

Cybersecurity Woordenboek



Van cybersecurity naar Nederlands

Van access control tot zero-day

De Nederlandse taal krijgt er in rap tempo nieuwe woorden bij. De Dikke van Dale alleen volstaat niet meer, want onze huidige maatschappij kent een hoge mate van ontwikkeling in het digitale domein. Een domein dat continu in beweging is om aan de behoefte van de samenleving te kunnen voldoen. De bijbehorende terminologie is niet voor iedereen makkelijk te begrijpen. Woorden als access control en zero-day worden op technisch vlak veel gebruikt, maar de precieze betekenis is buiten het vakgebied vaak onbekend. Er was dringend behoefte aan een Cybersecurity Woordenboek – een soort Dikke Digitale dus.

Vandaar dit initiatief van de Cybersecurity Alliantie en Cyberveilig Nederland. Een woordenboek dat de technische professional verbindt met andere professionals, die steeds meer met cybersecurity te maken krijgen. Als coördinerend minister voor cybersecurity presenteer ik met trots dit initiatief. Waarom dit woordenboek zo belangrijk is? We kunnen pas tot een digitaal veilig Nederland komen als alle betrokkenen weten waar ze het over hebben. Zo werken we samen aan een digitaal weerbaar Nederland.

In 2018 is de Nederlandse Cybersecurity Agenda (NCSA) gepubliceerd. Dit was het startschot voor een integrale aanpak van cybersecurity. Een samenwerking van partijen uit de publieke en private sector, de wetenschap en de samenleving. De Cybersecurity Alliantie is een van de initiatieven die is voortgekomen uit de NCSA. Dit platform voert concrete, kortlopende projecten uit die bijdragen aan een digitaal weerbaar Nederland. Een van die resultaten ligt voor u, in de vorm van een praktisch hulpmiddel om de digitale wereld inhoudelijk beter te begrijpen.

Onder leiding van Cyberveilig Nederland hebben ruim 60 organisaties, overheidspartijen en private partijen meegewerkt aan de samenstelling van het woordenboek. Er is een verklarende woordenlijst opgesteld met bijna 600 cybersecuritytermen om bijvoorbeeld rapporten, adviezen of offertes beter te begrijpen. Geen geheimtaal meer, maar begrippen met een heldere toelichting. Deze kennis geeft mensen het vertrouwen dat ze elkaar begrijpen. En vertrouwen in het digitale domein is essentieel in onze maatschappij.

Ferd Grapperhaus

Minister van Justitie en Veiligheid

Inleiding Cybersecurity

Woordenboek

Met trots presenteren wij de eerste druk van het Cybersecurity Woordenboek, waarin we de betekenis van veelvoorkomende cybertermen hebben uitgelegd.

Het Cybersecurity Woordenboek is het resultaat van een samenwerking van ruim 60 organisaties in Nederland én financiering vanuit de Cyber Security Alliantie, het ministerie van Economische Zaken en Klimaat en Cyberveilig Nederland.

In het woordenboek staan bijna 600 cybersecurity woorden uitgelegd in begrijpelijke taal. Op deze manier wordt het voor gebruikers van cybersecuritydiensten makkelijker om met specialisten het gesprek aan te gaan, technische rapporten en adviezen te begrijpen en offertes te beoordelen.

Het woordenboek is gemaakt met de volgende uitgangspunten:

1. De opgenomen termen worden veel gebruikt bij de afnemers van cybersecuritydiensten. Het woordenboek is daarom geschreven op een wijze dat niet-vakspecialisten de betekenissen goed kunnen begrijpen.
2. In deze eerste druk hebben we 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). We hopen natuurlijk wel dat een deel

van de definities definiërend zal worden (bijvoorbeeld die over de verschillende vormen van dienstverlening).

3. De termen in het woordenboek gaan uit van de context van cybersecurity. Daarom hebben we zo veel mogelijk de toevoeging ‘cyber’ weggelaten bij zowel de uitleg als de opgenomen vaktermen (met uitzondering van de woorden cyberaanval en cybersecurity).

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

5. Algemene termen die nog niet erg lang worden gebruikt binnen het cybersecuritydomein hebben we in deze eerste druk opgenomen. Voorbeelden zijn OT, SCADA, quantum computing en blockchain. Bij een nieuwe editie worden deze heroverwogen.

6. Overheidsorganisaties die als wettelijke (dienstverlenende) taak een sterke link hebben met cybersecurity zijn opgenomen. Bijvoorbeeld: het Nationaal Cyber Security Centrum (NCSC), het Digital Trust Centre (DTC) en de Autoriteit Persoonsgegevens. Niet opgenomen zijn: Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en Agentschap Telecom.

7. 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.

8. In het woordenboek geven we een uitleg bij de Nederlandse termen. De Engelse termen verwijzen naar de Nederlandse. Uitzonderingen zijn de termen die geen gangbare Nederlandse variant kennen, zoals Chief Information Security Officer (CISO). Dan is alleen de Engelse term opgenomen.

9. Voorbeelden van kwetsbaarheden zijn niet allemaal opgenomen, wel de vaktermen die voorkomen in de uitleg van de OWASP top 10 2017.

10. Namen van aanvallen en malware zijn niet opgenomen in de lijst. Ook niet wanneer deze veel media-aandacht hebben gekregen zoals Stuxnet, Wanacry en Notpetya.

11. 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 cybersecuritydiensten worden besproken. Voorbeelden zijn: TLS, SPF, DKIM, SSL.

12. 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.

13. Er is een fopwoord opgenomen in het woordenboek, vergelijkbaar met de fopwoorden uit vroegere woordenboeklijsten.

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

15. We gebruiken bij de uitleg van de termen “digitaal systeem” als verzamelnaam voor woorden als computer, computersysteem, computernetwerk. 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! Natuurlijk valt er ook nog veel te verbeteren aan de woordenlijst. Dat zullen we gaan doen in de tweede druk. Alle feedback is daarom zeer welkom!

Petra Oldengarm

Directeur Cyberveilig Nederland

Begrip

Betekenis

Zie ook

2-stapsverificatie

Tweefactor authenticatie.

Meerfactor authenticatie

2-trapsverificatie

Tweefactor authenticatie.

Meerfactor authenticatie

2FA

Twee Factor Authenticatie.

Meerfactor authenticatie

AAA

Authenticatie, autorisatie en accounting.

Aanval

Actie waarbij iemand met opzet de beveiliging probeert uit te schakelen of te omzeilen om in een digitaal systeem te komen.

Aanvalsfacilitator

Persoon die software, computers en netwerken ontwikkelt en verkoopt zodat anderen hiermee digitale aanvallen kunnen uitvoeren.

Aanvalsoppervlak

Het aantal manieren dat een aanvaller kan gebruiken om een digitaal systeem aan te vallen.

Aanvalsvector

Aanvalsvector

Een manier die een aanvaller kan gebruiken om in een digitaal systeem te komen.

Aanvalsoppervlak

Acceptable risk level

...

Risico acceptatie

Access control

...

Toegangsbeheer

Access Control List (ACL)

Een lijst waarop staat wie welke toegang en/of bevoegdheden heeft in een

informatiesysteem of onderdeel ervan.

Account

Stukje van een digitaal systeem waartoe een gebruiker toegang heeft. 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.

Inlogcode, wachtwoord, meefactorauthenticatie

Accountability

Verantwoordelijk worden gehouden voor het eindresultaat.

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

Een manier om via een ongewone 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.

Actor

Persoon, groep of organisatie die een digitaal systeem dreigt aan te vallen. Voorbeelden zijn: scriptkiddie, hacktivist, kwaadwillende medewerker, statelijke actor of een criminele actor.

Admin

...

*Administrator***Administrator**

Beheerder van een computersysteem 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.

Adversary simulation

Oefening waarbij een organisatie aanvallen naspeelt 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. Bijvoorbeeld door te bepalen welke informatie de beide teams krijgen. De samenwerking tussen het Red team en het Blue team heet ook wel purple teaming. Bij een Red team oefening 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 sys-

*Red team**Blue team**White team**Purple team*

teem binnen te dringen.

Adware

Kwaadaardige software die men in een computer zet, vaak zonder dat de gebruiker dat merkt. De software verzamelt informatie uit de computer. Die informatie gebruikt men om via advertenties doelgerichte reclame naar de gebruiker te sturen.

Malware

AED

Aanbieder van Essentiële Diensten. Een aanbieder die vanuit de Wet beveiliging netwerk- en informatiesystemen (Wbni) rechten en plichten heeft op het gebied van cybersecurity.

Agent

Speciaal computerprogramma dat leert van zijn eigen ervaringen. Men zet het vaak in voor een bepaald doel, bijvoorbeeld om een netwerk beter te beveiligen. Het programma is zelflerend en moet daarom heel betrouwbaar zijn.

AI

Artificial Intelligence.

Kunstmatige intelligentie

Air gap

Maatregel die ervoor zorgt dat een component of computer of netwerk niet meer verbonden is met een ander netwerk zoals internet.

Algoritme

Een proces, stappenplan of een serie regels die een computer moet volgen om een probleem of rekensom

op te lossen. Het lijkt op een soort recept.

Angel

1. Vrijwilliger op een hackerscongres.
2. Eerste investeerder in een bedrijf.

Anomaly

Iets wat afwijkt van het normale gedrag van een netwerk, computer, laptop, smartphone of ander digitaal apparaat, vaak veroorzaakt door malware of een hacker.

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

Anonymity

De opzet van het internet maakt het mogelijk om anoniem te handelen. Men kan dus niet achterhalen welke persoon of machine iets doet. Dit levert een bijdrage aan de vrijheid van meningsuiting en vrijheid van informatie. Maar het maakt het ook moeilijker om criminelen op te sporen.

Anonymization

Techniek waarbij data geanonimiseerd worden. Dit betekent dat men bepaalde kenmerken van de data weghaalt zodanig dat ze niet terug te halen zijn. Door deze kenmerken kun je achterhalen bij wie of wat de data horen.

Anomaly detection

Antivirus software

...

Endpoint Detection Response

AP

...

Autoriteit Persoonsgegevens

API

Application Programming Interface. Een programma waarmee applicaties onderling communiceren zonder dat mensen dit aansturen. Veelgebruikte methodes over het internet zijn bijvoorbeeld SOAP en REST.

Applicatie securitytest

...

Vulnerability assessment

APT

Advanced Persistent Threat. Voortdurende dreiging van een geavanceerde tegenstander. Dit zijn met name statelijke actoren. Er wordt gebruik gemaakt van cyberaanvallen waarbij de aanvaller langere tijd in een informatiesysteem 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 informatie stelen of

op een zeker moment het netwerk stilleggen. Een APT verschilt van een gewone dreiging door het motie, de gekozen middelen en de vasthoudendheid van de aanvaller.

Architectuur

Het ontwerp en de opbouw van een computersysteem en netwerk. Het ontwerp regelt hoe businessprocessen, applicaties, data en technologie samenhangen.

Assessment

Onderzoek naar de risico's van verschillende soorten dreigingen 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.

Assurance

Zekerheid dat je kunt vertrouwen op de kwaliteit van een bepaalde dienst of een bepaald proces.

Assurance level

Mate van zekerheid waarin je kunt vertrouwen op de kwaliteit van een bepaalde dienst of een bepaald proces.

Asymmetrische versleuteling

Informatie onbegrijpelijk maken voor anderen. Bijvoorbeeld een tekstbestand of netwerkverkeer. Dit wordt gedaan met twee sleutels, in tegenstelling tot symmetrische versleuteling waarbij één sleutel wordt gebruikt. De ontvanger heeft een andere sleutel dan de verzender. Ze delen die dus niet met elkaar. De informatie wordt onleesbaar gemaakt met een openbare sleutel van de ontvanger en de ontvanger gebruikt 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 waarheidsgetrouw is voor deze data.

Public Key Infrastructure

Attack surface

...

Aanvalsoppervlak

Attributie

Duiden dat een bepaalde organisatie of groep aanvallers een aanval heeft uitgevoerd of dat heeft proberen te doen.

Audit

Onderzoek waarmee men beoordeelt hoe de werkelijkheid zich verhoudt tot een bepaalde norm.

Audit log

1. Bestand waarin is vastgelegd wanneer, wie, wat

heeft gedaan in de computersysteem. Dit is soms zelfs een wettelijke verplichting zoals bijvoorbeeld het bijhouden van wanneer, welke zorgverlener in een patientendossier heeft gekken of wijzigingen heeft aangebracht. Als tweede wordt dit ook veelvuldig gebruikt om na te gaan wie bijvoorbeeld toegang heeft gehad tot computersystemen, informatie of onderdelen daarvan.

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.

Auditor

Persoon die een audit uitvoert.

Audit

Authenticatie

Wat men doet om vast te stellen of een ander wel is wie hij zegt te zijn. De ander kan een persoon zijn, maar ook bijvoorbeeld software of een apparaat.

Identity en access management

Autorisatie

De bevoegdheden die een gebruiker van een computersysteem heeft om toegang te krijgen tot gegevens of handelingen te mogen uitvoeren. Bijvoorbeeld het opstarten van programma's of het inzien, wijzigen of wissen van in-

	formatie.	
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.	
Availability	...	<i>Beschikbaarheid</i>
AVG	Algemene verordening gegevensbescherming. Dit is een privacywet die geldt in de hele Europese Unie (EU). Dankzij de AVG gelden in alle landen van de EU dezelfde basis/minimum regels voor de bescherming van persoonsgegevens. De AVG is in Nederland de opvolger van de Wet Bescherming persoonsgegevens.	
Awareness	...	<i>Bewustwording</i>
Backdoor	...	<i>Achterdeur</i>
Backup	Een reservekopie van gegevens of digitale systemen. Hiermee kan men gegevens of systemen herstellen als het origineel beschadigd of weg is.	
Baseline	Pakket maatregelen dat ervoor moet zorgen dat de beveiliging van een netwerk een basisniveau heeft.	

	Voorbeeld van een baseline is de BIO (Baseline Informatie Overheid).	
BCI	Business Continuity Impact.	<i>Business continuity impact</i>
Bedrijfsrisico	Risico dat er iets gebeurt wat negatieve gevolgen heeft voor de doelstellingen en resultaten van een bedrijf.	<i>Risico</i>
Behavioral targeting	...	<i>Profiling</i>
Beheersmaatregel	Een activiteit met als doel om de oorzaak of het gevolg van een ongewenste gebeurtenis te voorkomen, weg te nemen, of te verkleinen.	
Betrouwbaarheid	Mate waarin digitale (genetwerkte) systemen beschikbaar zijn voor gebruik. Cyberaanvallen, uitval en storingen kunnen de betrouwbaarheid beïnvloeden.	
Beschikbaarheid	<ol style="list-style-type: none"> 1. De zekerheid dat gebruikers in een informatiesysteem of bij informatie kunnen wanneer zij dat willen. 2. Een percentage van de tijd dat gebruikers in een digitaal systeem konden. Gepland systeemonderhoud telt niet mee. 	
Best practice	Een techniek, werkmethode of activiteit die in de in	

	de praktijk heeft bewezen effectief te zijn.	
Beveiliging	Alle maatregelen die nodig zijn om een digitaal systeem te beschermen tegen schadelijke invloeden.	<i>Risico, threat, kwetsbaarheid, asset</i>
Beveiligingsbewustzijn	De mate waarin mensen risico's herkennen en zich ervan bewust zijn dat deze de veiligheid van informatie in gevaar kunnen brengen.	
Beveiligingsincident	Gebeurtenis of actie waarbij de beveiliging van hardware, software, informatie, een proces of organisatie mogelijk in gevaar is gebracht of geheel of gedeeltelijk is doorbroken.	
Beveiligingslek	...	<i>Kwetsbaarheid</i>
Beveiligingsmaatregel	Iets wat men doet om risico's voor de veiligheid van informatie te verkleinen of weg te nemen.	
BIA	Business Impact Analyse of Business Impact Assessment.	<i>Business impact analyse</i>
Biometrie	Methode om vast te stellen wie iemand is. Men gebruikt hiervoor unieke kenmerken van het lichaam. Denk aan een vingerafdruk of irisscan.	<i>Meerfactor authenticatie</i>
BIV	Model om drie verschillende kenmerken van informatiebeveiliging aan te	<i>Beschikbaarheid, integriteit, betrouwbaarheid, CIA</i>

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?

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 tot de broncode, is het een whitebox test of crystalbox test.

Greybox test, whitebox test, crystal box test

Blackhat hacker

Iemand die met kwade bedoelingen inbreekt in een computersysteem. 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.

Whitelisting

Blockchain

Een digitaal overzicht waarin transacties worden gecontroleerd en opgeslagen

Cryptovaluta

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.

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

...

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

Botnet, Command & Control server

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, noemen ook wel een zombie. De gebruiker van een computer merkt vaak niets van een bot.

Bot herder

Iemand die een botnet beheert.

Bot, Botnet

Botnet

Een netwerk van computersystemen die zelfstandig kwaadaardige taken uitvoeren, zoals het versturen van spam of het uitvoeren van een DDoS-aanval. Een command-and-controlserver stuurt dit netwerk aan.

Command-and-control server

Bounty program

...

Bug bounty program

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 waar-

bij iemand met een hulpmiddel alle mogelijkheden uitprobeert om een geheim 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 besturings-systeem problemen krijgt doordat het meer data moet opslaan dan in het stuk geheugen dat hiervoor beschikbaar is past. Gevolg is dat het programma of systeem onvoorspelbaar wordt. Soms crasht een computersysteem 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.

Patch

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.

Business continuity

Hoe een organisatie erin slaagt om de bedrijfsprocessen door te laten gaan. Zelfs bij een grote verstoring.

Business continuity impact	Hoe ernstig de gevolgen zijn van een groot beveiligingsincident, als belangrijke ICT-bedrijfsprocessen en applicaties uitvallen.	
Business continuity plan	Plan waarin staat wat te doen bij storingen die ernstige gevolgen hebben voor de organisatie.	
Business e-mail compromise	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.	<i>CEO/CFO/CxO fraude</i>
Business Impact Analyse	Analyse waarin staat hoe de belangrijkste functies en processen in een organisatie eruit zien. 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. Dit is als gebruikers van een computernetwerk hun eigen apparaten, zoals een privé telefoon of laptop, mogen gebruiken voor zakelijk gebruik. Vaak mag dit alleen onder bepaalde voorwaarden.	

C&C server	...	<i>Command-and-control server</i>
C2 server	...	<i>Command-and-control server</i>
CA	Certificate Authority.	<i>Certificate authority</i>
CAAS	Cybercrime-as-a-service.	<i>Cybercrime-as-a-service</i>
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 dat hij kenmerken in foto's moet herkennen.	
CASB	Cloud Access Security Broker.	<i>Cloud access security broker</i>
Catphishing	Een variant van phishing. Hierbij proberen oplichters persoonlijke gegevens van iemand te stelen via nageemaakte sociale netwerksites en datingsites. Bij die gegevens gaat het meestal om persoonlijke informatie, creditcardnummers of geld.	<i>Phishing</i>

CEH

Certified Ethical Hacker.
Dit is een certificering voor professionals in informatie-beveiliging, specifiek voor ethisch hacken.

Censorship

Censuur. Informatie on-toegankelijk 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 de financiële afdeling overtuigen of onder druk zetten om geld over te maken.

*Spear phishing***CERT**

Beschermd term (afkorting voor Computer Emergency Response Team) van Carnegie Mellon voor het eerste CSIRT ter wereld. Deze term mag onder bepaalde voorwaarden ook door andere CSIRT's worden gebruikt.

*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.

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 te beoordelen. De producten moeten voldoen aan dezelfde 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

Medewerker die verantwoordelijk is voor informatiebeveiliging.

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

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

Beoordelen 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.

Click fraud

Een vorm van fraude waarbij de eigenaar van een website geld krijgt voor iedere keer dat een gebruiker op een advertentie klikt. Bij deze vorm van fraude klikken geautomatiseerde scripts, bots of personen telkens op deze advertenties. En zo zorgen ze voor inkomsten voor de website-eigenaar.

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 weet welke applicaties in de cloud men gebruikt.
- Men beschermt de bedrijfsgegevens die van en naar de cloud gaan.
- Men krijgt controle vanuit één centraal punt.

Cloud based security

...

Cloud security

Cloud computing

Een model waarbij op aanvraag computercapaciteit van anderen wordt gebruikt. De capaciteit deelt men bijvoorbeeld voor servers, opslag, applicaties en diensten.

Cloud security

1. De beveiliging van alle data, applicaties en het

netwerk van apparaten die in een cloudtoepassing zitten.

2. Cybersecuritydiensten die een aanbieder vanuit de cloud aan een klant levert.

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 doet men voor een groot deel handmatig.

Code execution

Actie waarbij iemand ongewild een 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. Voorbeeld van een code injection is SQL-injection.

Code review

Analyse van de broncode van een programma. Het doel is zwakke plekken te vinden. Men zoekt voor een groot deel handmatig, en

niet aan de hand van een uitputtende lijst van kwetsbaarheden.

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

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.

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 dataproctierecht 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

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 verschillende

Budapest Convention on Cybercrime

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 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 analyses en marketing.

Coordinated vulnerability disclosure

Standaard proces waarmee security onderzoekers zwakke plekken in computersystemen en producten kunnen melden. Ze mogen dat alleen doen als ze zich houden aan de spelregels van de organisatie voor dit soort meldingen. Het Nationaal Cyber Security Centrum (NCSC) heeft een handleiding waarin staat waaraan de spelregels moeten voldoen. Deze methode is de opvolger van de Responsible Disclosure. Het belangrijkste verschil met vroeger is dat de on-

Responsible disclosure

derzoeker nu niet meer alleen verantwoordelijk is voor de gevolgen van een beveiligingslek.

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).

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

Credentials

De gegevens waarmee een gebruiker of ander computersysteem bij een computersysteem 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.

Crisismanagement

Acties en maatregelen om een crisis in een organisa-

tie te voorkomen of op te lossen. Een crisis is een noodsituatie waarbij een organisatie ernstig verstoord raakt.

Critical infrastructure

...

Kritieke infrastructuur

Cross site request forgery

Een aanvaller lokt een gebruiker naar een andere webpagina. Zo 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

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.	
Cryptomining	Alle transacties in een blockchain verzamelen, controleren en verwerken. Dit gebeurt om dubbele uitgaves op te sporen.	
Cryptovaluta	Digitaal ruilmiddel. Een bekende cryptovaluta is de bitcoin.	
Crystal box test	...	<i>Black box test</i>
CSIRT	Computer Security Incident Response Team. Een team van deskundigen dat beveiligingsincidenten oplost. Dit kan een intern team zijn, maar ook een extern ingehuurd team.	<i>CERT</i>
CSMS	Cyber Security Management System. Dit systeem houdt bij of de maatregelen voor informatiebeveiliging goed werken.	<i>ISMS</i>
CSRF	Cross Site Request Forgery.	<i>Cross site request forgery</i>
CVD	Coordinated Vulnerability Disclosure.	<i>Coordinated vulnerability disclosure</i>
CVE	Common Vulnerabilities and Exposures. Een openbare lijst van bekende zwakke plekken in software. De lijst staat op 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 als eerste gaat oplossen. Meer informatie over het scoresysteem staat op <https://www.first.org/cvss/>.

CWE

Common Weakness Enumeration. Een openbare lijst met bekende soorten zwakke plekken in software. De lijst is te vinden op <https://cwe.mitre.org/>.

Cyber

Iets wat te maken heeft met digitale informatie en systemen die verbonden zijn met het internet.

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.

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 cyberdefense, cyberoffense of capacity building.	
Cyber offense	Het hebben van middelen om cyberaanvallen uit te voeren. Bijvoorbeeld strategische of militaire middelen. Term wordt met name gebruikt in de context van nationale veiligheid.	
Cyber resilience	...	<i>Cyberweerbaarheid</i>
Cyberaanval	Een gerichte aanval in of via cyberspace. Doelwitten kunnen zijn: personen, groepen, bedrijven en organisaties, overheden, andere landen.	
Cyberattack	...	<i>Cyberaanval</i>
Cyberbullying	Pesten op internet	
Cybercrime-as-a-service	Een dienst van criminelen om tegen betaling een digitale aanval uit te voeren. Hun afnemers zijn vaak ook criminelen. Bekende voorbeelden zijn het stelen en doorverkopen van creditcardgegevens of medische gegevens. En kwaadaardige software of DDoS-aanvallen doorverkopen.	
Cybercriminaliteit	Criminaliteit waarbij men een computersysteem aanvalt of misbruikt voor criminele activiteiten. Er	

zijn 2 types:

1. Cybercriminaliteit in brede zin. Dit zijn alle strafbare activiteiten waarbij iemand een informatiesysteem of computer gebruikt. Denk aan diefstal en vervalsing van betaalpassen, oplichting, afpersing, kinderporno, racisme en belediging.
2. Cybercriminaliteit in enge zin. Hierbij gebruikt men informatiesystemen en computers niet alleen als middel, maar zijn ze ook een doel. Bijvoorbeeld computers beschadigen, spamaanvallen, DDoS-aanvallen, virussen verspreiden.

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 informatienetwerk 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 en het aansturen op veilig gedrag van personeel.

Cybersabotage

Activiteiten waarbij men expres en gedurende een lange tijd informatiesystemen en informatiediensten beschadigt. Zodat gebruikers niet meer bij informatie kunnen wanneer zij dat willen. In het ergste geval gaat de informatie verloren. Of het systeem wordt verwoest.

Cybersecurity

Alle beveiligingsmaatregelen die men neemt om schade te voorkomen door een storing, uitval of misbruik van een informatiesysteem of computer. Ook worden maatregelen genomen om schade te beperken en/of herstellen als die toch is ontstaan. Voorbeelden van schade zijn dat men niet meer in een computersysteem kan komen wanneer men dat wil. Of dat de opgeslagen informatie bij anderen terecht komt of niet meer klopt. De maatregelen hebben te maken met processen in de organisatie, technologie en gedrag van mensen.

Cyberspace

Een ecosysteem van digitale (genetwerkte) technologieën, waarbinnen allerlei verschillende actoren informatie creëren, opslaan, uitwisselen, gebruiken en delen.

Cyberspionage

Het binnendringen van digitale systemen voor het verkrijgen van vertrouwelijke informatie, vaak strategisch, economisch of militair van aard, veelal door staten of bedrijven.

Cyberterrorisme

Terroristische activiteiten die men digitaal uitvoert. Bijvoorbeeld het beschadigen of uitschakelen van belangrijke informatienetwerken via internet.

Cyberveilig

...

Cyberweerbaar

Cyberverzekering

Een verzekering die betaalt voor de financiële schade die ontstaat als gevolg van een datalek, virus, hack of andere cyberaanval. De verzekering betaalt niet alleen voor schade bij de organisatie zelf, maar ook voor schade die ze aan anderen moet betalen. Daarnaast bieden de meeste verzekeraars ook hulp aan in de vorm van diensten, zoals herstel of communicatie.

Cyberwarfare

Digitale (genetwerkte) technieken gebruiken om de systemen van staten of organisaties aan te vallen. Vaak met een militair of strategisch doel.

Cyberweerbaarheid

De veerkracht van een organisatie en haar digitale systemen en processen. Cyberweerbaarheid wordt

uitgedrukt in de snelheid en effectiviteit waarmee een organisatie zich weet te herstellen na een incident.

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 leak prevention

...

*Data loss prevention***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.

Datadiode

Een communicatieapparaat dat zorgt voor een veilige verbinding zodat gegevens maar één kant op kunnen gaan.

Datalek

Een storing in de beveiliging van een computersys-

AVG

teem. Een gevolg hiervan kan zijn dat gegevens worden veranderd, deze verloren gaan of bij verkeerde personen terechtkomen. In de context van de AVG wordt met datalek vaak een storing in de beveiliging van persoonsgegevens bedoeld. Een storing kan een technische oorzaak hebben, maar ook bijvoorbeeld veroorzaakt worden door een persoon, zoals een mail naar een verkeerde persoon sturen.

DDoS

Distributed Denial of Service.

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 het gebruiken van die informatie om hen te ontdekken.

Decryptie

...

Ontleutelen, cryptografie

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

Een aanval op een website waarbij de aanvaller een website ongevraagd verandert.

Defensive capabilities

...

Cyber defense

Denial of Service aanval

Aanval waarbij men probeert om een computer, netwerk of dienstverlening uit te schakelen voor de gewone gebruiker of klant. Zet men hiervoor meer computers in, dan gaat het om een Distributed Denial of Service (DDoS-aanval).

Distributed Denial of Service aanval

Desinformatie

Misleidende of afleidende informatie die men met opzet verspreidt.

Nepnieuws

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 sabotage

...

Cybersabotage

Digitale spionage

...

Cyberspionage

Digitale veiligheid

Situatie waarin je geen schade hebt of krijgt door

verstoring of uitval van ICT.

Disaster recovery plan

Plan waarin staat hoe het digitale systeem moet herstellen na een grote storing.

Business continuity plan

Disk image

...

Forensic image

Distributed Denial of Service aanval

Aanval door een verzameling computers of andere apparaten die tegelijk proberen om een computer(netwerk) of dienstverlening uit te schakelen. Vaak gaat de aanval via een botnet.

DKIM

Domain Keys Identified Mail. DKIM is een techniek waarmee e-mailberichten kunnen worden geverifieerd. 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 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

Domain Name System. Het systeem dat op het internet gebruikt wordt om namen van computers te vertalen naar IP-adressen en andersom. Dat vertalen gaat simpel: de namen van de computer staan in een tabel en iedere naam krijgt een eigen nummer, zoals in een telefoonboek.

Domeinnaam, IP-adres

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.

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***DoS**

Denial of Service.

*Denial of Service aanval***DPA**

Data Protection Authority. De toezichthouder in een staat die toeziet op naleving en handhaving van wet- en regelgeving op het terrein van privacy en gegevensbescherming. In Nederland is dit de Autoriteit Persoonsgegevens.

*Autoriteit Persoonsgegevens***DPI**

Deep Packet Inspection.

*Deep packet inspection***DPIA**

Data Protection Impact Assessment. Een organisatie onderzoekt vooraf wat de risico's van gegevensverwerking zijn voor de privacy van personen. Dit is vaak verplicht volgens

Privacy impact assessment

	de Algemene verordening Gegevensbescherming.	
DPO	Data Protection Officer. De medewerker die controleert of een organisatie zich houdt aan de regels van de AVG.	<i>AVG</i>
Dreiging	Iets wat gevaar of schade kan opleveren voor een organisatie. Bijvoorbeeld een storing, reputatieschade of financieel verlies.	<i>Risico</i>
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 cloud-diensten, onlinezoekmachines en/of onlinemarktplaatsen aanbiedt. Een DSP valt in bepaalde omstandigheden onder de verplichtingen van de WBNI.	
DTC	Digital Trust Center. Onderdeel van het ministerie van Economische Zaken en Klimaat dat als doel heeft om ondernemers te helpen met veilig digitaal ondernemen.	

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 doelen als civiele doelen.

Dumpster-diver

Iemand die vertrouwelijke informatie probeert te vinden door het afval van iemand te doorzoeken.

E-discovery

Grote aantallen elektronische data doorzoeken voor een bepaald doel. Meestal voor een juridisch onderzoek of een rechtszaak.

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 maakt men door

gebruik te maken van kenmerken van al bekende kwaadaardige software. Of van van opvallend gedrag van nieuwe software in een computersysteem. Bij een incident gebruikt men deze software om specifieke zoekopdrachten uit te voeren op digitale systemen. Zo kan men dit incident helpen oplossen.

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.

Escrow

Een softwareleverancier vraagt een ander onafhankelijk bedrijf om 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***Exploit**

Programmacode of reeks acties waarmee iemand een zwakke plek in een digitaal systeem misbruikt. Het doel hiervan kan zijn om toegang te krijgen tot het systeem, om informatie

te stelen of te veranderen of om te zorgen dat anderen niet meer bij informatie kunnen. Men kan een exploit gebruiken als onderdeel van malware.

Exploitkit

Kant-en-klare kwaadaardige software die aanvallers op een website in kunnen zetten. De exploitkit maakt dan automatisch misbruik van zwakke plekken in de systemen van de bezoekers van de website en besmet hun systemen.

Fail Safely

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 over het netwerk 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.

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 bestaan. 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 wan-

neer en hoe de aanval heeft plaatsgevonden, welke informatie er is gestolen en wie er achter de aanval zat.

Funciescheiding

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 niet alles zelf uitvoeren waardoor het risico op misbruik afneemt.

**Functionaris
Gegevensbescherming**

Medewerker die controleert of een organisatie zich houdt aan de regels van de Algemene Verordening Gegevensbescherming (AVG).

Fysieke beveiliging

Maatregelen om te voorkomen dat iemand bijvoorbeeld op een computer of ander digitaal apparaat kan werken, of een beveiligd gebouw zomaar in kan lopen, terwijl hij dat niet mag.

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. Algemene Verordening Gegevensbescherming (AVG) is de Nederlandse uitwerking van deze Europese regelgeving.

*AVG***Gebruikersnaam**

Naam waarmee een gebruiker in een computersysteem kan inloggen.

*Inlogcode***Geheimhoudingsverklaring**

Overeenkomst waarbij twee of meer partijen met elkaar afspreken om informatie geheim te houden. Ze delen die dus niet met anderen.

Gijzelsoftware

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

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, whitehat hacker, blackhat hacker***Greybox test**

...

*Blackbox test***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.

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 computersysteem. 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

Persoon die digitale aanvallen uitvoert vanuit een ideologisch, niet terroristisch motief. Soms doet hij dat als lid van een groep. Hacktivist is een samenstelling van hacker en

activist.

Hall of Fame / Wall of Fame

Een lijst met namen van hackers die hebben meegeholpen om een informatiesysteem 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.

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 er mee 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 computersysteem dat met opzet niet goed beveiligd is. Het doel van dit systeem is om het te laten besmetten met software die een computersysteem 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

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 makkelijk te onthouden zijn, zoals www of smtp. De

FQDN is dan bijvoorbeeld
www.google.nl of smtp.
google.nl

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 dus 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 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.

Hunting

Een veelal handmatig proces waarin men in netwerkverkeer of op digitale systemen zoekt naar sporen van aanvallen die bestaande beveiligingsmaatregelen hebben omzeild.

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

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 voor doet 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?

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***IIoT**

Industrial Internet of Things. Internet of Things toegepast binnen een industriële omgeving.

Internet of Things

Incident

...

*Beveiligingsincident***Incident response**

Reactie op een beveiligingsincident. Het is een (gestructureerde) aanpak op alle niveaus: operationeel, tactisch en strategisch.

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 geprobeerd uit te voeren.

Industrial control system

Algemene naam voor verschillende typen controlesystemen. Bijvoorbeeld SCADA, DCS's, PLC's. Deze controlesystemen gebruikt men in de industrie om processen aan te sturen. Bijvoorbeeld een sluis openen of een windmolen uitzetten.

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 computersysteem, 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.

Informatie-beveiligingsbeleid

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

Informatie kopiëren of stelen terwijl men daarvoor geen toestemming heeft.

Information Security Officer

...

*Chief Information Security Officer***Initieel risico**

...

*Bruto risico***Inlogcode**

Combinatie van gegevens die men nodig heeft om in een computersysteem of een ruimte te komen. Bijvoorbeeld gebruikersnaam

Wachtwoord, gebruikersnaam

en wachtwoord.

Inlooptest

...

Mystery guest bezoek

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.

Integriteit

1. Bij data: juiste en volledige informatie, en verwerking van informatie.
2. Bij personen: de betrouwbaarheid van iemand.
3. Bij systemen: hun correcte werking.

Intelligence

...

Inlichtingen

Internet of Things

Apparaten die via het internet verbonden zijn en informatie kunnen uitwisselen. Bijvoorbeeld thermostaten, koelkasten en auto's.

Internet Protocol Security

Standaardafspraken over hoe men netwerkverkeer kan beveiligen. Hiermee kan worden gecontroleerd of informatie in het verkeer niet is aangepast en kun-

nen 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 computernetwerk gaan of die een digitaal systeem verstuurt en ontvangt. En een waarschuwing geven als er iets niet in orde lijkt.

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-adres

Internet Protocol adres. Adres dat de bron of bestemming van verkeer op Internet aangeeft.

Intrusion prevention

IPS

Intrusion Prevention System. Een geautomatiseerd systeem dat intrusion prevention doet.

IPSEC

Internet Protocol Security.

Internet Protocol Security

IPv4

Internet Protocol versie 4. IPv4 maakt communicatie van data tussen ICT-syste-

men 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.

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 beveiligingsincidenten, 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. Information Security Officer.

Chief Information Security Officer

2. Internationale set afspraken waar iets aan moet voldoen. De internationale afspraken voor informatiebeveiliging is de reeks ISO 2700x.

3. International Organization for Standardization.

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, uit-

Informatiebeveiliging

voeren, beoordelen en bijhouden. De bedrijfsrisico's bepalen aan welke normen een organisatie wil of moet voldoen. Voorbeelden: ISO 27001 en 27002.

Jamming

Het verstoren van draadloze signalen zoals bijvoorbeeld WiFi.

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.

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 risico'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 in-

frastructuur van een land die essentieel zijn. Worden deze onderdelen uitgeschaald, of vallen ze uit? Dan is de kans op economische en/of maatschappelijke ontwrichting groot.

Kroonjuwelen

Informatie en informatie-systemen 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.

Kunstmatige intelligentie

Technologie waarbij digitale systemen reageren op data, bijvoorbeeld afkomstig uit sensoren, en op basis daarvan zelfstandig acties ondernemen.

Kwantumcomputer

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.

Kwetsbaarhedescan

...

*Vulnerability scan***Kwetsbaarheid**

Fout in een digitaal systeem waardoor een aanvaller in het systeem kan komen. De aanvaller kan vervolgens bij informatie of toepassingen in het systeem komen, terwijl hij dat niet mag. Of de aanvaller zorgt ervoor dat de gebruiker niet meer bij deze informatie kan komen. Of de toepassing niet meer kan gebruiken.

*BIV***Lateral Movement**

Technieken die aanvallers gebruiken om geleidelijk door een netwerk te bewegen. Terwijl ze door het netwerk bewegen, zoeken ze naar informatie.

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 vulnerabiliteiten etc.

Least Privilege

Uitgangspunt dat iemand zo min mogelijk bij informatie en systemen kan. Dege ne kan alleen bij informatie en systemen die hij of zij nodig heeft voor het werk.

Legacy

...

*Legacy systemen***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 vaak bekende gebreken.

Local Privilege Escalation

Zichzelf meer rechten geven op een computersysteem. 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

LPE

Local Privilege Escalation.

Local Privilage Escalation

M2M

Machine-to-machine. Uitswisseling 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 advertentiebedrager. Zo worden grote groepen gebruikers besmet via een legitieme website.

Malware

Kwaadaardige software die aanvallers op een digitaal systeem zetten om er op afstand bij te kunnen, het te vernielen of informatie te

stelen. Malware is een samentrekking van het Engelse malicious software.

Man-in-the-middle aanval

Een aanval waarbij een aanvaller informatie van twee partijen ontvangt en doorstuurt. Bijvoorbeeld twee bedrijven. De partijen denken allebei dat ze de informatie direct naar elkaar versturen maar dat is niet zo. De aanvaller kan op deze manier de informatie af luisteren, maar ook veranderen.

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

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

Meerfactor authenticatie

Methode om vast te stellen of een gebruiker of digitaal systeem wel is wie of wat hij zegt te zijn. Je gebruikt hiervoor verschillende ma-

Authenticatie

nieren. Bijvoorbeeld een wachtwoord en een code die de gebruiker per sms krijgt. Of een combinatie van een vingerafdruk en een wachtwoord.

Meldplicht

Wettelijke plicht om een melding te doen als er iets misgaat met de beveiliging van een digitaal systeem, proces of organisatie. Bijvoorbeeld een groot datalek moet men melden bij de Autoriteit Persoonsgegevens.

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

Mitigatie

Schade als gevolg van een beveiligingsincident verminderen. Of beveiligingsrisico'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.

Mobile device management

Zorgen dat mobiele apparaten in een organisatie goed beheerd en beveiligd

MDM

	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.	
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. Wordt ook wel geldezel genoemd.	
Monitoring	Continu bewaken van een computer of digitaal netwerk. Bijvoorbeeld of het nog helemaal goed werkt, of er fouten voorkomen, enzovoort.	<i>Security monitoring</i>
MSP	Managed security provider.	<i>Managed security provider</i>
MSSP	Managed security service provider.	<i>Managed security service provider</i>
Multifactor authenticatie	...	<i>Meerfactor authenticatie</i>
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 een deze persoon deze organisatie. Men kan deze	<i>Penetratietest</i>

test combineren met een penetratietest. Bij deze test gaat de mystery guest een beveiligde ruimte in. Daar probeert hij in te breken op het lokale computernetwerk.

NAT

Network Address Translation.

Network Address Translation

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 belangrijkste zijn in Nederland. Bijvoorbeeld elektriciteit, toegang tot schoon drinkwater.

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 gedaan bij erg gevoelige informatie.

Negligible risk

Verwaarloosbaar risico. Risico waarvan de kans, de consequenties, of beiden zo klein is, 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.

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 aanvalder 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.	
Network access control	...	<i>Netwerktoegangsbeheer</i>
Network security	...	<i>Netwerkbeveiliging</i>
NIB-richtlijn	...	<i>WBNl</i>
Niet persoonsgebonden account	Account dat niet bij een bepaalde persoon hoort. Er zijn 2 soorten: <ol style="list-style-type: none"> 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. 	
NIS-directive	...	<i>WBNl</i>
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 cyberaanval- len te voorkomen en op te sporen. En hoe ze er beter op kunnen reageren.	

NOC

Network Operations Centre. 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.

Non-repudiation

...

*Onweerlegbaarheid***Non-state actor**

Niet-statelijke actor. Vaak gebruikt om alle 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.

Notice and take-down

Procedure voor website-eigenaren en netwerkbeheerders. Zij verwijderen content van internet wanneer die door een rechtbank als illegaal is bestempeld, of wanneer daar een verdenking van is. Wordt veel gebruikt in het licht van schendingen van het auteursrecht.

NPA

Niet Persoonsgebonden Account

Niet persoonsgebonden account

Obfuscation

lets 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.

Ontslutelen

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 bijvoorbeeld 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

Open source

Software waarvan de broncode voor iedereen te lezen

Broncode

is. Hierdoor kan iedereen de software kopiëren, veranderen en delen. Een voorbeeld van open source software is Android, een besturingssysteem voor mobiele apparaten.

Open source intelligence

Inlichtingen verzamelen over een onderwerp door bronnen te gebruiken die voor iedereen toegankelijk zijn.

Operational Technology

Automatisering van een productieomgeving. Bijvoorbeeld robots en machines. Hierbij is het vooral belangrijk dat men bij informatie kan wanneer men dat wil, en dat de informatie klopt. Deze twee dingen zijn bij operational technology belangrijker dan betrouwbaarheid: dat alleen die mensen de informatie krijgen voor wie die bedoeld was.

OSCP

Offensive Security Certified Professional. Diploma voor pentesters. Het examen duurt 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 tech-

	nische systemen.	
OSINT	Open Source INTelligence.	<i>Open source intelligence</i>
OT	Operational Technology of Operations Technology.	<i>Operational Technology</i>
OTP	One Time Password.	
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.	
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.	
Password	...	<i>Wachtwoord</i>
Patch	Nieuwe versie van software. In deze nieuwe versie heeft de leverancier kwetsbaarheden in het systeem hersteld. Hij heeft geen nieuwe functies toegevoegd.	<i>Update</i>
Patch management	Proces waarbij men regel-	

matig patches installeert op 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. En 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.

Penetratietest

Handmatige controle waarbij men zo diep mogelijk wil binnendringen in een 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. Dat gebeurt wel bij een vulnerability scan.

Pentest

...

Penetratietest

Persoonsgegevens

Gegevens die verwijzen naar een persoon. Met deze gegevens kan men vaststellen wie iemand is. Bijvoorbeeld naam, adres, nummer van het paspoort.

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:

- een om de tekst om te zetten in een code.
- en een om de code weer

Cryptografie

terug te zetten in tekst.
Whatsapp maakt gebruik van PGP.

Phishing

Aanval waarbij de aanvaller iemand verleidt om belangrijke informatie te geven, zoals bijvoorbeeld inloggegevens of creditcardgegevens. Phishing gebeurt vaak via e-mails. Maar aanvallers doen het ook via de telefoon, een sms of een app-bericht.

PIA

Privacy Impact Assessment.

Privacy Impact Assessment

PII

Personally Identifiable Information.

Persoonsgegevens

PKI

Public Key Infrastructure.

Public Key Infrastructure, Certificate

Poortscan

Scan van openstaande poorten op een digitaal systeem waarmee inzichtelijk wordt gemaakt welke poorten openstaan. Een poort is een manier 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.

Port scan

...

Poort scan

Post-quantum crypto

Vorm van versleuteling die niet te kraken is met kwantumcomputers.

Kwantum Computer

Post-quantum key exchange

Afspraken over hoe je sleutels uitwisselt. Het gaat om sleutels die niet te kraken zijn met kwantumcomputers.

Cryptografie, kwantum computing

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.

Private key

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 crypto

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.

Privileged account

Account op een digitaal systeem dat meer rechten geeft om bepaalde dingen te doen. Bijvoorbeeld bestanden en instellingen veranderen. In Windows-systemen heet dit account de administrator. In Unix en Linuxsystemen de root.

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.

Pseudonimisering

Methode om gegevens niet meteen te kunnen verbinden met een persoon. De persoonsgegevens vangt 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, asymmetrische crypto

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

...

Adversary simulation

Quantum Computer

...

Kwantumcomputer

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

...

Gijzelsoftware

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

Recovery

...

Disaster recovery

Red team

...

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

...

Cyberweerbaarheid

Responsible disclosure

Actie waarbij men gevonden beveiligingslekken op een verantwoorde manier bekend maakt. Meestal meldt men het lek eerst bij

Coordinated vulnerability disclosure

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.

Restrisico

...

*Netto risico***Reverse engineering**

Hardware of software onderzoeken om te snappen hoe deze precies werken. De onderzoeker weet van tevoren niet hoe de software of hardware ontworpen is. Bijvoorbeeld het onderzoeken van malware om de exacte werking te achterhalen.

Risico

Kans op schade of verlies in een computersysteem, 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

Dreiging, threat

organisatie kan men denken aan financiële schade of het verlies van de goede naam van de organisatie.

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 bedrijf 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**

Hoeveel risico iemand wil nemen om iets te kunnen bereiken.

*Mitigatie***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.

Risicomanagement

Een continu proces waarbij

Bedrijfsrisico, risicoanal-

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).

yse, 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:

- de kans op een incident verkleinen.
- 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.

Risk appetite

...

*Risicobereidheid***Role based access control**

Bepalen of een gebruiker bij een computersysteem 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 beveiligingsincident, zoals een datalek.

Rootkit

Malware die een aanvalleur gebruikt als hij eenmaal toegang heeft tot een computersysteem. De rootkit zit zo diep in het systeem dat het lange tijd ongemerkt in het computersysteem kan blijven zitten. De rootkit kan ook een geheime toegang tot het systeem maken.

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 priv sleutel. De openbare

sleutel deelt men met elkaar via een certificaat.

Sandbox

Afgeschermd deel in een digitaal systeem. Software die op deze plek werkt, kan geen andere processen in de computer verstoren. Men gebruikt vaak een sandbox om software in te draaien die vaak aangevallen worden. Of om te testen of iets malware is en wat het dan doet.

SAST

Static Application Security Testing. Techniek waarmee men automatisch zwakke plekken in een broncode kan controleren.

SCADA

Supervisory Control and Data Acquisition. Meetsignalen en regelsignalen van machines in grote industriële systemen verzamelen, doorsturen, verwerken en zichtbaar maken. Bijvoorbeeld van windturbines.

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.

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.

Script kiddie

Iemand die cyberaanvallen doet voor de lol. Of omdat hij wil laten zien dat een site of computernetwerk kwetsbaar is. Vaak zijn het jonge hackers die niet goed snappen wat de gevolgen kunnen zijn van hun acties. Ook weten zij vaak niet heel veel, en gebruiken ze hulpmiddelen van anderen.

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 beveiligingsproblemen heeft.

ligingslekken bevat.

Secure development lifecycle

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. Microsoft heeft dit ontwikkeld in 2002. Verschillende organisaties gebruiken nu SDL. Soms een eigen versie ervan.

Secure Sockets Layer

SSL. 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.

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

CVE

Common Vulnerabilities and Exposures (CVE). Dit is een databank met informatie over kwetsbaarheden in computersystemen en netwerken.

2. Adviesdiensten op het gebied van informatiebeveiliging en cybersecurity.

Security awareness

...

Beveiligingsbewustzijn

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 gebruik 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

SIEM

dingen in het systeem heeft veranderd, terwijl hij dat niet mocht.

Security monitoring

Continu bewaken van een computer of digitaal netwerk met als doel om verdacht gedrag op te sporen.

Security monitoring

Security Operations Center

Afdeling of team dat informatiesystemen controleert of bewaakt. Dit doen zij voor de eigen organisatie of voor klanten.

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 en PCI-DSS.

Security test

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 beveiligingsmaat-

Obfuscation

regelen 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.

Segregation of duties

...

*Functiescheiding***Service account**

...

*Niet persoonsgebonden account***Severity**

Hoe ernstig een zwakke plek van een digitaal systeem is.

Shell

Computerprogramma waarmee een gebruiker met een commandoregel opdrachten kan geven aan het besturingssysteem van een computer.

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 uit het systeem te stelen.

SIEM

Security Information and Event Management.

Security Information and Event Management

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 opspoot met hulp van vooraf afgesproken patronen, instructieregels of tekens.

Signing

...

Digitale handtekening

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 SSO 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.

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.

Smart blockchain

Nieuwe term die geen zinvolle betekenis heeft.

Sniffen

De informatie die in een computernetwerk rondgaat, afluisteren en analyseren.

Cryptografie

SOC

Security Operations Center.

Security Operations Center

Social engineering

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.

Source code

...

Broncode

SPAM

E-mails of andere elektronische berichten waar de ontvanger niet om heeft gevraagd en die hij ook niet wil ontvangen.

Spear phishing

Een phishingaanval die gericht is op een bepaald persoon. Soms is de aanval ook speciaal aangepast voor deze persoon. Daarom is het heel moeilijk om te herkennen dat het een phishingaanval is.

Phishing

SPF

Sender Policy Framework. SPF is een techniek waarmee een domeinhouder de IP-adressen van verzendende mailservers kan publiceren in de DNS. 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.

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.

SSL

Secure Socket Layer.

Secure Socket Layer

SSO

Single Sign On.

*Single sign on***State actor**

Statelijke actor, dat wil zeggen een land. Term wordt veel gebruikt in de context van nationale veiligheid en in geopolitieke discussies over cybersecurity.

State-sponsored attack

Cyberaanval die een staat financiert of op een andere manier ondersteunt.

Stepping stone server

Beveiligde manier om in een digitaal netwerk te komen. Dit wordt ook wel een jumpserver genoemd.

Storing

...

*Uitval***Supply chain attack**

Een aanval waarbij een aanvaller een organisatie niet rechtstreeks aanvalt, maar via één van de leveranciers. Hierdoor is het mogelijk om organisaties die zelf een goede beveiliging hebben, toch succesvol aan te vallen.

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.

Versleutelen

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).

Tabletop exercise

Oefening waarbij een groep mensen in een kamer een bepaald incident na speelt. De deelnemers zoeken samen naar een oplossing.

Tampering

Een digitaal systeem of informatie beschadigen door met opzet informatie, hardware en software te veranderen. Bijvoorbeeld een mail veranderen en versturen.

Testbed

Nagemaakte situatie waarin men testen kan doen.

Threat

...

Dreiging

Threat actor

...

Actor

Threat hunting

...

Hunting

Threat intelligence

Informatie 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 opsporings-technieken.

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 om data of informatie in te delen in klassen. Hoe men dit indeelt, hangt af van met wie men de informatie mag delen. De klassen zijn rood, oranje, groen en wit.

TLS

Transport Layer Security.

Transport Layer Security

Toegangsbeheer

Controle om te bepalen wie naar binnen mag in een ruimte of digitaal systeem.

Token

Een middel dat men gebruikt om ergens in te mogen. Dat kan bijvoorbeeld een ruimte in een gebouw zijn of een digitaal systeem.

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

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.

Transport Layer Security

Transport Layer Security zorgt voor beveiligde internetverbindingen, met als doel de veilige uitwisseling van gegevens tussen internetsystemen. Bijvoorbeeld websites of mailservers. Dit maakt het voor cybercriminelen moeilijker om internetverkeer te onderscheppen of te manipuleren. TLS is de opvolger van SSL.

Cryptografie, authenticatie

Trojan	Type kwaadaardige software waarmee een aanval- ler via een geheime ingang in een systeem kan komen. Vaak is deze verhuud in software die een gebruiker graag wil hebben en zelf installeert, zonder dat hij er zeker van is dat deze be- trouwbaar is.	<i>Malware</i>
True negative	Niets doen zolang een computersysteem normaal werkt.	
True positive	Een aanval herkennen die ook echt een aanval is.	
Trusted Third Party	Verklaring van een onafhan- kelijk onderzoeksbureau waarin staat in hoeverre de ICT-dienstverlening en ICT-kennis van een organi- satie aan bepaalde stan- daarden voldoet.	<i>TPM</i>
TTP	Tactics, techniques and procedures. Tactieken, technieken en processen die een aanvalleur gebruikt. TTP's worden gebruikt om de manier van werken van aanvallers te bepalen. Een Red team oefening is hier een voorbeeld van.	
Tweestapsauthenticatie	...	<i>Meerfactor authenticatie</i>
Two-factor authenticatie	...	<i>Meerfactor authenticatie</i>
Typo - squatting	Vorm van misbruik van het internet. Men maakt mis- bruik de situatie dat men-	

sen kleine fouten in een url vaak niet zien. Bijvoorbeeld men gebruikt een domeinnaam die maar één letter verschilt van de domeinnaam van de website die de bezoeker wilt bezoeken.

Uitval

Situatie dat gebruikers niet meer in een digitaal systeem kunnen werken.

Unknown unknown

Onbekend en onkenbaar risico. Een risico dat pas ontdekt wordt wanneer het zich voor de eerst tijdens een incident toont.

Update

Nieuwe versie van software of firmware door de producent. Deze repareert bekende zwakke plekken, zorgt eventueel voor nieuwe beveiliging en extra functies.

*Patch***Username**

...

*Gebruikersnaam***Versleutelen**

Informatie (bijvoorbeeld een tekstbestand of netwerkverkeer) onbegrijpelijk maken voor anderen. 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

Cryptografie, ontsleutelen

te versturen of bijvoorbeeld om vast te stellen dat een bericht ook echt komt van degene die zegt dat hij het heeft verstuurd.

Vertrouwelijkheid

Informatie is vertrouwelijk als het alleen gezien wordt door iemand die het gegeven ook mag zien. Degene die het gegeven maakt, bepaalt wie het mag zien. Vertrouwelijkheid is een van de kwaliteitskenmerken van gegevens.

Virtual Machine

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.

Virus

Vorm van schadelijke software die men op een computersysteem zet met als doel om het systeem uit

Malware

te schakelen, te beschadigen of gegevens te stelen. Men ontwerpt het virus zo dat het zichzelf probeert te verspreiden naar andere digitale systemen.

Vishing

Voice phishing.

Voice phishing

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.

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.

Vulnerability

...

Kwetsbaarheid

Vulnerability assessment

Handmatige controle waarbij men zwakke plekken in een systeem opspoorde. 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 management

Wat een organisatie doet om er voortdurend voor te zorgen dat zwakke plekken in de eigen digitale systemen worden opgespoord en hersteld.

Vulnerability scan

Een geautomatiseerde controle die zwakke plekken in een systeem opspoor. Alleen als het vals alarm is, haalt men die er handmatig uit.

Kwetsbaarhedenscan

Wachtwoord

Reeks van letters, cijfers en of andere karakters waarmee een gebruiker in een computersysteem 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

Wachtwoord manager

Software waarin een gebruiker de combinatie van wachtwoord en gebruikersnaam kan opslaan. Dit is een soort digitale kluis. Vaak kan de software ook zelf wachtwoorden aanmaken, websites herkennen en automatisch invullen. Ook geeft de wachtwoord manager vaak aan of een

wachtwoord sterk genoeg is, en of je deze al eerder hebt gebruikt.

WBNI

Wet Beveiliging Netwerk- en Informatiesystemen. 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).

White Team

...

Red Team, Red teaming, Blue teaming, Purple teaming

Whitebox test

...

Blackbox test

Whitehat hacker

Iemand die inbreekt in een computersysteem 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

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.

Blacklisting

Worm

Kwaadaardige code die zichzelf, zonder tussen-

Malware

komst van een mens, vermenigvuldigt en verspreidt over verschillende digitale systemen. Bekende voorbeelden van wormen zijn Wannacry en Notpetya.

XaaS

Algemene naam voor het uitbesteden van diensten. Bij cloud computing heet het IaaS (Infrastructure as a Service). Of 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).

XSS

Cross Site Scripting.

Cross site scripting

Zero trust

Model met strenge regels voor wie in een digitaal systeem mag, en wat hij daar mag zien en doen. 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-day

1. Afkorting voor zero day vulnerability. Een zwakke plek in software of hardware die nog 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. 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.

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

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.

Governance Board

Edwin van Andel

CEO

Zeroceptor

Bibi van den Berg

Hoogleraar Cybersecurity Governance

Universiteit Leiden

Sandor de Coninck

CTO en CISO

Rijkswaterstaat

Jessica Conquet

Voorzitter

PVIB (Platform voor Informatiebeveiliging)

Michel van Eeten

Hoogleraar Governance of Cybersecurity

TU Delft

Dirk Jan van den Heuvel

Managing Director

Secura

Ben Kokx

Director Product Security

Philips

Petra Oldengarm

Directeur

Cyberveilig Nederland

Michel Verhagen

Programmamanager

Digital Trust Center (DTC)

Ministerie van Economische Zaken en
Klimaat

Hans de Vries

Directeur

Nationaal Cyber Security Centrum (NCSC)

Ministerie van Justitie en Veiligheid

André Weimar

Directeur Inkoop-, Facilitair- en

Huisvestingsbeleid Rijk

Ministerie Binnenlandse Zaken en
Koninkrijksrelaties

Larissa Zegveld

Voorzitter

Forum Standaardisatie

Het Cybersecurity woordenboek is mede mogelijk gemaakt door:

Achmea	Expertise Centrum
AIVD	Ministerie van Economische Zaken en Klimaat / Digital Trust Center
AON	Ministerie van Infrastructuur en Waterstaat
Audittrail	Ministerie van Justitie en Veiligheid / NCSC
Axsemble	Ministerie van Justitie en Veiligheid / NCTV
Betaalvereniging Nederland	Ministerie van Volksgezondheid, Wetenschap en Sport
Bitdefender	MKB Cyberadvies Nederland
Chubb	Motiv
Cisco	Nationale Politie
Compumatica	NBIP
Computest	NIDV
Connectztrust	Northwave
Cybersprint	Océ
Cyberveilig Nederland	Onvio
Deep Blue Security	Onyx Cybersecurity
Digital Trust Center	Openbaar Ministerie
DINL	Philips
ECP	Platform voor Informatiebeveiliging (PVIB)
Eneco	Purasec
ERP Security	Qbit
ESET Nederland	Rabobank
Forum Standaardisatie	Secura
Fox-IT	SecWatch
Gemeente Rotterdam	Serverius
Guardian360	Siemens
Haagse Hogeschool	Soul:Made
HackDefense	Technische Universiteit Delft
Hague Security Delta (HSD)	Tektok
Hoffmann	Tesorion
Hudson Cybertec	Topicus
Informatiebeveiliging.nl	TÜV Nederland
KIWA	Universiteit Leiden
KnowBe4	Verbond van Verzekeraars
KPN Security	VNO NCW
Microsoft	Z-CERT
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	Zercopter
Ministerie van Defensie / Defensie Cyber	

Colofon

Cybersecurity Woordenboek. Van cybersecurity naar Nederlands.
2e druk

Uitgever: Cyberveilig Nederland

Redacteur: Petra Oldengarm / Liesbeth Holterman

Copyright: Creative Commons Naamsvermelding 4.0 Internationaal (CC BY 4.0)

www.cyberveilignederland.nl/woordenboek

ISBN 9789083026411.



Ministerie van Economische Zaken
en Klimaat



coolermedia
THE EXPLANATION COMPANY

Omslagontwerp en opmaak: Cooler Media

