbeeld toegang tot de broncode, logbestanden en toegang tot een eenvoudig gebruikersaccount.	*Blackbox test, Crystalbox test, Greybox test*
Whitehat hacker	Iemand die inbreekt in een digitaal systeem met positieve intenties. Het doel is beveiligingslekken op te sporen. De term 'white hat' komt uit cowboyfilms waarin de held altijd een witte hoed droeg. Een whitehat hacker wordt ook wel een ethische hacker genoemd.	*Hacker, greyhat hacker, blackhat hacker*
Whitelisting	...	*Allow listing, blacklisting, blocklisting, deny-listing, whitelisting*
Worm	Kwaadaardige code die zichzelf, zonder tussenkomst van een mens, vermenigvuldigt en verspreidt over verschillende digitale systemen. Bekende voorbeelden van wormen zijn Wannacry en Notpetya.	*Malware*

BEGRIP	BETEKENIS	ZIE OOK
XaaS	Algemene naam voor het uitbesteden van diensten. Bij cloud computing heet het IaaS (Infrastructure as a Service), PaaS (Platform as a Service) en Saas (Software as a Service). Andere voorbeelden zijn DaaS (Database as a Service) en BaaS (Blockchain as a Service).	
XDR	Extended Detection and Response. Een detectie- en responsplatform dat verschillende technieken combineert voor een betere verdediging.	*Cross Site Scripting*
XSS	Cross Site Scripting.	*Worm*
Zero-click aanval	Veel voorkomende cyberaanvallen, zoals phishing, dwingen een gebruiker tot actie. Bij een zero-click aanval is dit niet nodig. Ze werken ook zonder dat een gebruiker ergens op 'klikt'.	
Zero-day	1. Afkorting voor zero-day vulnerability. Een kwetsbaarheid waarvoor nog geen patch beschikbaar is, omdat de maker van de kwetsbare software nog geen tijd (nul dagen) heeft gehad om de kwetsbaarheid te verhelpen.De zwakke plek is pas een risico als er een exploit voor is gemaakt die de zwakke plek effectief weet te misbruiken. 2. Afkorting voor zero-day exploit. Een zero day exploit is een speciale exploit. Hij is speciaal omdat de zwakke plek die wordt misbruikt niet bij de leverancier bekend is en dus ook nog niet is hersteld. Omdat de zwakke plek nog niet bekend is, kan niemand zich er goed tegen beschermen. Daarom is een zero day exploit heel waardevol voor aanvallers. Ontdekkers van zero days kunnen ze voor veel geld verkopen aan criminelen of inlichtingendiensten.	

BEGRIP	BETEKENIS	ZIE OOK
Zero trust	Hoe een intern netwerk qua onderling vertrouwen is ingericht. Het uitgangspunt is: vertrouw niets of niemand, controleer altijd of een gebruiker of computer wel is wie hij zegt te zijn. Een gebruiker mag alleen in een digitaal systeem als het systeem heeft gecontroleerd wie hij is en waar hij is.	
Zero Trust Architecture (ZTA)	Een model voor security-architectuur waarbij een aantal principes leidend zijn. Zo geeft de plaats waar een apparaat zich in het netwerk bevindt het apparaat geen verhoogde toegang (het netwerk wordt niet vertrouwd). Naast gebruikers moeten ook apparaten geauthenticeerd worden. Door meerlaagse security checks wordt vertrouwen zoveel mogelijk vervangen door controles. Informatie wordt altijd versleuteld uitgewisseld.	
Zombie-computer	Computer die is besmet met een bot. De naam zombie komt van het idee dat de eigenaar niet merkt dat de computer door een aanvaller wordt misbruikt.	*Bot, botnet*
Zone	Een verzameling apparatuur waaraan dezelfde beveiligingseisen worden gesteld.	
Zonering	Het opdelen van een netwerk in verschillende niveaus van betrouwbaarheid.	*Netwerk-segmentatie, compartimentering*
Zorgplicht	De plicht die organisaties hebben om de producten en diensten die zij bieden veilig te maken om het risico op aanvallen te verkleinen. En om de gevolgen van een aantal te verkleinen als die er toch komt.	*Cyber-beveiligingswet, DORA, Europese- wet en regelgeving, Bestuurs-aansprakelijkheid*

Het Cybersecurity Woordenboek is mede mogelijk gemaakt door:

- Achmea
- Alert Online
- Algemene Inlichtingen en
- Veiligheidsdienst (AIVD)
- AON
- Audittrail
- Axxemble
- Betaalvereniging Nederland
- Bitdefender
- Canon Production Printing
- Chubb
- Cisco
- Compumatica
- Computest
- Connect2trust
- Cybersprint
- CyberTGR
- Cyberveilig Nederland
- Data Expert
- Deep Blue Security
- Demiroz Consultancy B.V.
- Digital Trust Center / Ministerie Econonomische Zaken
- DINL: Digitale - Infrastructuur Nederland
- DIVD: Dutch Institute for Vulnerability Disclosure
- ECP | Platform voor de Informatie Samenleving
- Eneco
- ERP Security
- ESET Nederland
- Eurofins
- Eviden
- Fortinet
- Forum Standaardisatie
- Fox-IT
- Gemeente Den Haag
- Gemeente Rotterdam
- Guardian360
- Haagse Hogeschool
- HackDefense
- Hoffmann
- Hogeschool NOVI
- Hudson Cybertec
- Informatiebeveiliging.nl
- KIWA
- KnowBe4
- KPN Security
- Mazars
- Microsoft
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- Ministerie van Defensie/ Defensie Cyber Expertise Centrum
- Ministerie van Economische Zaken
- Ministerie van Infrastructuur en Waterstaat
- Ministerie van Volksgezondheid, Wetenschap en Sport
- MKB Cyberadvies Nederland
- Nationale Politie
- NBIP
- NCSC: Nationaal - Cybersecurity Centrum
- NCTV: Nationaal Coördinator Terrorisme en Veiligheid
- NIDV
- Northwave
- Onsnet
- Onvio
- Onyx Cybersecurity
- Openbaar Ministerie
- Parell
- Philips
- Platform voor - Informatiebeveiliging (PVIB)
- Purasec
- QVOX
- Rabobank
- Rijkswaterstaat
- Scalys
- Secura
- Secure IT
- Securify
- Security Delta (HSD)
- SecWatch
- Siemens Nederland
- Sopra Steria
- SURF
- Technische Universiteit Delft
- Tesorion
- Topicus
- TÜV Nederland
- Universiteit Leiden
- Verbond van Verzekeraars
- VNO NCW
- Waternet AVG
- Z-CERT
- Zerocopter
- Zuyd Hogeschool

Colofon

Cybersecurity Woordenboek. Van cybersecurity naar Nederlands.
4e druk

Uitgever: Cyberveilig Nederland i.s.m.
ECP. Platform voor de Informatiesamenleving
Redactie: Petra Oldengarm, Liesbeth Holterman, Ellis Brouwer

www.cyberveilignederland.nl/woordenboek
ISBN 9789083026466

CYBERVEILIG NEDERLAND

ECP Platform voor de InformatieSamenleving

RANSOMWARE BACK-U
PATCH TRIPLE EXTORTIO
MALWARE PENTEST
BULLETPROOF ANGE
AIR GAP ASSURANC
KLIKFRAUDE HOSTIN
WACHTWOORDKLUIS

RANSOMWARE BACK UP

PATCH TRIPLE EXTORTION

MALWARE PENTEST

BULLETPROOF ANGEL

AIR GAP ASSURANCE

KLIKFRAUDE HOSTING

WACHTWOORDKLUIS

Cybersecurity Woordenboek

4e druk