Afkortingen- en begrippenlijst

0-day	Zie Zero-daykwetsbaarheid.
Aanval	Een digitale aanval is een opzettelijke inbreuk op cybersecurity.
Aanvalsfacilitato	Actor die middelen en infrastructuur ontwikkelt en uitbaat om tegen betaling andere actoren in staat te stellen digitale aanvallen uit te voeren.
Actor	Persoon, groep of organisatie die een dreiging vormt.
AIVD	Algemene Inlichtingen- en Veiligheidsdienst.
AP	Autoriteit Persoonsgegevens.
Authenticatie	Het vaststellen van de identiteit van een gebruiker, computer of applicatie.
Beschikbaarheid	Beschikbaarheid betreft het waarborgen, dat vanuit hun functie geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen (informatiesystemen).
Bitcoin	Digitale munteenheid, zie cryptovaluta.
Botnet	Een verzameling van besmette systemen die door actoren centraal bestuurd kan worden. Botnets vormen de infrastructuur voor veel vormen van internetcriminaliteit.
Clouddienst	Ict-infrastructuur die via het internet beschikbaar wordt gesteld als dienst.
Crimineel	Actor die aanvallen pleegt met economische of financiële motieven.
Cryptojacking	Het (zonder medeweten van de eigenaar) gebruiken van de rekenkracht van systemen om cryptovaluta te delven.

Cryptomining	Het delven van cryptovaluta door het uitvoeren van cryptografische berekeningen.
Cryptovaluta	Verzamelnaam voor digitale munteenheden die cryptografische berekeningen gebruiken als echtheidskenmerk en voor transacties.
Cvd	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.
Cybercrime	Vorm van criminaliteit gericht op ict of de informatie die een ict-systeem verwerkt. Er zijn verschillende soorten cybercrime:• in enge zin, een vorm van criminaliteit met ict als doelwit (high tech crime);• een vorm van criminaliteit waarbij voor de uitvoering het gebruik van ict van overwegende betekenis is (cybercriminaliteit);• in brede zin, iedere vorm van (traditionele) criminaliteit waarbij gebruik wordt gemaakt van ict (gedigitaliseerde criminaliteit).
Cybercrime-as-a-service (Caas)	Cybercrime-as-a-service is een werkwijze in de ondergrondse economie waarbij actoren gebruik kunnen maken van de (betaalde) diensten van aanvalsfacilitatoren om aanvallen te plegen.
Cybervandaal	Zie scriptkiddie.
Cybersecurity	Cybersecurity is het geheel aan maatregelen om schade door verstoring, uitval of misbruik van ict te voorkomen en, indien er toch schade is ontstaan, het herstellen hiervan. Die schade kan bestaan uit de aantasting van de beschikbaarheid, vertrouwelijkheid of integriteit van informatiesystemen en informatiediensten en de daarin opgeslagen informatie.
DDoS	Distributed Denial of Service is een vorm van Denial-of-Service waarbij een bepaalde dienst (bijvoorbeeld een website) niet beschikbaar wordt gemaakt door deze te bestoken met veel netwerkverkeer vanuit een groot aantal verschillende bronnen.
Defacement	Een defacement (of bekladding) is het vervangen van een webpagina met de boodschap dat deze gehackt is, eventueel met aanvullende boodschappen van activistische, idealistische of aanstootgevende aard.
DKIM	DomainKeys Identified Mail is een protocol om legitieme e-mail door de verzendende e-mailserver digitaal te laten ondertekenen. De eigenaar van het verzendende domein publiceert legitiem sleutels in een DNSrecord.
DMARC	Domain-based Message Authentication, Reporting and Conformance is een protocol waarmee de eigenaar van een domein aangeeft wat er met niet-authentieke e-mail vanaf zijn domein moet gebeuren. De authenticiteit van de e-mail wordt eerst vastgesteld aan de hand van SPF en DKIM. De domeineigenaar publiceert het gewenste beleid in een DNS-record.

DNS	Het Domain Name System is het systeem dat internetdomeinnamen koppelt aan ip-adressen en omgekeerd. Zo staat het adres www.ncsc.nl bijvoorbeeld voor ip-adres 159.46.193.36. Verder vermeldt een DNS-record onder meer hoe e-mails aan dat domein afgehandeld moeten worden.
DoS	Denial of Service is 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 DDoS-aanval uitgevoerd.
Encryptie	Het versleutelen van informatie om deze onleesbaar te maken voor onbevoegden.
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.
Exploitkit	Hulpmiddel om een aanval op te zetten door te kiezen uit kant-en-klare exploits, in combinatie met gewenste gevolgen en besmettingsmethode.
Hacker/Hacken	De meest gangbare en de in dit document gehanteerde betekenis van hacker is iemand die met kwaadaardige bedoelingen probeert in te breken in ict-systemen. Oorspronkelijk werd de term hacker gebruikt voor iemand die op onconventionele wijze gebruikmaakt van techniek (waaronder software), veelal om beperkingen te omzeilen of onverwachte effecten te bereiken.
Hacktivist	Samentrekking van hacker en activist: actor die uit ideologische motieven digitale aanvallen van activistische aard pleegt.
ICS	Industriële controlesystemen zijn meet- en regelsystemen, bijvoorbeeld voor de aansturing van industriële processen of gebouwbeheersystemen. ICS verzamelen en verwerken meet- en regelsignalen van sensoren in fysieke systemen en regelen de aansturing van de bijbehorende machines of apparaten.
Incident	Een incident is een gebeurtenis waarbij informatie, informatiesystemen of -diensten verstoord worden, uitvallen of misbruikt worden.
Informatiebeveiliging	Informatiebeveiliging is het proces van het vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit, alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.
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.
Injectie	Aanvalstechniek waarbij gebruikersinvoer wordt gemanipuleerd om naast gegevens ook systeemopdrachten te bevatten. SQL-injectie wordt vaak gebruikt om communicatie tussen een applicatie en de achterliggende database te beïnvloeden, om gegevens te manipuleren of stelen.

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.
Integriteit	Integriteit omhelst het waarborgen van de juistheid en volledigheid van informatie en de verwerking ervan.
IoT	Het internet of things is 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.
IP	Het internetprotocol zorgt voor de adressering van internetverkeer zodat het bij het beoogde doel aankomt.
Kwetsbaarheid	Eigenschap van een samenleving, organisatie of informatiesysteem (of een onderdeel daarvan) die een kwaadwillende partij de kans geeft om de legitieme toegang tot informatie of functionaliteit te verhinderen en te beïnvloeden, of om die ongeautoriseerd te benaderen.
Lek	Aantasting van de vertrouwelijkheid als gevolg van natuurlijk, technisch of menselijk falen.
Malware	Samentrekking van malicious software. Malware is de term die als generieke aanduiding wordt gebruikt voor onder andere virussen, wormen en trojans.
Middel	Een techniek of computerprogramma waarmee een aanvaller misbruik kan maken van bestaande kwetsbaarheden of deze kan vergroten.
MIVD	Militaire Inlichtingen- en Veiligheidsdienst.
Phishing	Verzamelnaam voor digitale activiteiten die tot doel hebben informatie van mensen te ontfutselen. Deze informatie kan worden misbruikt voor bijvoorbeeld fraude of identiteitsdiefstal.
Ransomware	Gijzelsoftware. Type malware dat systemen of informatie daarop blokkeert en alleen tegen betaling van losgeld weer toegankelijk maakt.
Sabotage	Het opzettelijk, zeer langdurig, aantasten van de beschikbaarheid van informatie, informatiesystemen of - diensten. In extreme gevallen leidend tot vernietiging.
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.
Spam	Ongewenste e-mail, doorgaans commercieel van aard.
Spearphishing	Spearphishing is 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.

SPF	Sender Policy Framework is een protocol waarmee de eigenaar van een domeinnaam aangeeft welke servers er legitiem e-mail namens zijn domein mogen versturen. De domeinnaameigenaar publiceert de lijst met geautoriseerde servers in een DNS-record.
Spionage	Aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie door statelijke of staatsgelieerde actoren.
Staatsgelieerde actor	Actor gelieerd aan een 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).
Storing	Zie uitval of verstoring.
Systeemmanipulatie	Het aantasten van informatiesystemen en -diensten gericht op de vertrouwelijkheid of integriteit van informatiesystemen en -diensten. Deze systemen of diensten worden daarna ingezet om andere aa vallen uit te voeren.
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.
Trojan	Type malware dat heimelijk toegang tot een systeem biedt aan een aanvaller via een achterdeur.
Tweefactorauthenticatie	Een manier van identiteit vaststellen waarvoor twee onafhankelijke bewijzen van identiteit zijn vereist.
Uitval	Aantasting van de integriteit en beschikbaarheid als gevolg van natuurlijk, technisch of menselijk falen.
Verstoring	Het opzettelijk, tijdelijk, aantasten van de beschikbaarheid van informatie, informatiesystemen of - diensten.
Vertrouwelijkheid	Met vertrouwelijkheid wordt gedoeld op het waarborgen dat informatie alleen toegankelijk is voor degenen, die hiertoe zijn geautoriseerd.
Wiperware	Type malware dat sabotage pleegt door gegevens te verwijderen of permanent ontoegankelijk te maken.
Worm	Type malware dat zichzelf automatisch verspreidt onder andere systemen.
Zero-daykwetsbaarheid	Een zero-daykwetsbaarheid is 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.