DigiTaal

Cyberwoordenboek

voor onderwijs & onderzoek

powered by SURF

Voorwoord

In cybersecurity is aan afkortingen en vaktermen geen gebrek. En ga je met deze onderwerpen aan de slag in onderwijs en onderzoek, dan komt er nog een flinke hoeveelheid woorden bij. Denk bijvoorbeeld aan de namen van overlegstructuren, de diverse brancheorganisaties, de verschillende security community's, en security- en privacy-diensten die de sector veel gebruikt.

Dit DigiTaal Cyberwoordenboek voor onderwijs & onderzoek helpt je inzicht te krijgen in de terminologie die we hanteren en hoe we samenwerken. Juist voor onderwijs en onderzoek is dat belangrijk omdat we dan nog beter en sneller kennis kunnen delen. Zodat we als sector nog weerbaarder worden én blijven.

Deze publicatie is niet bedoeld als uitputtend naslagwerk, maar ik hoop dat het bijdraagt aan het spreken van dezelfde cybertaal. En dat het mensen helpt helpt sneller hun weg te vinden in de vele overlegstructuren en activiteiten op het gebied van cybersecurity in onderwijs en onderzoek. Alleen samen we komen we verder!

Ik wil iedereen heel hartelijk bedanken voor de bijdrage en inzet waardoor dit boek tot stand gekomen is. Heb jij suggesties of aanvullingen? Neem dan contact op via info@cybersaveyourself.nl

Rosanne Pouw
Productmanager Cybersave Yourself

Inleiding

Het idee voor dit boek ontstond omdat de sector onderwijs en onderzoek op het gebied van cybersecurity en privacy veel sectorspecifieke woorden, overleggen, organisaties en diensten heeft. Samenwerken is belangrijk voor onze sector: we hopen dat dit overzicht daaraan bijdraagt.

Voor de generieke cybersecurity-termen is gebruik gemaakt van het cybersecurity woordenboek, ontwikkeld en beheerd door Cyberveilig Nederland in samenwerking met het ECP, het Platform voor de InformatieSamenleving.

Dit woordenboek bevat:

- Termen in de context van cybersecurity. De toevoeging 'cyber' is daarom zoveel mogelijk weggelaten.
- Veelgebruikte termen door cybersecurity- en privacyprofessionals in onderwijs en onderzoek.
- Toelichting op deze termen, het zijn echter geen exacte definities.
- Algemene IT-termen die niet cybersecurity-specifiek zijn, en/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.
- Community's op het gebied van cybersecurity en privacy.
- Organisaties die zich inzetten voor cybersecurity en privacy.
- Certificeringen op het gebied van cybersecurity. De certificerende instanties die deze certificering bekrachtigen, zoals SANS, ISACA, ISC2, EC-Council, IAPP zijn niet opgenomen.
- De meeste vaktermen die voorkomen in de uitleg van de OWASP top 10.
- Securityprotocollen op internet.nl en de protocollen die vaak in gesprekken tussen aanbieders en afnemers van cybersecuritydiensten worden besproken.
- Normenkaders: SURF toetsingskader Informatiebeveiliging, SURF Toetsingskader Privacy en de ISO/IEC 27000.
- Geen namen van aanvallen en malware. Ook niet wanneer deze veel media-aandacht hebben gekregen zoals Stuxnet, WannaCry en NotPetya.

Leeswijzer

- Navigeer door het woordenboek door onderaan op een letter te klikken. Of zoek via het zoekvenster, of via Command-/Windows-toets + F
- Soms staat er achter een woord een woord in oranje vlak. Dat is een verwijzing naar een gerelateerde term. Bijvoorbeeld bij 'Chief Information Security Officer' wordt verwezen naar 'CISO' waar de uitleg te vinden is.
- 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.

Gerelateerde termen:

# #

0-day
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Zero-day

2FA
Tweefactorauthenticatie

Meerfactor-authenticatie

2-stapsverificatie
Tweefactorauthenticatie

Meerfactor-authenticatie

2-trapsverificatie
Tweefactorauthenticatie

Meerfactor-authenticatie

A

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

Aanvaller
Iemand die met kwade bedoelingen een aanval op een digitaal systeem uitvoert. Bijvoorbeeld door de beveiliging uit te schakelen of te omzeilen, of door een DDoS-aanval waardoor het systeem tijdelijk niet beschikbaar is.

Gerelateerde termen:

Acceptable risk level

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Risico-acceptatie

Acceptable Use Policy (AUP)

Beleid voor aanvaardbaar gebruik. Dit beleid bepaalt welke handelingen/activiteiten de gebruikers/klanten mogen verrichten. Bij het gebruik van een systeem buiten de AUP kunnen veiligheidsoverwegingen een rol spelen.

Access Control

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Toegangsbeheer

Access Control List (ACL)

Overzicht van gebruikers en systemen en hun toegangsrechten en bevoegdheden in een digitaal systeem of onderdeel daarvan.

Account

Element van een digitaal systeem dat een gebruiker representeert. Bij een account hoort informatie over de gebruiker, zoals persoonlijke gegevens, inloggegevens en informatie waar de gebruiker bij mag.

Account hijacking

Identity theft

Vorm van identiteitsdiefstal, namelijk het overnemen van een account.

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

Backdoor

Een achterdeur verwijst naar elke methode waarmee bevoegde en onbevoegde gebruikers de normale beveiligingsmaatregelen kunnen omzeilen en gebruikerstoegang kunnen krijgen op een computersysteem, netwerk of software.

Actor

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

Gerelateerde termen:

Admin

Gerelateerde termen: **Administrator**

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Administrator

Beheerder van een computersysteem of computernetwerk. Deze persoon heeft meer rechten dan een gewone gebruiker. Zo kan deze bijvoorbeeld instellingen aanpassen en bepalen wat gebruikers in een computernetwerk mogen doen en wat niet.

Adversary simulation

Gerelateerde termen: **Penetratietest**

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, ook wel Control team genoemd. 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.

Adware

Gerelateerde termen: **Malware**

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

AI

Artifical Intelligence of kunstmatige intelligentie. Dit zijn intelligente systemen die:

1. zelfstandig taken kunnen uitvoeren in complexe omgevingen, en
2. hun eigen prestaties verbeteren door te leren van ervaringen.

Algoritme

Set van regels en instructies die een computer uitvoert bij het maken van berekeningen om een probleem op te lossen of een vraag te beantwoorden.

Allow listing

Gerelateerde termen: **Whitelisting**, **Deny listing**

Actie waarmee je in een lijst vastlegt welke applicaties, gebruikers en acties je toestaat. Alles wat niet op de lijst staat wordt automatisch geblokkeerd. Het tegenovergestelde is blacklisting of deny listing.

Gerelateerde termen:

Analysesoftware
Software voor het analyseren van en werken met (statistische) data.

Anonimiseren
Maskeren, wijzigen of verwijderen van gegevens zodat deze niet meer herleidbaar zijn tot een persoon.

Anonymising proxy
Een proxyserver of proxydienst die gebruikt wordt om de oorsprong van netwerkverkeer mee te verbergen.

Anonymising VPN
VPN-server of VPN-dienst die de oorsprong van netwerkverkeer verbergt.

Antivirus software
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Endpoint detection response

AP
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Autoriteit Persoons-gegevens

API
Application Programming Interface. Een programma waarmee applicaties onderling communiceren zonder dat mensen dit aansturen.

Applicatie securitytest
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Vulnerability assessment

APT
Statelijke actor

Advanced Persistent Threat. Voortdurende dreiging van een geavanceerde tegenstander. Dit zijn met name statelijke actoren. Het gaat om cyberaanvallen waarbij de aanvaller langere tijd ongemerkt toegang heeft tot een informatiesysteem 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 motief, de vasthoudendheid en soms ook de gekozen middelen van de aanvaller.

Archivering
Opslaan van onderzoekspublicaties en -data in een online opslagservice.

Gerelateerde termen:

Assessment
Onderzoek naar de risico's van verschillende soorten dreigingen in één of meerdere digitale systemen. Voorbeelden van onderzoeken zijn penetratie-testen, 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, personeels-informatie etc.

Asset management
Het beheer van de digitale systemen die van waarde zijn voor een organisatie.

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. 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.

Public key infrastructure
Cryptografie

ATT&CK framework
Gecategoriseerde verzameling van aanvalstechnieken onder beheer van MITRE. Het MITRE ATT&CK framework wordt bijvoorbeeld gebruikt om inzichtelijk te maken tegen welke aanvalstechnieken een organisatie beschermd is en welke maatregelen nog nodig zijn. Het maakt ook inzichtelijk welke maatregel of technologie helpt tegen welke aanvalstechnieken.

Attack surface
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Aanvals-oppervlak

Gerelateerde termen:

Attribuut
(Persoons)gegeven gekoppeld aan een account. Wordt bijvoorbeeld bij SURFconext en SRAM gebruikt om toegang te geven.

Account
Digitale identiteit
SURFconext
SRAM
eduID

Audit
1. Onderzoek naar een onderdeel van een organisatie of proces, waarbij de werkelijke situatie vergeleken wordt met vastgestelde normen.
2. Systematisch, onafhankelijk en gedocumenteerd proces voor het verkrijgen van auditbewijsmateriaal, en het objectief beoordelen daarvan om vast te stellen in welke mate aan de auditcriteria is voldaan.

Audit log
1. Bestand waarin is vastgelegd wanneer, wie, wat heeft gedaan in een computersysteem. Soms is dit een wettelijke verplichting, zoals bij patiëntendossiers.
2. Bestand waarin staat in welke de onderdelen van een audit zijn uitgevoerd.

Auditor
Persoon die een audit uitvoert.

Audit

Authenticatie
Het verifiëren dat diegene die inlogt met het account van een gebruiker, proces of apparaat, ook diegene is aan wie die dit account is uitgereikt. Authenticatie is vaak een voorwaarde om toegang te verlenen tot bronnen in een informatiesysteem.

Identity en access management
SURFcertificaten
SURF Research Access Management

Autorisatie
De (toegangs)rechten 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 informatie.

SURF Research Access Management

Autorisatiematrix
Tabel met de uitgegeven rechten binnen een organisatie.

Gerelateerde termen:

Autoriteit Persoonsgegevens (AP)

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

Beschikbaarheid

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

AVG

Algemene Verordening Gegevensbescherming, de Nederlandse uitwerking van de Europese GDPR (General Data Protection Regulation) die ervoor zorgt dat in de hele EU dezelfde basisregels voor de bescherming van persoonsgegevens gelden. De AVG is de opvolger van de Wet bescherming persoonsgegevens.

Awareness

Bewustwording

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Awarenesstraining

Een training die erop is gericht het beveiligingsbewustzijn van medewerkers te vergroten. Een voorbeeld is een e-learning.

AWS

Amazon Web Services (AWS) is het cloudplatform van het Amerikaanse Amazon. SURF ontwikkelt ict-oplossingen en langdurige ondersteuning op de private cloud van SURF en op commerciële clouds zoals AWS en Azure.

Azure

Azure is het cloud computing platform van Microsoft. SURF ontwikkelt ict-oplossingen en langdurige ondersteuning op de private cloud van SURF en op commerciële clouds zoals AWS en Azure.

B

Gerelateerde termen:

Backdoor — Achterdeur
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Back-up
Een reservekopie van gegevens of digitale systemen. Hiermee kunnen gegevens of systemen hersteld worden 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).

Behavioural targeting — Profilering
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Beheersmaatregel
Een activiteit met als doel om de oorzaak of het gevolg van een ongewenste gebeurtenis te voorkomen, weg te nemen, of te verkleinen.

Beleidsgestuurd databeheer
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Benchmark — SURFaudit
Een techniek om de prestatie van verschillende systemen, apparaten of organisaties met elkaar te vergelijken.

Beschikbaarheid
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.

Gerelateerde termen:

Besturingssysteem
Een besturingssysteem is de fundamentele software die communiceert tussen de hardware en de gebruiker van een computer, smartphone of tablet, en die alle andere software en hardware op het apparaat beheert.

Betrouwbaarheid
Mate waarin digitale systemen (in een netwerk) beschikbaar zijn voor gebruik. Cyberaanvallen, uitval en storingen kunnen de betrouwbaarheid beïnvloeden.

Beveiliging
Alle maatregelen die nodig zijn om een digitaal systeem te beschermen tegen schadelijke invloeden.

Risico
Dreiging
Kwetsbaarheid
Asset

Beveiligingsincident(en)
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

SURFcert
Incident

Beveiligingslek
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Kwetsbaarheid
Zero-day

Beveiligingsmaatregel
Maatregel om risico's voor de veiligheid van informatie te verkleinen of weg te nemen.

Bewustwording
Het informeren en trainen van mensen zodat zij weten hoe ze cyberveilig en privacybewust kunnen werken en daar ook naar gaan handelen.

Cybersave Yourself

Bewustzijn
De mate waarin eindgebruikers op de hoogte zijn van cybersecurity-dreigingen en -risico's. Een hoog bewustzijn is belangrijk voor het voorkomen van incidenten.

Cybersave Yourself

Biometrie
Het bepalen van de identiteit van een persoon door middel van unieke biometrische gegevens, met bijvoorbeeld een vingerafdruk of irisscan.

Meerfactor-authenticatie

Gerelateerde termen:

BIV

Model om drie verschillende kenmerken van informatiebeveiliging aan te duiden:

- beschikbaarheid: is de informatie en het systeem op het gewenste moment te zien en te gebruiken?
- integriteit: klopt de informatie?
- vertrouwelijkheid: wie mag de informatie zien en het systeem gebruiken?

Beschikbaarheid **Integriteit** **Vertrouwelijkheid** **CIA**

Blackbox test

Veiligheidstest waarbij de tester 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** **Crystalbox 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

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Deny listing **Blocklisting** **Allow listing**

Blocklisting

Lijst van gebruikers, IP-adressen of applicaties die geblokkeerd worden in een systeem of netwerk.

Blokkeren & filteren

Techniek waarmee op geautomatiseerde wijze domeinen of websites ontoegankelijk worden gemaakt, of bepaalde informatie niet kan worden gedeeld. Blokkeren betekent dat een eindgebruiker geen toegang heeft tot een website op basis van de URL. Bij filteren heeft de eindgebruiker geen toegang tot bepaalde inhoud op een website.

Blue team/blue teaming

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Adversary simulation

Gerelateerde termen:

Bot

Een computerprogramma dat zelfstandig taken kan uitvoeren. Bot is een afkorting van robot. Een bot kan onschuldig zijn, bijvoorbeeld als zoekmachines bots gebruiken om websites te vinden. Maar iemand kan een bot ook gebruiken om in te breken in een computer. Of om de computer zo klaar te maken dat een ander kan inbreken. Een computer die besmet is met een bot, wordt ook wel een zombie genoemd. De gebruiker van een computer merkt vaak niets van een bot.

Botnet
Command-and-control server

Bot herder

Iemand die een botnet beheert.

Bot
Botnet

Botnet

Een netwerk van computersystemen die zelfstandig taken uitvoeren. Wordt vaak ingezet door cybercriminelen, bijvoorbeeld voor het versturen van spam of het uitvoeren van een DDoS-aanval. Een command-and-controlserver stuurt dit netwerk aan.

Command-and-control server

Bounty programme

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Bug bounty

Broncode

De leesbare tekst die een programmeur heeft geschreven in een programmeertaal. Er bestaan verschillende programmeertalen, zoals C, C++, Pascal.

Escrow

Brute force-aanval

Een aanvalsmethode waarbij iemand met verschillende methoden probeert je wachtwoorden of encryptiesleutels te achterhalen.

Bruto risico

Risico-inschatting waarbij niet wordt gekeken of men het risico kan verkleinen of wegnemen.

Netto risico

Buffer overflow

Situatie waarin een programma of besturingssysteem problemen krijgt doordat het meer data moet opslaan dan in het beschikbare geheugen 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 mag.

Kwetsbaarheid
Bug

Gerelateerde termen:

Bug
Een fout in de hardware of software van een digitaal systeem.

Bug bounty
Beloning voor het vinden en melden van een beveiligingslek in een digitaal systeem, gegeven door de eigenaar van het systeem.

Bulletproof hosting
Een hostingdienst (zoals cloud-hosting, dedicated servers of webhosting) die zeer tolerant is naar materiaal dat wordt opgeslagen of gedeeld via haar servers. Deze bedrijven nemen geen maatregelen bij abuse-meldingen, klachten of notificaties voor activiteiten op hun servers. Daarom zijn ze populair bij spammers, cybercriminelen en aanbieders van illegaal materiaal.

Business continuity
Vermogen van een organisatie om - zelfs bij een incident of crisis - producten en diensten te leveren met de vastgestelde capaciteit en binnen aanvaardbare termijnen.

Business continuity impact (BCI)
De gevolgen van een beveiligingsincident op de belangrijkste ict-bedrijfs-processen en applicaties.

Business continuity plan (BCP)
Gedocumenteerde informatie die een organisatie richting geeft te reageren op een verstoring, zodat zij de bedrijfsvoering kan herstellen en hervatten.

Business e-mail compromise (BEC)
CEO-/CFO-/ CxO-fraude

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.

Business impact analyse (BIA)
Proces voor het analyseren van de impact in de tijd gemeten van een verstoring op de organisatie. Deze analyse is onderdeel van een Business Continuity Plan en is te gebruiken om je voor te bereiden op grote storingen.

Gerelateerde termen:

C

BYOD
Bring Your Own Device. Gebruikers mogen hun eigen apparaten - zoals een prive laptop of telefoon - gebruiken op een zakelijke computernetwerk.

C&C server
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Command-and-control server

CA (Certificate authority)
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Certificate authority

Captcha
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.

Capture the flag (CTF)
Tijdens een capture the flag (CTF) dag strijden verschillende teams tegen elkaar om zo snel mogelijk vooraf bepaalde flags (stukjes informatie) te veroveren. Ze doen dit via verschillende manieren van hacken.

CASB
Cloud Access Security Broker

Cloud access security broker

Catfishing
Persoonlijke gegevens stelen via nagemaakte sociale netwerksites en dating-sites. Het gaat meestal om persoonlijke informatie, creditcardnummers of geld. Een social engineering techniek.

Social engineering

Gerelateerde termen:

Cbw/Cyberbeveiligingswet

De Cyberbeveiligingswet is de Nederlandse uitwerking van de Europese NIS2-richtlijn. De NIS2-richtlijn wil de cyberveiligheid in de Europese Unie naar een hoger gemeenschappelijk niveau brengen door de digitale weerbaarheid van zogenoemde kritieke entiteiten (organisaties die essentieel zijn voor de samenleving) te versterken. Risicomanagement en incidentmanagement zijn belangrijke onderwerpen in de Cbw.

CEH (Certified Ethical Hacker)

Certified Ethical Hacker

Certified Ethical Hacker

Censorship

Censuur. Informatie ontoegankelijk maken, of het onmogelijk maken om informatie te delen.

CEO-/CFO-/CxO-fraude

Vorm van fraude waarbij een aanvaller e-mails verstuurt aan een financiële afdeling zogenaamd uit naam van de CEO of CFO van een bedrijf. De aanvaller wil hiermee een medewerker van de financiële afdeling overtuigen of onder druk zetten om geld over te maken.

Spear phishing

CERT (Computer Emergency Response Team)

Computer Emergency Response Team, naam bedacht door Carnegie Mellon voor het eerste response team ter wereld. Ook de term Computer Security Incident Response Team (CSIRT) wordt gebruikt.

CSIRT

SURFcert

Certificaat

1. Digitaal document dat aantoont dat een product, digitaal systeem of persoon is wie deze zegt dat die 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.

SURFcertificaten

Certificate authority

Erkende instantie die digitale certificaten uitgeeft. Daarvoor stelt ze eerst vast dat de aanvrager is, wie deze zegt te zijn.

SURFcertificaten

Certificate schema

Systeem om een bepaald type producten te beoordelen. De producten moeten voldoen aan dezelfde eisen, regels en procedures. Een certificeringssysteem staat in ISO/IEC17000: 2004.

Gerelateerde termen:

Certificerende instelling

Instantie of instelling die 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.

Certified Ethical Hacker

Certificering voor professionals in informatiebeveiliging, specifiek voor ethisch hacken.

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 (CISO)

De medewerker die aangewezen verantwoordelijk is voor informatie-beveiliging. Dit is een rol op strategisch niveau. De directie blijft altijd de eindverantwoordelijke voor informatiebeveiliging.

CIA (Confidentiality, Integrity en Availability)

BIV

De Nederlandse afkorting is BIV: Beschikbaarheid, Integriteit en Vertrouwelijkheid, waarbij de termen in een andere volgorde worden genoemd.

CISM (Certified Infromation Security Manager)

Dit is een certificering voor professionals in informatiebeveiliging.

CISO (Chief Information Security Officer)

Chief Information Security Officer

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

CISSP (certified Information System Security Professional)

Dit is een certificering voor professionals in informatiebeveiliging.

Gerelateerde termen:

Classificatie

BIV

Beoordeling hoe gevoelig of belangrijk informatie of een systeem is. Dit is nodig om de juiste maatregelen te kunnen nemen om de informatie of het systeem te beschermen. En ook het systematisch indelen in groepen of categorieën, volgens vastgestelde criteria. Bij security classificatie wordt vaak gebruik gemaakt van BIV: beschikbaarheid, Integriteit en Vertrouwelijkheid.

Click fraud

Klikfraude

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Closed source

Open source

Software waarvan de broncode door de auteurs niet wordt vrijgegeven.

Cloud access security broker

Een beveiligingsoplossing voor toepassingen in de cloud. Daarbij wordt een schakel geplaatst tussen het bedrijfsnetwerk en de cloud. Dat levert de volgende voordelen op:

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

Cloud based security

Cloud security

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

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.

Clouddiensten

SURFconext

Software die op externe servers staat en waar je online toegang toe kunt krijgen om deze te gebruiken.

Cloudopslagdienst

SURFdrive

Bestanden veilig bewaren, synchroniseren en delen. Dat kan in de commerciële cloud of met SURFdrive in de communitycloud van SURF.

Gerelateerde termen:

Code assessment

Code audit

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Code audit

Een analyse van de broncode van een programma, met als doel zwakke plekken te vinden. Dit gebeurt volgens een norm die vooraf objectief is vastgesteld. Een code audit gebeurt voor een groot deel handmatig.

Code execution

Aanval 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 onder meer om zwakke plekken te vinden. Je zoekt voor een groot deel handmatig, en niet aan de hand van een uitputtende lijst van kwetsbaarheden.

COMIT

Coördinerend Overleg Managers Informatie-Technologie van hogescholen.

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. Dit kan een eenvoudige taak zijn, zoals het openen van een programma, of een complexe actie die systeemwijzigingen doorvoert.

Command-and-control server

De machine die een aanvaller gebruikt om commando's te sturen naar systemen waarin die heeft ingebroken. Bijvoorbeeld als de aanvaller een DDoS-aanval wil doen of een bot in een botnet wil aansturen.

Communitycloud

SURFdrive

Een exclusieve cloud voor een specifieke community waar je bestanden kunt opslaan. SURFdrive is de communitycloud voor het Nederlandse onderwijs en onderzoek.

Gerelateerde termen:

Compartimentering

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Segmentering

Compliance

De activiteiten die worden uitgevoerd 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.

SURFaudit

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 grondslagen van het dataprotectierecht en privacyrecht. Data mogen niet verwerkt worden, tenzij de persoon waarover de data gaan, toestemming heeft gegeven. Deze toestemming is expliciet, geïnformeerd, vrijwillig en ondubbelzinnig.

Control

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Beheersmaatregel

Control framework

Principes, uitgangspunten, manieren van denken, processen en afspraken die een organisatie gebruikt voor het omgaan met veiligheidsrisico's.

Control team

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Adversary simulation

Convention on Cybercrime

Convention on Cybercrime van de Council of Europe. Internationaal verdrag dat tot doel heeft om de wetten van de aparte landen op het gebied van cybercrime op elkaar aan te laten sluiten. Het Verdrag beoogt landen samen te laten werken op dit terrein en kennis uit te laten wisselen op het gebied van opsporingstechnieken. 63 landen hebben dit verdrag geratificeerd, en nog eens 4 landen hebben het getekend.

Gerelateerde termen:

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 eigenaar van de website bewaart de informatie om die later te kunnen gebruiken voor analyses en marketing.

Coordinated Vulnerability Disclosure
Coordinated vulnerability disclosure is de praktijk van het gecoördineerd melden van aangetroffen beveiligingslekken. Hierbij worden afspraken gehanteerd die doorgaans neerkomen op dat de melder de ontdekking niet deelt met derden totdat het lek verholpen is, en de getroffen partij geen juridische stappen tegen de melder zal ondernemen. Voorheen werd dit responsible disclosure genoemd.

Cracker
Een aanvaller die met kwade bedoelingen in een computernetwerk inbreekt, bijvoorbeeld om gegevens te stelen of een netwerk te beschadigen.

Hacker

Cracking
Met kwade bedoelingen in een computernetwerk inbreken, bijvoorbeeld om gegevens te stelen of een netwerk te beschadigen.

Hacken

Credential harvesting
Het aanvallen van een organisatie om op illegale wijze inloggegevens (van werknemers) te verkrijgen.

Credentials
De gegevens waarmee een gebruiker of ander computersysteem bij een computersysteem kan aantonen dat die is wie deze zegt te zijn. Bijvoorbeeld een gebruikersnaam in combinatie met een wachtwoord of een via SMS opgestuurde code.

Crisismanagement
Gecoördineerde activiteiten om een organisatie te leiden, sturen en controleren met betrekking tot crisis. Een crisis is een abnormale of buitengewone gebeurtenis of situatie die een organisatie of gemeenschap bedreigt en een strategische, adaptieve en tijdige reactie vereist om de levensvatbaarheid en integriteit te behouden.

Crisisoefening
Het oefenen van het reactievermogen van een organisatie bij een groot cyberincident.

OZON/NOZON

Gerelateerde termen:

Critical infrastructure
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Kritieke infrastructuur

Cross site request forgery
Een aanvaller lokt een gebruiker naar een andere webpagina. Zo kan deze 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 functionaliteiten die niet voor hem bedoeld zijn.

Crypto
Cryptografie

Cryptografie
Cryptovaluta

Crypto mule/crypto-ezel
Iemand die zijn account van een online cryptocurrency-wallet beschikbaar stelt aan criminelen. Criminelen gebruiken deze accounts om er geld op te laten storten dat ze hebben gestolen door oplichting en deze vervolgens om te wisselen naar cryptocurrency. Wordt ook wel crypto-ezel genoemd.

Cryptografie
Informatie omzetten in een code zodat een ander het niet kan lezen. Dit doe je als je gevoelige informatie veilig wil bewaren of versturen. Meestal bestaat cryptografie uit een algoritme voor versleutelen en ontsleutelen en één of meerdere sleutels.

Asymmetrische versleuteling

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
Proces waarbij computers complexe wiskundige problemen oplossen om cryptocurrency-transacties te verifiëren en toe te voegen aan een block-chain. Cryptomining omvat alle transacties in een blockchain: het maken, verzamelen, controleren en verwerken van cryptovaluta.

Cryptovaluta
Digitaal ruilmiddel. Een bekende cryptovaluta is de bitcoin.

Gerelateerde termen:

Crystalbox test
Veiligheidstest van een systeem waarbij de tester veel voorkennis heeft van het systeem. Bijvoorbeeld toegang tot de broncode.
Blackbox test

CSIRT
Computer Security Incident Resonse Team
CERT
SURFcert

CSMS
Cyber Security Management System. Dit systeem houdt bij of de maatregelen voor informatiebeveiliging goed werken.
ISMS

CSRF
Cross Site Request Forgery
Cross site request forgery

CVD
Coordinated Vulnerability Disclosure
Coordinated Vulnerability Disclosure

CVE
Common Vulnerabilities and Exposures. Een openbare lijst van bekende zwakke plekken in software. De lijst staat op cve.org.

CVSS
Common Vulnerability Scoring System. Systeem om een score te geven aan een zwakke plek in software. Hoe hoger de score, hoe zwakker de plek. Een organisatie kan deze score gebruiken om te bepalen welke zwakke plekken ze als eerste gaat oplossen. Meer informatie over het scoresysteem staat op www.first.org/cvss.

CWE
Common Weakness Enumeration. Een openbare lijst met bekende soorten zwakke plekken in software. De lijst is te vinden op cve.org

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

Cyber defense
Verdediging op nationaal niveau tegen cyberaanvallen met strategische of militaire middelen.

Gerelateerde termen:

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 resilience
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Gerelateerde termen: **Cyber-weerbaarheid**

Cyberaanval
Een gerichte aanval in of via cyberspace. Doelwitten kunnen zijn: personen, groepen, bedrijven en organisaties, overheden, andere landen.

Cyberattack
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Gerelateerde termen: **Cyberaanval**

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
Certified Ethical Hacker

Cybercrisis
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Gerelateerde termen: **Cybercrisis-oefening** **(N)OZON**

Cybercrisisoefening
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Gerelateerde termen: **(N)OZON**

Cyberdreiging
Een actor met een motief en een methode om schade aan een digitale omgeving toe te brengen.

Gerelateerde termen:

Cyberhygiëne
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 bevorderen van veilig gedrag van personeel.

Cybersabotage
Opzettelijk en langdurig de beschikbaarheid van digitale diensten, processen of systemen aantasten. Sabotage vereist een langdurige voorbereiding (maanden of jaren), specifieke technische kennis en is voornamelijk afkomstig van statelijke actoren. Digitale sabotage kan ingrijpende gevolgen hebben.

Cybersave Yourself
Awareness toolkit met awarenessmateriaal voor onderwijs en onderzoek.

Cybersecurity
Alle beveiligingsmaatregelen die je 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 te herstellen als die toch is ontstaan. Voorbeelden van schade zijn dat je niet meer in een computersysteem kan komen wanneer je 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
Het 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 digitaal worden uitvoerd. Bijvoorbeeld het beschadigen of uitschakelen van belangrijke informatienetwerken via internet.

Cyberveilig
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Cyber-weerbaarheid

Gerelateerde termen:

Cyberverzekering
Een verzekering die uitkeert bij financiële schade die ontstaat als gevolg van een datalek, virus, hack of andere cyberaanval. De verzekering keert uit voor schade bij de organisatie zelf, als ook voor schade die ze aan anderen moeten vergoeden. Daarnaast bieden de meeste verzekeraars ook dekking aan in de vorm van diensten, zoals assistentie, forensische expertise, herstel of communicatie. Uitkering hangt af van dekking en polisvoorwaarden.

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

Cyberweerbaarheid
Het vermogen om (relevante) digitale risico's tot een aanvaardbaar niveau te reduceren. Dat gebeurt door middel van een verzameling van maatregelen om cyberincidenten te voorkomen. En wanneer cyberincidenten zich hebben voorgedaan, deze te ontdekken, schade te beperken en herstel eenvoudiger te maken.

D

DANE
DNS

DANE staat voor DNS-Based Authentication of Named Entities en is een protocol dat een extra beveiligingslaag toevoegt aan internetcommunicatie, met name voor e-mail en websites.

Dark net
Dark web

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Dark web
Een besloten deel van het internet dat je niet vindt met normale browsers en zoekmachines. Het staat vooral bekend als een plek waar criminelen hun zaken doen.

Gerelateerde termen:

DAST
Dynamic Application Security Testing. Categorie van softwaretools die een applicatie testen op kwetsbaarheden, terwijl deze in werking is.

Data leak prevention
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

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.

Datacenter
Een datacenter, of data processing center (DPC), is een faciliteit voor het hosten van data van één of meer bedrijven. Het is een fysieke ruimte met een groot aantal servers.

Datalek
Bij een datalek gaat het om toegang tot persoonsgegevens zonder dat dit mag of zonder dat dit de bedoeling is. Waarbij de oorzaak een inbreuk op de beveiliging van deze gegevens is. Ook het ongewenst vernietigen, verliezen, wijzigen of verstrekken van persoonsgegevens door zo'n inbreuk valt onder een datalek.

AVG

Dataleverancier
Een dataleverancier verzamelt gegevens vanuit één of meerdere bestaande databronnen en stelt deze data ter beschikking aan derden. Bij een cyber-crime levert een dataleverancier gegevens zijn slachtoffers aan fraudeurs. Deze gegevens kunnen komen uit bestaande en nieuwe datalekken of de dataleverancier steelt zelf gegevens. De gegevens worden voornamelijk verhandeld via het darkweb en via (veelal besloten) sociale media groepen binnen Facebook en Telegram.

Datamanagement
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

iRODS Hosting

Datatransferprotocollen
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Rekendienst
Data Archive

Gerelateerde termen:

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
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Ontsleutelen
Cryptografie

Deep fake
Deepfakes zijn media gemaakt of bewerkt door AI waarbij het beeld, de stem of de video wordt vervangen door de beeltenis van iemand anders.

Deep learning
Een subveld van kunstmatige intelligentie (AI) en machinaal leren waardoor computers complexe patronen kunnen herkennen in grote datasets. Het wordt bijvoorbeeld gebruikt in beeld- en spraakherkenning of het besturen van zelfrijdende auto's.

Machine learning

Deep packet inspection
Algemene naam voor technieken om in detail gegevens mee te analyseren die via netwerken verspreid worden. Hierbij wordt meer dan alleen het adres van de afzender en de ontvanger onderzocht. Het doel is om zo meer bedreigingen te kunnen opsporen. Dit maakt het mogelijk om cyberaanvallen, malware en ongewenst verkeer te detecteren, beleid af te dwingen, en het netwerk te optimaliseren.

Deep web
Het deep web - vaak verward met het dark web - bevat alle inhoud die niet door zoekmachines wordt geïndexeerd, zoals e-mailaccounts, databases en inhoud achter logins.

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

Gerelateerde termen:

Defense in depth
Meerlaagse/gelaagde beveiliging: achter elkaar schakelen van beveiligingsmaatregelen, zodat als er één faalt, de anderen een aanval alsnog tegenhouden.

Defensive capabilities
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Cyber defense

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

Distributed Denial of Service-aanval

Deny listing
Actie waarmee in een lijst wordt vastgelegd welke applicaties, gebruikers en acties worden blokkeerd. Al het andere dat niet op de lijst staat is dus wel toegestaan. Het tegenovergestelde is whitelisting of allow listing.

Blacklisting
Blocklisting
Allow listing

Desinformatie
Misleidende of afleidende informatie die met opzet verspreid wordt.

Nepnieuws

Detectiecapaciteit
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

SURFsoc

DevSecOps
Softwareontwikkeling die rekening houdt met de veiligheid vanaf het begin van het ontwikkelingsproces en tot het einde van de levenscyclus van een product. Is een combinatie van de woorden ontwikkeling, beveiliging en operaties.

Digitale certificaten
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

SURFcertificaten
certificaten

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

Gerelateerde termen:

Digitale identiteit

eduID

Een set van gegevens die horen bij een persoon of andersoortige entiteit. Deze gegevens zijn online beschikbaar. Hiermee kun je toegang krijgen tot diensten. Waar mogelijk bepaal je zelf welke identiteitgegevens je deelt en met wie.

Digitale sabotage

Cybersabotage

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Digitale soevereiniteit

De mate waarin landen en staten in staat zijn hun eigen data, informatiesystemen en technologische infrastructuur onder controle te hebben en te houden.

Digitale spionage

Cyberspionage

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Digitale veiligheid

Situatie waarin je geen schade hebt of krijgt door verstoring of uitval van ict.

Digitale leer- en werkomgeving

De digitale leer- en werkomgeving (DLWO) is het geheel van systemen dat studenten, onderzoekers en medewerkers van een onderwijsinstelling in staat stelt hun activiteiten uit te voeren. De DLWO is dus een combinatie van digitale diensten.

Disaster recovery plan (DRP)

Business continuity plan

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

Disk image

Forensic image

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Distributed Denial of Service-aanval (DDos)

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 gewaarmerkt. Het gebruik van DKIM verkleint de kans op misbruik van e-mailadressen doordat ontvangers betrouwbaar echte e-mails van phishingmails of spam kunnen onderscheiden. Ook kunnen ontvangers controleren of de inhoud van de e-mail door derden is gemanipuleerd.

Gerelateerde termen:

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
DNS-beheer
SURFdomeinen

DNS-beheer
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

DNSSEC
SURFdomeinen

DNS-firewall
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

SURFdomeinen

DNSSEC
Domain Name System Security Extensions. Beveiligingsoplossing om een aanval op een domeinnaam tegen te gaan. In vaktaal heet zo'n aanval DNS-spoofing. Bij zo'n aanval wordt bijvoorbeeld een bezoeker van een bepaalde website doorgestuurd 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.

SURFdomeinen

Domeinnaam
Een unieke naam op internet. Meestal geldt een domeinnaam voor websites, maar je kan ook een domeinnaam aanvragen voor een persoonlijk mailadres.

IP-adres

Gerelateerde termen:

DoS
Denial of Service

Denial of Service-aanval

Double extortion
Aanval waarbij bestanden of systemen van het slachtoffer zijn versleuteld: de sleutel wordt tegen betaling aangeboden. Naast versleuteling worden gevoelige gegevens van het slachtoffer buitgemaakt, betaling moet voorkomen dat ze gelekt worden.

Single Extortion
Triple Extortion
Quadruppel Extortion

Doxing/Doxxing
Aanval waarbij vertrouwelijke informatie over een persoon of organisatie publiek wordt gemaakt. Dit gebeurt doorgaans via het internet. Deze informatie wordt verkregen via open bronnen, social engineering of via (vaak ongeautoriseerde) toegang tot gesloten systemen. De doeleinden waarvoor doxing kan worden toegepast zijn: shaming, afpersing of als ongevraagde hulp aan de opsporing.

DPA
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 de Algemene Verordening Gegevensbescherming.

Privacy impact assessment

DPO
Data Protection Officer. De medewerker die controleert of een organisatie zich houdt aan de regels van de AVG.

AVG

Dreiging
Een actor met een motief en een methode om schade aan een digitale omgeving toe te brengen.

Risico

Dreigingsinformatie
Verzamelde, verrijkte en geanalyseerde informatie over dreigingen in het digitale domein. Met als doel deze dreigingen tijdig te identificeren en de weerbaarheid van de ontvangers te verhogen.

Threat intelligence

Gerelateerde termen:

Dreigingslandschap
Een overzicht van alle mogelijkhe 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 van clouddiensten, online zoekmachines en/of online marktplaatsen. Een DSP valt in bepaalde omstandigheden onder de verplichtingen van de wet beveiliging netwerk- en informatiesystemen (Wnbi), die wordt vervangen door de Cyberbeveiligings-wet (Cbw).

DTC (Digital Trust Center)
Het DTC is door het Ministerie van Economische Zaken opgericht en heeft als missie om ruim 2 miljoen Nederlandse bedrijven weerbaarder te maken tegen toenemende cyberdreigingen.

DTIA
Data Transfer Impact Assessment. Een DTIA kan zelfstandig of als onderdeel van een Data Protection Impact Assessment (DPIA) en beoordeelt de impact wanneer je persoonsgegevens deelt met een ontvanger buiten de Europese Economische Ruimte (EER).

SURF Vendor Compliance

DPIA

Dual control
Beveiligingsmaatregel 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
Alle technologie die 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.

Gerelateerde termen:

Dutch Institute for Vulnerability Disclosure (DIVD)
Vrijwilligersorganisatie die scans uitvoert op het Internet naar bekende kwetsbaarheden in digitale systemen. Als ze deze vinden, maken ze een melding bij de organisaties waar ze zijn aangetroffen. De organisatie werkt wereldwijd. Ook leiden ze hackers op.

DLWO (Digitale Leer- en Werk Omgeving)
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Digitale Leer- en Werk Omgeving

E

E-discovery
Grote aantallen elektronische data doorzoeken met een bepaald doel. Meestal een juridisch onderzoek of een rechtszaak.

EDR
Endpoint Detection and Response

Endpoint detection response

edu.nl
Met edu.nl kun je een willekeurige lange URL korter maken. Je kunt een link aanmaken die begint met edu.nl. Edu.nl is veiliger en privacy-vriendelijker dan commerciële alternatieven. Alleen personen uit het mbo, hbo, wo en bij SURF aangesloten instellingen kunnen links aanmaken. Iedereen kan een edu.nl-link openen. Edu.nl slaat geen persoonsgegevens op en trackt bezoekers niet.

eduID
Een eduID is een account voor gebruikers binnen onderwijs en onderzoek. Het is van jou, en bestaat onafhankelijk van een onderwijsinstelling. Je kunt eduID bijvoorbeeld gebruiken als je bij meerdere instellingen tegelijk onderwijs wilt volgen. Of na je studie, als je naast je werk een opleiding of cursus wilt volgen.

Gerelateerde termen:

eduroam

Eduroam (education roaming) maakt het voor leerlingen, studenten, onderzoekers en medewerkers mogelijk om op een veilige manier gebruik te maken van het draadloze netwerk van hun onderwijs- of onderzoeksinstelling. Zij kunnen daarnaast met hun eigen inloggegevens probleemloos gebruik maken van het eduroam-netwerk bij andere onderwijs- of onderzoeksinstelling wereldwijd.

eduroam Visitor Access

Met eduroam Visitor Access kunnen bezoekers van onderwijs- en onderzoeksinstellingen op een laagdrempelige en veilige manier toegang krijgen tot het vertrouwde eduroam wifi-netwerk.

Gerelateerde termen: eduroam

eduVPN

eduVPN maakt het medewerkers, onderzoekers en studenten mogelijk om op een veilige en eenvoudige manier te verbinden met internet en toegang te krijgen tot afgeschermde systemen van hun instelling.

Gerelateerde termen: Virtual Private Network

E-mailondertekening

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Gerelateerde termen: SURFcertificaten

E-mailspoofing

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Gerelateerde termen: Spoofing

Encryptie

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Gerelateerde termen: 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.

Gerelateerde termen: Patch, Update

Endpoint detection response

Software die computers, laptops en vergelijkbare digitale apparaten beschermt tegen kwaadaardige software. Bij deze beschermende software worden kenmerken van al bekende kwaadaardige software gebruikt. Of kenmerken van opvallend gedrag van nieuwe software in een computersysteem. Deze software wordt bij een incident gebruikt om specifieke zoekopdrachten uit te voeren op digitale systemen. Dit helpt bij het oplossen van het incident.

Gerelateerde termen:

End-to-end encryptie

SURFfilesender

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

ENISA

European Union Agency for Network and Information Security. Europees agentschap dat als doel heeft netwerken en informatie binnen de EU beter te beveiligen.

Escrow

Een softwareleverancier vraagt een ander onafhankelijk bedrijf om ervoor te zorgen dat de broncode van een computerprogramma vertrouwelijk wordt bewaard, bijvoorbeeld voor het geval dat de leverancier failliet gaat of bij een juridisch conflict.

Ethical hacker / Etische hacker

Whitehat hacker

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Exfiltration/ Exfiltratie

Aanval waarbij vertrouwelijke informatie van een gehackte organisatie naar de systemen van de hacker of een nader gehackt systeem wordt verplaatst..

Exploit

Aanval waarmee iemand programmacode of een reeks acties gebruikt om 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. Een exploit is te 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.

Externe audit

SURFaudit

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Gerelateerde termen:

F

Fail Safety
Beveiligingsmaatregel die ervoor zorgt dat bij een storing of defect het beveiligde object in een veilige status blijft. Bijvoorbeeld: bij stroomuitval blijven alle buitendeuren gesloten.

FAIR-principes
De FAIR-principes zijn een richtlijn om wetenschappelijke data beter vindbaar, toegankelijk, uitwisselbaar en herbruikbaar te maken.

Fake news
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Nepnieuws

False negative
De situatie dat een beveiligingssysteem een dreiging of aanval niet opmerkt terwijl deze wel plaatsvindt.

False positive
De situatie dat een beveiligingssysteem een dreiging of aanval opmerkt terwijl er niets gebeurt.

Federatieve authenticatie en autorisatie (infrastructuur)
Een infrastructuur waarbij verschillende organisaties samenwerken om gebruikersidentiteiten en toegangsrechten te beheren. Bestaat doorgaans uit een deel afspraken en een deel techniek.

SURFconext
eduID
SRAM

FG
Functionaris Gegevensbescherming

Functionaris Gegevens-bescherming

Filteren & blokkeren
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Blokkeren & filteren

Gerelateerde termen:

Firewall
Hardware of software die computers en netwerken beschermt tegen aanvallen. Een firewall bekijkt alles wat over het netwerk gaat en blokkeert bepaald verkeer op het netwerk.

SURFfirewall

Firewall-regels
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

SURFfirewall

FIRST
FIRST is het wereldwijde Forum of Incident Response and Security Teams. SURFcert is lid van FIRST.

SURFcert

Forensic image
Een exacte kopie van bijvoorbeeld een harde schijf, USB-stick of geheugen van een digitaal systeem. In de kopie staat alle informatie die nodig is om te achterhalen wat er op het origineel staat en heeft gestaan. Denk aan bestanden en mappen, soms ook als ze al verwijderd zijn. Beveiligingsbedrijven, politie en openbaar ministerie gebruiken deze kopie vaak voor onderzoek.

Forensisch onderzoek
Technisch sporenonderzoek op (forensische kopieën van) digitale systemen tijdens of na een aanval. De onderzoekers verzamelen en analyseren bewijsmateriaal en proberen zo vragen te beantwoorden over de aanval. Bijvoorbeeld wanneer en hoe de aanval heeft plaatsgevonden, welke informatie is gestolen en wie achter de aanval zat.

Incident response

Functiescheiding
Het uitgangspunt dat verschillende personen nodig zijn om een serie van kwetsbare activiteiten uit te voeren. Bijvoorbeeld, een persoon geeft toestemming voor een nieuw account. Een ander maakt het account aan. Weer een ander bepaalt de rechten die iemand krijgt. Zo kan niet één persoon alles zelf uitvoeren, waardoor het risico op misbruik afneemt.

Functionaris Gegevensbescherming
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.

Gerelateerde termen:

G

Gap-analyse
Analyse om te bepalen in hoeverre een systeem of organisatie voldoet een de veiligheidseisen. En wat de organisatie eventueel nog moet regelen om aan alle eisen te voldoen.

GDPR
Gerelateerde termen: AVG

General Data Protection Regulation. Algemene Verordening Gegevens-bescherming (AVG) is de Nederlandse uitwerking van deze Europese regelgeving.

GÉANT
GÉANT (Gigabit European Academic Network) is het pan-Europese datanet-werk voor de onderzoeks- en onderwijsgemeenschap. Het verbindt nationale onderzoeks- en onderwijsnetwerken (NREN's) in heel Europa. SURF is de NREN in Nederland.

Gebruikersnaam
Gerelateerde termen: Inlogcode

Naam waarmee een gebruiker in een computersysteem kan inloggen.

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

Gijzelsoftware
Gerelateerde termen: Ransomware

Kwaadaardige software waarbij een slachtoffer afgeperst wordt, nadat diens digitale systeem of de bestanden erop met een code op slot zijn gezet (gegijzeld). De aanvaller biedt de code tegen betaling aan, zodat het slacht-offer er weer bij kan.

Governance
Gerelateerde termen: SURFaudit

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

GRC-tool
Gerelateerde termen: SURFaudit

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Gerelateerde termen:

Greybox test

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Blackbox test

Greyhat hacker

Iemand die met zijn handelen soms ethische of juridische grenzen over gaat, maar geen kwade of criminele bedoelingen heeft, zoals een blackhat hacker.

Hacker
Whitehat hacker
Blackhat hacker

Grooming

Het proces waarbij een dader het vertrouwen wint van het slachtoffer, met als doel deze persoon te misbruiken door aanranding, verkrachting, uitbuiting, de productie van (kinder)porno, ontvoering of mensenhandel.

H

Hack

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Hacken

Hacken

1. Actie om in of bij een computer, netwerk, hardware of software te komen. Als je dat ongevraagd of zonder geldige reden doet, is zo'n actie illegaal.
2. Het vinden van nieuwe toepassingen. Bijvoorbeeld tijdens hackathons, workshops waarin je 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

Gerelateerde termen:

Hacktivist
Samentrekking van de woorden hacker en activist: actor die uit ideologische motieven digitale aanvallen van activistische aard pleegt..

Hall of Fame / Wall of Fame
Een lijst met namen van hackers die hebben meegeholpen een informatiesysteem te beveiligen. Bijvoorbeeld door zwakke plekken in de beveiliging te vinden en die te melden bij de leverancier via coordinated vulnerability disclosure (CVD).

CVD
Hacker

Hardening
Niet-gebruikte functies in hardware en software uitzetten of weghalen. En de rechten van andere functies waar mogelijk beperken. Zo verklein je het aanvalsoppervlak en daarmee het risico van aanvallen.

Hash / Hashwaarde
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Hashing

Hashing
Bij hashing haal je gegevens door een formule en krijg je een reeks tekens terug — een hash genaamd. Het is, net zoals encryptie, een manier om online data te beveiligen tegen hackers en cybercriminelen.

HBO-CISO
Overleg waar CISO's van de hogescholen in zijn vertegenwoordigd.

Hertest
Vervolgtest om na te gaan of de zwakke plekken die eerder bij een penetratietest zijn gevonden, inderdaad weg zijn.

Penetratietest

Heuristic detection
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Machine learning

Honey token
Gegevens met een speciaal kenmerk, die bij diefstal terug te vinden zijn. Zo kan je 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 computer-systeem wil aanvallen. Daarna kan je deze software analyseren.

Deception technology

Gerelateerde termen:

Host
Een apparaat dat via internet kan communiceren met een ander apparaat. Een host heeft een eigen hostnaam en IP-adres.

Hostnaam
De naam van een digitaal systeem. Samen met het domein waar het systeem bijhoort 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

HyperText Transfer Protocol Secure (HTTPS)
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 (deel)oorzaak van cybersecurity-incidenten. Denk bijvoorbeeld aan nalatigheid, iets niet of verkeerd begrijpen, iets vergeten te doen, of een verkeerde handeling uitvoeren.

Human factor
Menselijke factor. Als iets misgaat in de cybersecurity, komt dat regelmatig ook door een menselijke factor: iemand maakt een fout. Vaak heeft deze persoon dat zelf niet door.

Hunting
Zoektocht naar sporen in netwerkverkeer of op digitale systemen van aanvallen die beveiligingsmaatregelen hebben omzeild. Hunting gebeurt veelal handmatig.

Gerelateerde termen:

I

Industrial and Automation Control Systems (IACS)

Verzameling netwerken, control systemen, SCADA-systemen en andere systemen die kwetsbaar zijn voor cyberaanvallen.

IAM

Identity en Access Management

Identity en access management

IBP-netwerk

Netwerk Informatiebeveiliging en Privacy; netwerk van security- en privacy-professionals bij mbo-instellingen. Het netwerk wordt aangestuurd door de Regiegroep IBP, waarin 10 mbo-instellingen zijn vertegenwoordigd, aangevuld met experts vanuit SURF, de MBO Raad en MBO Digitaal. Er is ook een apart netwerk IBP in het po en vo.

ICS

Industrial control system

Industrial control system

Ict-inkoop

Ict-producten en -diensten kun je zelf inkopen, maar dit kost veel tijd, kennis en geld. Je kunt ook gebruik maken van een van de inkoopmogelijkheden van SURF. Vraag en behoefte bij instellingen worden gebundeld en vervolgens wordt op basis daarvan soft- en hardware ingekocht tegen de best mogelijke voorwaarden.

Identificatie

1. Identificatie verwijst in ict-systemen naar het vaststellen van de identiteit van een persoon, vaak door middel van een gebruikersnaam.
2. Identificatie volgens de AVG verwijst naar het vaststellen van de identiteit van een (natuurlijke) persoon.

Identiteit

1. Die eigenschappen of karakteristieken die mensen of objecten uniek maken.
2. Dat wat mensen of objecten uniek identificeerbaar maakt.

Gerelateerde termen:

Identiteitsfederatie
Een samenwerking tussen verschillende organisaties of entiteiten waarbij afspraken zijn gemaakt om gebruikersidentiteiten en toegangsrechten op een gestandaardiseerde en veilige manier te beheren en te delen. Wordt doorgaans aangeboden en beheerd door een 'trusted third party' (in O&O: een NREN).

Gerelateerde termen: SURFconext, eduID, SRAM, GEANT

Identiteitsfraude
Vorm van bedrog waarbij iets of iemand zich voordoet als iemand anders. Bijvoorbeeld spullen huren met de paspoortgegevens van iemand anders. Of iemands inloggegevens gebruiken om in te breken in een systeem.

Gerelateerde termen: Identity theft

Identity broker
Bedrijf dat ervoor zorgt dat een programma of website verschillende manieren van aanmelden aanbiedt aan gebruikers. Bijvoorbeeld aanmelden met een Google-account of via Facebook.

Identity en access management
Algemeen begrip voor twee processen:
- identificatieproces: wie ben je?
- autorisatieproces: wat mag je?

Gerelateerde termen: IAM, SURFconext

Identity provider/OpenID provider
Software waarmee accounts van de organisatie via (open) standaarden gebruikt kunnen worden in een identiteitsfederatie. Gebruikers van deze organisatie kunnen met het account van hun organisatie inloggen op allerlei diensten.

Identity theft
Het misbruiken van iemands persoonsgegevens om zich voor te doen als iemand anders. Zo kan een crimineel bijvoorbeeld iemands geld stelen, spullen kopen op andermans kosten, of criminele handelingen doen uit naam van die persoon.

Gerelateerde termen: Identiteitsfraude

IDS
Intrusion Detection System

Gerelateerde termen: Intrusion detection

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

Gerelateerde termen: Internet of Things

Gerelateerde termen:

Impact

BIV

Bij risicobeoordeling duidt impact op het niet halen van doelstellingen en de mogelijke vervolgschade. Bijvoorbeeld vervolgschade op financien, fysieke veiligheid, gezondheid, sociale veiligheid, reputatie of compliance. In geval van informatierisico's is dat de impact op vertrouwelijkheid, integriteit en beschikbaarheid van informatie.

Incident

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.

Incident response

SURFcert

Reactie op een beveiligingsincident. Het is een (gestructureerde) aanpak op alle niveaus: operationeel, tactisch en strategisch. Incident response kan gezien worden als een soort brandweer; komt meteen in actie als er iets gebeurt.

Indicator of compromise (IoC)

Informatie die je kunt gebruiken om te kijken of iemand een aanval heeft uitgevoerd op één van je systemen. De informatie bevat vaak kenmerken van een aanvaller, van een aanvalsmethode of van malware. Bijvoorbeeld, als je 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, zoals SCADA, DCS's, PLC's. Deze controlesystemen worden in de industrie gebruikt om processen aan te sturen. Bijvoorbeeld een sluis openen of een windmolen uitzetten.

Informatiebeveiliging

SURFaudit

Alle maatregelen om te zorgen dat de juiste informatie beschikbaar is voor de juiste personen. Vaak, maar niet altijd, gaat het om computersystemen. Het gaat om alle 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.

Gerelateerde termen:

Informatiebeveiligingsbeleid
Algemene regels waarmee een organisatie beveiligingsrisico's zo klein mogelijk wil maken. Van tevoren spreek je af hoe groot de beveiligingsrisico's mogen zijn.

Informatiediefstal
Informatie stelen of kopiëren terwijl daarvoor geen toestemming is.

Informatierisico
Onzekerheid of de informatie waarmee je werkt vertrouwelijk, beschikbaar en integer is en blijft.

Information Security Officer (ISO)
Persoon die verantwoordelijk is voor de uitwerking van de informatiebeveiliging van een organisatie. Er zijn verschillende niveau, zoals de CISO (strategisch) of de TISO (technisch).

Chief Information Security Officer

Infrastructuur
In de ict-context bedoelen we hiermee: het geheel van ict-voorzieningen die instellingen nodig hebben voor onderwijs en onderzoek. Denk aan netwerk, computersystemen en beveiliging. De vaak onzichtbare digitale infrastructuur laat mensen op afstand samenwerken en maakt vernieuwend onderzoek en onderwijs mogelijk.

SURFsoc

ISO

Initial access broker
Partij die illegaal toegang tot netwerken verkrijgt en deze toegang aan anderen verkoopt. Deze anderen gebruiken de gekochte toegang bijvoorbeeld voor de uitvoering van ransomware-aanvallen.

Cybercrime-as-a-service

Ransomware affiliate

Initieel risico
De situatie op het eerste moment van registratie van het risico, nog voordat er beheersmaatregelen zijn genomen. Dit wordt ook wel het bruto risico genoemd.

Bruto risico

Inlogcode
Combinatie van gegevens die je nodig hebt om in een computersysteem of een ruimte te komen. Bijvoorbeeld gebruikersnaam en wachtwoord.

Wachtwoord

Gebruikersnaam

Inloggegevens
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Persoons-gegevens

SURFconext

Gerelateerde termen:

Inloggen
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

eduID
Inlogcode
SURFconext

Inlogproces
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

SURFsecureID

Inlooptest
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Mystery guest bezoek

Inputvalidatie
Geldigheidscontrole op invoergegevens. Techniek om onnauwkeurige, incomplete of onlogische invoer te herkennen.

Insider threat
Dreiging van binnenuit 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.

Instellingsaccount
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Account

Integriteit
1. Bij data: juiste en volledige informatie, en verwerking van informatie.
2. Bij personen: de betrouwbaarheid van iemand.

BIV
Classificatie

Intelligence
De kennis waarmee je cyberaanvallen kunt voorkomen of beperken door de dreigingsgegevens te bestuderen en informatie over tegenstanders te verstrekken.

Threat Intelligence
Dreigings-informatie

Internet of Things (IoT)
Apparaten die via het internet verbonden zijn en informatie kunnen uitwisselen. Bijvoorbeeld smartboards, VR-brillen, thermostaten, sensoren en camera's in een smart classroom.

Internet Protocol Security
Standaardafspraken over hoe je netwerkverkeer kan beveiligen. Hiermee kan worden gecontroleerd of informatie in het verkeer niet is aangepast en kunnen anderen de informatie onderweg niet afluisteren.

Gerelateerde termen:

Internetdomeinen

SURFdomeinen

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Internetstandaard

Om wereldwijd gegevens tussen verschillende computers te kunnen uitwisselen, zijn internationale afspraken nodig over de manier waarop de computers met elkaar praten. Zeg maar de digitale 'stekkers en stopcontacten' die alles met elkaar verbinden. Deze afspraken noemen we internetstandaarden of -protocollen. Ze zijn belangrijk om instellingen en diensten veilig te houden. SURF neemt deel aan het Platform Internetstandaarden: kijk op internet.nl voor de meest actuele standaarden.

Intrusion

Een informatiesysteem of computernetwerk binnengaan, of binnendringen, terwijl daar geen toestemming voor is.

Intrusion detection

Het proces waarbij netwerk- of systeemactiviteiten automatisch worden gemonitord om ongeoorloofde toegang, misbruik of afwijkend gedrag te ontdekken en te signaleren.

Intrusion prevention

IPS

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

IoT-apparaten

iotroam

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

iotroam

Met iotroam kun je IoT-apparaten op een veilige en herleidbare manier aansluiten op het netwerk van je eigen instelling. Via de selfserviceportal kunnen studenten, docenten, medewerkers en onderzoekers eenvoudig zelf hun eigen apparaten koppelen.

Gerelateerde termen:

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

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

Intrusion prevention

IPSEC
Internet Protocol Security

Internet Protocol Security

IPv4
Internet Protocol versie 4. IPv4 maakt communicatie mogelijk van data tussen ict-systemen binnen een netwerk, zoals internet. 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 mogelijk, zoals internet. 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.

Information Sharing and Analysis Centre (ISAC)
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.

Information Security Management System (ISMS)
Managementsysteem voor de beveiliging van informatie. Met dit systeem bewaak je het proces van informatiebeveiliging.

Gerelateerde termen:

ISO

1. Information Security Officer
2. Internationale set afspraken en normen voor diverse activiteiten. De internationale afspraken voor informatiebeveiliging is de reeks ISO 2700x.

Chief Information Security Officer

ISO/IEC 27000 serie

Aantal ISO-normen waarin staat hoe een organisatie informatie goed kan beveiligen. In de normen staat hoe een organisatie beveiligingsmaatregelen kan vaststellen, invoeren, uitvoeren, beoordelen en bijhouden. De bedrijfsrisico's bepalen aan welke normen een organisatie wil of moet voldoen. Voorbeelden: ISO 27001 en 27002.

Informatiebeveiliging

J

Jamming

Het verstoren van draadloze signalen, zoals bijvoorbeeld wifi.

K

KAAIWOO (Kontaktgroep Administratieve Automatisering Instellingen)

Kontaktgroep Administratieve Automatisering Instellingen voor Wetenschappelijk Onderwijs (KAAIWO) is een periodiek informeel overleg van functionarissen binnen het wo die verantwoordelijk zijn voor informatievoorziening t.b.v. bestuur en beheer, bestuurlijke informatievoorziening of administratieve automatisering. De nadruk ligt op het op informele wijze, zonder bepaalde bestuurlijke inbedding, uitwisselen van kennis en informatie.

Kans (risico)

De waarschijnlijkheid dat een specifieke gebeurtenis zal plaatsvinden. In cybersecurity bereken je de kans met de formule: dreiging maal kwetsbaarheid.

Kennisnet

Publieke dienstverlener op het gebied van ict met name in het primair, voortgezet en (voortgezet) speciaal onderwijs en op specifieke onderwerpen voor het mbo.

Keylogger

Software die kan bijhouden en vastleggen wat iemand op een toetsenbord typt. Aanvallers gebruiken zo'n programma vaak om wachtwoorden of creditcardgegevens te stelen.

Kill chain

Verschillende fases van een doelgerichte aanval. Vanaf het verkennen van een mogelijk doelwit, het daadwerkelijk binnendringen, het maskeren van de aanval en het realiseren van het uiteindelijke doel.

Klikfraude

Vorm van fraude waarbij geautomatiseerde scripts, bots of personen telkens op advertenties klikken. Waardoor de eigenaar van de website onterecht inkomsten krijgt van de adverteerder.

Gerelateerde termen:

Known unknown

Een bekend risico, dat wil zeggen een risico waarvan we weten dat het bestaat. Er zijn grofweg twee typen bekende risico's. Van sommige bekende risco's weten we 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

Diensten, producten of onderdelen van de infrastructuur van een land die essentieel zijn. Worden deze onderdelen uitgeschakeld of vallen ze uit, dan is de kans op economische of maatschappelijke ontwrichting groot.

Kroonjuwelen

Informatie en informatiesystemen die het allerbelangrijkst zijn voor een organisatie. Het heeft grote gevolgen voor de organisatie als mensen niet meer bij deze informatie kunnen komen wanneer zij dat willen. Of als de informatie niet meer klopt, of ongewild bij anderen terechtkomt. Een voorbeeld van een kroonjuweel is intellectueel eigendom.

Kwantumcomputer

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Quantum-computer

Kwetsbaarhedenscan

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Vulnerability scan

Kwetsbaarheid

Zwakke plekken in digitale systemen, processen en menselijk handelen. In cybersecurity gaat het vaak over een zwakke plek in een digitaal systeem, software of netwerk waardoor een aanvaller in het systeem kan komen. De aanvaller kan zo bij informatie of toepassingen in het systeem komen, terwijl diegene dat niet mag. Of de aanvaller zorgt ervoor dat de gebruiker niet meer bij de informatie kan komen of de toepassing niet meer kan gebruiken.

Lateral movement/ Laterale beweging

Technieken die aanvallers gebruiken om geleidelijk door een netwerk te bewegen. Terwijl ze door het netwerk bewegen, zoeken ze naar informatie met als doel hogere gebruikersrechten te verkrijgen.

Lawful hacking

Het toestaan van hacken door politie en justitie voor opsporingsdoeleinden, onder strikte juridische voorwaarden. Dit kan gaan om het ontsleutelen van versleutelde informatie, het gebruiken van backdoors, het gebruiken van bekende vulnerabilities etc.

Gerelateerde termen:

L

LDAP
Lightweight Directory Access Protocol. Een netwerkprotocol dat beschrijft hoe gegevens uit directoryservices benaderd moeten worden.

Least privilege
Uitgangspunt waarin de gebruiker alleen bij informatie en systemen die nodig zijn voor het uitvoeren van het werk van de gebruiker.

Legacy
Verzamelnaam voor verouderde hardware of software, die niet meer door leveranciers ondersteund wordt.

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.

Links
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

edu.nl

Local Privilege Escalation (LPE)
Uitbreiding van rechten op een computersysteem door een gebruiker of hacker, via een hack of bug in dat systeem.

Location-based services
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

SURFwireless

Log
Een digitaal logboek. Bestand waarin een digitaal systeem automatisch veranderingen en gebeurtenissen bijhoudt.

M2M
Machine-to-machine. Uitwisseling van informatie tussen machines onderling.

Gerelateerde termen:

Machine learning
Ontwikkeling van technieken waarmee computers kunnen leren.

Malvertising
Het verspreiden van malware door die aan te bieden aan een advertentie-bemiddelaar. Zo worden grote groepen gebruikers besmet via een legitieme website.

Malware
Kwaadaardige software die aanvallers op een digitaal systeem zetten, met als doel op afstand toegang te hebben, informatie te stelen of het systeem te vernielen. Malware is een samentrekking van het Engelse malicious software.

Managed security
Het uitbesteden van het beheer, de monitoring en het onderhoud van IT-beveiliging aan een externe partij. Bijvoorbeeld diensten als het beheren van firewalls, inbraakdetectie, antivirus, kwetsbaarheidsscans en respons op incidenten.

Managed Security Service Provider

M

Managed security service provider
Gespecialiseerd bedrijf dat continue beveiligingsdiensten levert aan een klant. Bijvoorbeeld managed firewalls, managed endpoint protection etc.

Managed security

Man-in-the-middle-aanval
Een aanval waarbij een aanvaller zich tussen twee partijen bevindt. De partijen denken direct met elkaar te communiceren. Maar de aanvaller kan informatie afluisteren of wijzigen en hier misbruik van te maken.

Gerelateerde termen:

MBO Digitaal

MBO Digitaal is een platform van de MBO Raad en werkt nauw samen met MBO Voorzieningen, Kennisnet en SURF. Het is een aanspreekpunt voor mbo-scholen en andere (keten)partijen op het gebied van digitalisering en onderwijsvernieuwing.

MDR (Managed Detection & Response)

SURFsoc

Bewaking van digitale infrastructuur door een SOC/SIEM/XDR oplossing. Gecombineerd met een (managed) dienst voor beheer van de oplossing en opvolging van de alarmsignalen die de SOC/SIEM/XDR oplossing doorgeeft..

Meerfactorauthenticatie (MFA)

Authenticatie

Een beveiligingsmethode waarbij gebruikers hun identiteit moeten bewijzen met minimaal twee onafhankelijke factoren, zoals iets wat ze weten (wachtwoord), iets wat ze hebben (tijdelijke code of token), of iets wat ze zijn (vingerafdruk of gezichtsscan). Deze gelaagde beveiliging maakt het voor cybercriminelen veel moeilijker om toegang te krijgen tot systemen en gevoelige informatie.

Meldplicht

Cyber-beveiligingswet
AVG
AP
CSIRT

Wettelijke plicht om een incident te melden aan een toezichthouder of anderen. Verschillende wetten kennen een meldplicht. Het meest bekend is de meldplicht in de AVG, die verplicht een datalek te melden aan de AP. Soms moet er ook gemeld worden an natuurlijke personen van wie de persoonsgegevens betroekken zijn geweest in een incident. Ook de Cyberbeveiligingswet kent een meldplicht voor organisaties die onder de wet vallen, waarbij incidenten boven bepaalde drempelwaarden bij het CSIRT en de toezichthouder gemeld moeten worden.

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-oplossing

Multifactor-authenticatie
SURFsecureID

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Microsoft-token

SURFsecureID

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

MISP (Malware Information Sharing Platform)

SURFcert

MISP is een open source softwareoplossing voor het verzamelen, opslaan, verspreiden en delen van cyberbeveiligingsindicatoren en dreigingen over cyberbeveiliging.

Gerelateerde termen:

Mitigatie
Schade als gevolg van een beveiligingsincident verminderen. Of beveiligingsrisico's verkleinen om zo incidenten te voorkomen.

Risico

Mitigerende maatregel
Een activiteit die als doel heeft de oorzaak of het gevolg van een ongewenste gebeurtenis weg te nemen, of te verkleinen.

Mobile Device Management (MDM)
Het geheel van maatregelen in een organisatie die ervoor zorgen dat mobiele apparaten - zoals smartphones en tablets - goed worden beheerd. Beveiliging hoort daar ook bij, zoals het instellen van een pincode voor apparaten. Of zorgen dat op afstand gegevens op deze apparaten kunnen worden gewist.

MDM

Money mule
Iemand die zijn bankrekening of pinpas uitleent aan criminelen. Criminelen gebruiken de bankrekening om er geld op te laten storten dat ze hebben gestolen door oplichting. Deze persoon wordt ook wel geldezel of katvanger genoemd.

Catfishing

Monitoring
Continu bewaken van een computer of digitaal netwerk, om te controleren of het nog goed werkt.

Security monitoring

MSSP (Managed Security Service Provider)
De MSSP zorgt proactief en continu voor de beveiliging van de IT-omgeving van een klant. Dit ontlast interne IT-teams, betere bescherming door specifieke expertise bij de MSSP en het gebruik van geavanceerde technologieën.

Managed security service provider

SURFcert

Multifactorauthenticatie
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Meerfactor-authenticatie

MFA-oplossing

SURFsecureID

Mystery guest bezoek
Beveiligingstest waarbij een daartoe aangewezen persoon op bezoek gaat bij een organisatie. De mystery guest probeert in ruimtes en bij informatie te komen die niet toegankelijk zouden moeten zijn. Deze test kan gecombineerd worden met een penetratietest. Bij zo'n gecombineerde test gaat de mystery guest een beveiligde technische ruimte in.en probeert in te breken op het lokale computernetwerk.

Penetratietest

Gerelateerde termen:

N

NAT (Network Address Translation)

NAT is een techniek waarmee particuliere IP-adressen binnen een lokaal netwerk omgezet worden in een enkel openbaar IP-adres om te communiceren met het internet. Dit biedt een fundamentele beveiligingslaag door interne IP-adressen te verbergen, waardoor externe partijen de interne netwerkstructuur niet kunnen zien en het moeilijker is om directe aanvallen op individuele apparaten uit te voeren.

NCSC

Nationaal Cyber Security Centrum. Onderdeel van het ministerie van Justitie en Veiligheid. In dit centrum komt alle informatie over cyberveiligheid samen. Het centrum werkt voor de Rijksoverheid en voor processen die het belangrijkst zijn in Nederland. Bijvoorbeeld elektriciteit en toegang tot schoon drinkwater.

NDR

SURFsoc

Network Detection & Response

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.

Nepnieuws

Nieuws dat niet waar is. Het doel van nepnieuws is de mening van de ontvangers beïnvloeden.

Netto risico

Risicomanagement

Een netto (rest) risico is de inschatting van een risico waarbij de huidige aanwezige beheersmaatregelen in beschouwing worden genomen.

Netwerk probe

Netwerksensor

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Gerelateerde termen:

Netwerkbeveiliging
De set van technische maatregelen die wordt genomen om een computernetwerk zo goed mogelijk te beveiligen. Voorbeelden zijn firewalls, endpoint protectie, IDS en IPS.

Intrusion detection
Endpoint protection
Firewall

Netwerksegmentatie
Het verdelen in segmenten van een fysiek computernetwerk in verschillende logische onderdelen die van elkaar afgeschermd kunnen worden. Op elk netwerksegment kunnen verschillende beveiligingsmaatregelen worden toegepast. Zo krijgt een aanvaller die in een bepaald netwerksegment is gekomen, niet automatisch toegang tot andere (kwetsbare) delen in het computernetwerk.

iotroam

Netwerksensor
Systeem dat precies kan aflezen welke informatie via een netwerk wordt verstuurd.. Het systeem kan deze informatie onderzoeken, en uitzoeken of er een probleem is met de beveiliging.

SURFsoc

Netwerktoegangsbeheer
Beveiligingsmaatregel die alleen bekende en geautoriseerde apparaten op een netwerk toelaat.

Network access control
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Netwerk-toegangsbeheer

Network security
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Netwerk-beveiliging

NIB-richtlijn
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Wbni

Niet-persoonsgebonden account (NPA)
Een account dat niet bij een bepaalde persoon hoort. Er zijn 2 soorten:
1. Een non-interactieve NPA wordt gebruikt door systeemfuncties en kan niet gebruikt worden door een eindgebruiker om in te loggen.
2. Een interactieve NPA is vaak een gedeeld account voor bepaalde beheertaken. Meerdere personen kunnen dit account gebruiken.

Gerelateerde termen:

NIS2

De Network and Information Security Directive (NIS2-richtlijn) is vastgesteld door de Europese Unie (EU) en bedoeld om de cyberbeveiliging en weerbaarheid van essentiële diensten in EU-lidstaten te verbeteren. Deze richtlijn wordt vertaald naar de Nederlandse wetgeving in de vorm van de Cyberbeveiligingswet (Cbw).

Cbw

NIST

National Institute of Standards and Technology

NIST-framework

NIST Cybersecurity Framework

Algemene regels van het National Institute for Standards and Technology (NIST) uit de Verenigde Staten. De regels geven aan wat organisaties beter kunnen doen om cyberaanvallen te voorkomen en op te sporen en hoe ze er beter op kunnen reageren. Het is raamwerk met zes stappen: besturen (govern), identificeren (identify), beschermen (protect), detecteren (detect), reageren (respond), herstellen (recover).

NOC

Network Operations Centre. Een of meer plaats of plaatsen van waaruit een netwerk wordt bewaakt en eventueel beheerd. Er vindt controle plaatst op de stabiliteit van de netwerkverbindingen en servers en de hoeveelheid data. Je beheert een netwerk door in te loggen op servers en andere onderdelen van het netwerk. Zo nodig gebeurt dat op afstand.

No-log VPN

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Anonymizing VPN

Non-repudiation

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Onweerlegbaarheid

Non-state actor

De term wordt 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.

Normenkader

Een gestructureerd geheel van afspraken, standaarden, richtlijnen en criteria dat dient als referentie voor het beoordelen van de kwaliteit, veiligheid of effectiviteit van processen, systemen of organisatorische activiteiten. Als je op basis van een normenkader gaat toetsen, wordt het normenkader ingezet als toetsingskader.

Toetsingskader

SURFaudit

Gerelateerde termen:

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

NPG-account
NPA

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Nummerspoofing
Spoofing

Spoofing via SMS of spraakoproep, waarbij de beller van een ander, geïmiteerd nummer lijkt te komen. Het lijkt bijvoorbeeld of iemand via het telefoonnummer van de bank belt, terwijl dat niet zo is.

O

Obfuscation
Iets verhullen om het anderen moeilijk te maken. Beveiligers kunnen bijvoorbeeld systemen of informatie verhullen om het aanvallers moeilijk te maken. Aanvallers verhullen bijvoorbeeld vaak de broncode in hun malware om het beveiligers moeilijk te maken.

Offensieve capaciteiten
Digitale middelen die tot doel hebben het handelen van de tegenstander te beïnvloeden of onmogelijk te maken. Deze capaciteiten kunnen in een militaire operatie worden ingezet ter ondersteuning van conventionele militaire capaciteiten.

Gerelateerde termen:

Onbeveiligde verbindingen

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

eduVPN

Ontsleutelen

Versleutelde informatie leesbaar maken. Bijvoorbeeld een versleuteld tekstbestand of netwerkverkeer. Dit wordt gedaan met één of twee sleutels: symmetrische of asymmetrische versleuteling. De informatie die onleesbaar is gemaakt door de zender, maakt de ontvanger weer leesbaar met behulp van de sleutel(s). Je versleutelt informatie bijvoorbeeld om deze veilig te versturen. Of bijvoorbeeld om vast te stellen dat een bericht ook echt komt van de persoon die zegt dat hij het heeft verstuurd.

Cryptografie
Versleutelen
SURFcertificaten

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 publiek beschikbaar is. Dit in tegenstelling tot de meeste software, die alleen in binaire vorm wordt verspreid. Open source software stelt anderen in staat om de werking te verifiëren en aanpassingen aan de software aan te brengen of voor te stellen. Open source maakt het ook makkelijker om kwetsbaarheden in software te vinden, omdat de broncode hiervoor gelezen kan worden. Nadeel kan zijn dat hierdoor ook kwetsbaarheden ontstaan die niet snel opgemerkt worden.

Broncode

Open source intelligence (OSINT)

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

Intelligence

OpenID Connect (OIDC)

OpenID Connect betekent dat je één sleutel hebt om op veel verschillende internetdiensten in te loggen, zonder steeds verschillende wachtwoorden te moeten onthouden. Het is een manier om Single Sign-on (SSO) mogelijk te maken. Dit is een (open) standaard voor het veilig uitwisselen van authenticatieberichten.

Single Sign On

Operational technology (OT)

Automatisering van een productieomgeving. Bijvoorbeeld robots en machines. Hierbij is het vooral belangrijk dat informatie altijd beschikbaar is en dat de informatie klopt. Deze twee dingen zijn bij operational technology belangrijker dan vertrouwelijkheid.

BIV

Gerelateerde termen:

OSCP
Offensive Security Certified Professional. Diploma voor pentesters. Het examen duurt 24 uur. In deze tijd moet de tester verschillende soorten systemen hacken.

Pentesten

OSI model
Open Systems Interconnection Model. Referentiemodel dat is ontwikkeld vanuit ISO. Het doel van dit model is een open communicatie tussen verschillende technische systemen.

OSINT
Open Source INTelligence

Open source intelligence

OT
Operational Technology of Operations Technology.

Operational technology

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.

OZON
OZON is dé sectorbrede cybercrisisoefening voor onderwijs en onderzoek. Als instelling kun je om de 2 jaar meedoen aan OZON. In het jaar dat OZON niet plaatsvindt, kun je meedoen aan NOZON, een tabletop-cybercrisis-oefening.

crisisoefening

Gerelateerde termen:

P

P2P
Peer-to-peer. Een logisch netwerk van computers die in dit netwerk gelijkwaardig zijn, en diensten aan elkaar kunnen aanbieden.

Packet Capture (PCAP)
Netwerktechniek waarbij datapakketten die over een netwerk reizen worden onderschept en vastgelegd voor analyse. Netwerkbeheerders en -security teams gebruiken deze techniek om de werking en prestaties van een netwerk te begrijpen, problemen te diagnosticeren, beveiligingsdreigingen op te sporen of de naleving van regelgeving te controleren.

Parameter
Een variabele van een bepaald type die kan worden veranderd of 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.

Passkey
Een digitaal certificaat dat wordt gebruikt als authenticatiemethode voor een website of applicatie. Passkeys worden vaak opgeslagen door het besturingssysteem of de webbrowser, en zijn dan beschikbaar op elk apparaat.

Password
Wachtwoord

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Patch
Update

Nieuwe versie van software. In deze nieuwe versie heeft de leverancier kwetsbaarheden in het systeem hersteld. Er zijn geen nieuwe functies toegevoegd.

Patch management
Proces waarbij, indien mogelijk, patches worden geïnstalleerd op een digitaal systeem. Het proces dat zorgt voor het verwerven, testen en installeren van patches (wijzigingen ter opheffing van bekende beveiligingsproblemen in de code) op (verschillende softwarecomponenten van) een computersysteem.

Gerelateerde termen:

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 we geld kunnen pinnen en elektronisch kunnen 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 kaart-houders opslaan, verwerken of versturen. De regels gaan over eisen voor het technische systeem waarin gegevens van de kaarthouder worden opgeslagen. En over eisen voor het verwerken en versturen van deze gegevens.

PEC
Het Privacy Expertise Centrum is een kennisplatform voor en door privacy-professionals in onderwijs en onderzoek. Door kennis te delen, waarborgen we de bescherming van persoonsgegevens en verhogen we de privacy in de sector. (pec.surf.nl)

Penetratietest
Handmatige controle waarbij je via zwakke plekken in het systeem dieper het systeem in probeert te dringen. Het doel is om te testen hoe ver aanvallers het systeem in kunnen komen. De test wordt met toestemming uitgevoerd en vooraf wordt afgesproken hoeveel informatie de pentester heeft over het systeem.

Applicatie securitytest
Vulnerability scan
Blackbox testing

Pentest
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Penetratietest

Persistent Threat
Een langdurige en doelgerichte cyberaanval waarbij een aanvaller langdurig en onopgemerkt toegang krijgt tot een netwerk om gegevens te stelen of het systeem te ontregelen.

Gerelateerde termen:

Persoonsgegevens

Gegevens die verwijzen naar een natuurlijk persoon. Met deze gegevens kun je vaststellen wie iemand is. Bijvoorbeeld naam, adres, nummer van het paspoort. Ook herleidbaar naar een persoon.

SURFconext

PGP

Pretty Good Privacy. Een standaard manier om informatie onleesbaar voor anderen te maken met gebruik van zowel symmetrische als asymmetrische versleuteling. Hierbij worden 2 verschillende formules gebruikt:

1. tekst wordt omgezet in code
2. code wordt weer omgezet in tekst

Cryptografie

Phishing

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

Smishing
Vishing

Phishingkit/ Phishingpanel

Software om phishingwebsites op te zetten en te beheren. De phishingkit biedt doorgaans de phisher mogelijkheden om verschillende neppagina's te beheren en via een beheerderspagina de bezoekers van de phishingwebsite te instrueren. Phishingkits worden tegenwoordig ook aangeboden als een dienst, een vorm van cybercrime-as-a-service.

PIA

Privacy Impact Assessment

Privacy Impact Assessment

PII

Personally Identifiable Information

Persoons-gegevens

PKI

Public key infrastructure

Public key infrastructure
Certificate

PO

Een Privacy Officer (PO) is verantwoordelijk voor het actualiseren en bewaken van het privacybeleid binnen de instelling en het ondersteunen van de uitvoering. PO's waarborgen de naleving van de AVG en het beschermen van persoonsgegevens.

AVG

Gerelateerde termen:

Poortscan
Scan van openstaande poorten op een digitaal systeem. Hiermee wordt inzichtelijk gemaakt welke poorten open staan. 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
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Poortscan

Post-quantum key exchange
Een methode om gedeelde geheime sleutels die bestand zijn tegen aanvallen van toekomstige quantumcomputers uit te wisselen.

Cryptografie
Quantum-computer

Pretexting
Het inzetten van psychologische trucs om iemand persoonlijke, gevoelige informatie te ontfutselen of te manipuleren om bepaalde handelingen te verrichten. Dit wordt gebruikt in social engineering.

Privacy by Default
Zo groot mogelijke privacy garanderen door de standaardinstellingen van een product, dienst of systeem.

AVG

Privacy by Design
Bij het ontwerp van een product, dienst of systeem zoveel mogelijk rekening houden 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. Dit heet dan een Data Privacy Assessment of een gegevensbeschermingseffectbeoordeling.

DPIA

Privacybeleid
Met een privacybeleid brengt een organisatie in kaart welke maatregelen zij heeft genomen om de persoonsgegevens van bijvoorbeeld klanten, patiënten, cliënten te beschermen. Hiermee laat de organisatie ook aan de doelgroep en de Autoriteit Persoonsgegevens zien dat ze voldoet aan de AVG.

Gegevens-bescherming
AP
AVG

Privacy-vriendelijke URL-shortener
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

edu.nl

Gerelateerde termen:

Private key
Sleutel die gebruikt wordt om te versleutelen en ontsleutelen wanneer gebruik gemaakt wordt gemaakt van asymmetrische versleuteling. Het is van belang dat deze sleutel geheim wordt gehouden.

Public key
Versleutelen
Assymetrische versleuteling

Privilege escalation
Aanvalsmethode waarbij de aanvaller de zwakke plekken in een digitaal systeem gebruikt om meer rechten te krijgen in het digitale systeem. Zo komt de aanvaller op plekken waar hij niet zou mogen komen.

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

Profilering
Techniek waarbij je 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.

Provisioning/deprovisioning
Het proces van het toekennen (provisioning) en intrekken (deprovisioning) van toegang en middelen (resources) voor gebruikers binnen een ict-systeem. Dit proces speelt een cruciale rol in het beheer van gebruikersaccounts, rechten en apparaten en draagt bij aan zowel beveiliging als efficiëntie in organisaties.

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.

State-actors
Non-state actors

Proxyserver
Een proxyserver is een computer die als tussenstation dient tussen de gebruiker en de computer waarop de gewenste informatie staat, bereikbaar via het internet. Proxyservers hebben verschillende doelen. Webproxy's bufferen het internetverkeer zodat je verbinding sneller is. Open proxy's verbergen je IP-adres en helpen je online identiteit en locatie deels te verbergen. Reverse proxy's helpen om de toevoer van verkeer vanaf het internet beter te verdelen. Omdat veel spam gebruikt maakt van open proxy's, worden hier vaak beveiligingsmaatregelen op getroffen.

Gerelateerde termen:

Pseudonimisering
Beveiligingsmaatregel waarbij de koppeling tussen gegevens en personen wordt verbroken. De persoonsgegevens worden via een formule vervangen door een code (pseudoniem). De code en de persoonsgegevens worden apart bewaard. Er is altijd na te gaan om welke persoon het gaat.

Public key
Sleutel die gebruikt wordt om te versleutelen en ontsleutelen wanneer gebruik wordt gemaakt van asymmetrische versleuteling. Deze sleutel is openbaar, in tegenstelling tot de private key.

Private key
Versleutelen
Assymetrische versleuteling

Public key infrastructure
Alle rollen, regels en procedures die nodig zijn om verantwoord om te gaan met digitale certificaten. De certificaten worden bijvoorbeeld gebruikt om teksten via asymmetrische versleuteling onleesbaar te maken voor anderen of bij authenticatie.

Assymetrische versleuteling
Public key
Private key
Versleutelen

Purple team/purple teaming
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Adversary simulation

Q

Quadrupel extortion
Aanval waarbij de bestanden of systemen van het slachtoffer zijn versleuteld: de sleutel wordt tegen betaling aangeboden. Voor extra pressie wordt gedreigd geexfiltreerde informatie openbaar te maken. Naast DDoS-aanvallen worden nu ook klanten of aandeelhouders van het slachtoffer direct benaderd.

Quantumcomputer
Computer die informatie opslaat en bewerkt door de eigenschappen te gebruiken van deeltjes die kleiner zijn dan een atoom. De quantumcomputer kan heel veel sneller rekenen dan gewone computers. Hierdoor kan een quantumcomputer bijvoorbeeld gemakkelijk beveiligingscodes kraken en zijn er in de toekomst daardoor nieuwe manieren van beveiliging nodig.

Encryptie

Gerelateerde termen:

Quarantaine

Beveiligingsmaatregel waarbij een apparaat of documenten worden geïsoleerd van andere apparaten of documenten. Dit kan bijvoorbeeld doordat een firewall een apparaat netwerktoegang ontzegt, of doordat securitytooling op een apparaat geïnstrueerd wordt om de netwerktoegang van dat apparaat uit te schakelen of te beperken. Quarantaine wordt toegepast wanneer bijvoorbeeld een malwaredreiging met risico op verspreiding wordt aangetroffen op een apparaat: in afwachting van onderzoek wordt het apparaat in quarantaine geplaatst om verspreiding van de dreiging te voorkomen.

R

Rainbow table

Tabel met mogelijke wachtwoorden en de versleutelde versies van deze wachtwoorden. Je 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-aanval

Random

Iets wat niet te voorspellen is.

Ransomware

Ransomware is een samenvoeging van de woorden ransom (losgeld) en software. De aanvallers gijzelen data van het slachtoffer en voeren zo druk uit om het slachtoffer over te halen te betalen. Die gijzeling bestaat vaak uit het versleutelen van de gegevens van het slachtoffer.

Gijzelsoftware

Quadruple Extortion

Ransomware affiliate

Partij die ransomware-aanvallen uitvoert met ransomware-tooling, die wordt gehuurd van een ransomware operator, waarmee de affiliate een partnerrelatie heeft. Ransomware affiliates maken vaak gebruik van toegang tot netwerken die wordt gekocht bij Initial Access Brokers.

Ransomware operator

Initial access broker

Gerelateerde termen:

Ransomware operator
Partij die ransomware ontwikkelt, en vaak ook een platform onderhoudt waarop gecommuniceerd kan worden tussen slachtoffer en operator voor onderhandelingen en betalingen. Ransomware operators maken vaak gebruik van een 'affiliate program' waardoor andere groepen de daadwerkelijke aanvallen uitvoeren, en de ransomware operator zich beperkt tot het ontwikkelen van de tooling en het platform, en een percentage van ransomwinst opstrijkt.

Ransomware simulation
Gespecialiseerde en gecontroleerde ransomware-oefening.

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 de beperking van het aantal inlogpogingen dat een gebruiker binnen korte tijd kan doen.

RBAC
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Role based access control

Recovery
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Disaster recovery plan (DRP)

Red team/red teaming
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Adversary simulation

Registratieplicht
Organisaties die vallen onder de Cyberbeveiligingswet zijn verplicht zich te registreren in het nationale entiteitenregister. Het doel van de registratieplicht is om de digitale weerbaarheid van de EU te vergroten en om inzicht te krijgen in de digitale infrastructuur.

Cyber-beveiligingswet

Rekendienst
Capaciteit en expertise voor high performance computing, dataverwerking en cloud computing die als diensten aangeboden worden door SURF.

Gerelateerde termen:

Reliability

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Gerelateerde termen: **Betrouwbaarheid**

Remote access

Mogelijkheid om van buitenaf in een computernetwerk te komen. Bijvoorbeeld in een bedrijfsnetwerk, zodat je thuis kunt werken.

Gerelateerde termen: **eduVPN**

Resilience

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Gerelateerde termen: **Cyberweer-baarheid**

Responsible disclosure

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Gerelateerde termen: **Coordinated vulnerability disclosure**

Restrisico

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Gerelateerde termen: **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 niet meer zeker is of gegevens nog kloppen. Bij gevolgen voor de organisatie valt te denken aan financiële schade of het verlies van de goede naam van de organisatie.

Gerelateerde termen: **Dreiging**

Risico (formule)

Dreiging * Kwetsbaarheid * Impact

Gerelateerde termen: **Risico-management**

Risicoacceptatie

Bij risicoacceptatie wordt ervoor gekozen geen aanvullende maatregelen te nemen om de weerbaarheid van de organisatie te verhogen. Acceptatie kan alleen door degene die verantwoordelijk is voor het proces of systeem. Meestal is dit het bestuur of directeur.

Gerelateerde termen:

Risicoanalyse
Methode om inzicht te krijgen in de risico's die je loopt. De proces- of systeemeigenaar kijkt daarbij onder andere naar het volgende: onzekerheden, oorzaken, gevolgen, kans, gebeurtenissen, scenario's, beheersmaatregelen en hun effect.

Risicoassessment
Een proces in 3 stappen waarin risico's worden:
- geidentificeerd (vinden en beschrijven van risico's),
- geanalyseerd (waarbij wordt nagedacht over onzekerheden, oorzaken, gevolgen, kans, gebeurtenissen, scenario's, beheersmaatregelen en hun effect)
- en geevalueerd (het beslismoment wat je verder nog met de risco's wil doen).

Risicobeheersing
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Risico-management

Risicobereidheid
De hoeveelheid en het soort risico dat een organisatie bereid is na te streven, te behouden of te nemen.

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.

Risico-identificatie
Het vinden en beschrijven van risico's.

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

Risicomanagement
Een continu proces waarbij bedrijfsrisico's voortdurend worden bewaakt. Onderdelen van dit proces zijn bijvoorbeeld het identificeren, evalueren, prioriteren van risico's en het nemen van maatregelen (accepteren, mitigeren, overdragen of vermijden).

Bedrijfsrisico
Risicoanalyse
Mitigerende maatregel
SURFaudit

Gerelateerde termen:

Risicomitigatie

maatregelen die een organisatie neemt om risico's te verkleinen of helemaal te laten verdwijnen. Grijpt een organisatie in, dan kan dat twee doelen hebben:

1. De kans op een incident verkleinen.
2. De gevolgen verkleinen als dat incident toch plaatsvindt.

Risiconiveau

Risicoprofiel

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

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 de kans en de gevolgen.

Risk appetite

Risicobereidheid

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Role based access control

Bepalen of een gebruiker bij een computersysteem mag komen. Daarbij wordt gekeken 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 aanvaller gebruikt als deze 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 wordt bepaald welke patronen of tekens in data op een netwerk verdacht kunnen zijn. Daarna zoekt het systeem naar deze patronen of tekens.

S

S/MIME
Secure/Multipurpose Internet Mail Extensions. Techniek waarbij e-mails worden omgezet in code met een openbare sleutel en een privésleutel. De openbare sleutel deel je met elkaar via een certificaat.

SAML
Security Assertion Markup Language; een (open) standaard voor het veilig uitwisselen van authenticatieberichten gebaseerd op XML/SOAP.

Sandbox
Afgeschermd deel in een digitaal systeem. Sandboxes worden vaak gebruikt om software te testen, of om mogelijk schadelijke software te testen. Software die in de sandbox gebruikt wordt, kan geen andere processen in de computer verstoren.

SAST
Static Application Security Testing; een techniek waarmee je automatisch zwakke plekken in een broncode kan controleren.

SBoM (Software Bills of Materials)
Lijst van alle softwarecomponenten in software of een computersysteem, met informatie over de versies, licenties en beveiliging.

SCA
Gerelateerde termen: SAST

Software Composition Analysis waarbij een inventaris wordt gemaakt van de verschillende componenten in de software. Bijvoorbeeld welke Open Source componenten er in zitten, en welke versies er gebruikt worden. Dit helpt om kwetsbaarheden op te sporen en de beveiliging en compliance te verhogen. SCA is een doorontwikkeling van Static Application Security Testing (SAST) waarbij alleen de broncode wordt geanalyseerd.

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

Gerelateerde termen:

Schaduw IT

Shadow IT

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

SCIM

System for Cross-domain Identity Management - specificatie om het beheer van identiteiten over verschillende (cloud) omgevingen heen eenvoudiger te maken. Wordt doorgaans gebruikt voor het (de)provisionen van gebruikers.

SCIPR

Informatiebeveiligers en privacyofficers van onderwijs- en onderzoeksinstellingen werken samen in SCIPR (SURF Community voor Informatiebeveiliging en PRivacy). Het is een community of practice en helpt informatiebeveiliging verder te professionaliseren bij instellingen. De community stelt met elkaar onder andere beleid op.

SCIRT

Technisch, operationele securityspecialisten van onderwijs- en onderzoeksinstellingen kunnen terecht bij SCIRT, de SURF Community van Incident Response Teams. Operationele security-experts bespreken in SCIRT actuele security-uitdagingen en wisselen de laatste tips & trucs uit met vakgenoten.

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.

Scriptkiddie

Iemand die cyberaanvallen doet voor de lol of om te 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.

Gerelateerde termen:

Scrubbing

Gegevens filteren die naar een systeem gaan. Het doel is onder andere om te zorgen dat DDoS-aanvallen niet succesvol kunnen zijn of om DDoS-aanvallen onschadelijk te maken.

SEC

Het SURF Security Expertise Centrum (SEC). Dit is de plek waar instellingen informatie en expertise vinden, en ondersteuning krijgen om zich te beschermen tegen cybersecuritydreigingen en -aanvallen, hun cyberweerbaarheid te versterken en hun cybersecurityvolwassenheid te vergroten. (sec.surf.nl)

Sectoraal CSIRT

Cbw
CERT

Voor organisaties die onder de Cyberbeveiligingswet vallen is er een toegewezen sectoraal CSIRT. Hieraan moeten incidenten gemeld worden en het CSIRT levert bijstand. SURFcert is het sectoraal CSIRT vinstellingen die door OCW zijn aangewezen in het kader van de Cbw.

Secure coding

Een gestructureerde aanpak om software te ontwikkelen, met als doel software te maken die minder beveiligingslekken bevat.

Secure development lifecycle

Een proces waarin je 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 proces ontwikkeld in 2002. Verschillende organisaties gebruiken nu SDL, of 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 vinden we met elkaar dat dit model niet meer veilig is en er is een opvolger: Transport Layer Security (TLS).

Security

Beveiliging

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Gerelateerde termen:

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. Zo'n bericht wordt vaak gemaakt als de zwakke plekken in de lijst staan met 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

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Bewustzijn
Awareness training

Security by default

De aanduiding, dat de maker of leverancier van een product ervoor zorgt, dat het 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 dat product koopt of in gebruikt neemt, is dan helemaal zelf verantwoordelijk om dit 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)

Een systeem waarin je informatie uit computersystemen verzamelt en analyseert. Het doel is om verdacht gedrag te ontdekken. Om zien dat iemand dingen in het systeem heeft veranderd, terwijl hij dat niet mocht.

Security monitoring

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

Security operations center (SOC)

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

Security-monitoring
SURFsoc

Security rating

De score die aangeeft hoe goed een persoon, netwerk of computer is beveiligd. Deze score wordt vaak automatisch berekend en helpt organisaties om te weten waar risico's zijn.

Gerelateerde termen:

Security scan
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Vulnerability scan

Security through obscurity
Een digitaal systeem beveiligen door de beveiligingsmaatregelen geheim te houden. Het idee is, dat iemand van buiten de organisatie moeilijker kan inbreken, als diegene niet weet hoe het systeem is beveiligd. Dit wordt over het algemeen niet gezien als een goede beveiligingsmethodiek.

Obfuscation

Securityrisico
Combinatie van kwetsbaarheden en dreigingen die een risico vormen voor de Beschikbaarheid, Integriteit of Vertrouwelijkheid (BIV) van informatie.

Securitystandaarden
Standaarden voor veiligheid die belangrijk zijn binnen cybersecurity, bijvoorbeeld over wat te doen om informatie te beveiligen. Voorbeelden zijn: ISO 2700x, NEN 7510, BIO, SOC1-2-3, ISAE3402, NIST-CSF en PCI-DSS.

Securitytest
Een algemene naam voor testen die zijn bedoeld om zwakke plekken in een systeem te vinden. Geautomatiseerde scans horen hier niet bij.

Segmentering
Een netwerk opdelen in kleinere beheersbare segmenten. Hierdoor kunnen organisaties gevoelige informatie beter beschermen.

Segregation of duties (SoD)
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Functiescheiding

Self-assessment
Een vorm van auditen waarbij je als instelling zelf onderzoekt of toetst of je aan een bepaald kader voldoet.

Assessment
Toetsingskader
Toetsingskader Informatie-beveiliging
SURFaudit

Service-account
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

NPA

Gerelateerde termen:

Serviceprovider/Relying party

Software waarmee aanbieders van applicaties, diensten en/of resources het authenticeren van gebruikers kunnen 'uitbesteden' aan identity- of OpenID-providers, via een identiteitsfederatie. Hierdoor hoeven deze aanbieders zelf geen wachtwoorden meer op te slaan.

Severity

Hoe ernstig een zwakke plek van een digitaal systeem is.

Sextortion

Deepfakes

Sextortion is iemand chanteren met naaktbeelden. Dit wordt ook wel afpersing genoemd. Het gaat bijvoorbeeld om naaktfoto's of video's die van iemand zijn gemaakt met een webcam. Het kan ook gaan om nepfoto's of nepvideo's.

Shadow IT

Shadow IT is hardware of software binnen een onderneming, die niet ondersteund wordt en niet opgezet is door de ict-afdeling, maar wel een rol speelt in de bedrijfsvoering.

Shell

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

Shodan

Een zoekmachine voor alle systemen die op het internet zijn aangesloten.

Shouldersurfing (schoudersurfen)

Social engineering

Meekijken over de schouder van een gebruiker van een digitaal systeem om informatie te verkrijgen, met als doel de gegevens te misbruiken.

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

Gerelateerde termen:

SIEM-systeem

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

SURFsoc

SIGINT

Signal Intelligence: het verzamelen van informatie door signalen van elektronische communicatiekanalen op te vangen.n.

Signature

1. Een specifiek patroon waaraan of waarmee je een cyberaanval kan herkennen.
2. Een digitale handtekening

Signature based detection

Een techniek waarmee je aanvallen opspoort met hulp van vooraf afgesproken patronen, instructieregels of tekens.

Signing

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Digitale handtekening

Sim-swapping

Het proces waarbij een kwaadwillende de telecomprovider van het slachtoffer overtuigt een 06-nummer over te zetten naar een simkaart die in diens bezit is.

Single extortion

Aanval waarbij bestanden of systemen van het slachtoffer zijn versleuteld; de sleutel wordt tegen betaling aangeboden.

Triple extortion
Double extortion
Quadrupel extortion

Single sign-on (SSO)

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.

SURFconext

Situation awareness

Overzicht van de (relevante) informatie en elementen binnen een ecosysteem, deze begrijpen en inzicht in hoe een situatie zich zal ontwikkelingen zodat je goede beslissingen kan maken over risico's en dreigingen.

Gerelateerde termen:

SIVON
SIVON is de ict-coöperatie van en voor het primair onderwijs en voortgezet onderwijs. Samen met partners en in constant overlegmet de markt, behartigen zij vanuit publieke waarden het belang van hun leden.

Ict-inkoop

Skimmen
De gegevens van een bankpas of creditcard illegaal kopiëren. Als de eigenaar met de pas betaalt of geld pint, kopieert de crimineel de magneetstrip.

Smishing
Vorm van phishing waarbij het phisingbericht per sms verstuurd wordt.

Phishing

Snellius
Snellius is de Nationale Supercomputer beheerd door SURF. Onderzoekers kunnen gebruik maken van Snellius bij omvangrijke of complexe experimenten, zoals simulaties en modelleringen. Een belangrijk kenmerk van Snellius is het snelle interne netwerk.

Supercomputer

Sniffen
Afluisteren en analyseren van ie informatie die in een computernetwerk rondgaat.

Cryptografie

SO
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Information Security Officer (ISO)

SOAR
Security orchestration, automation and response. Het stelt organisaties in staat om beveiligingswerkzaamheden op drie belangrijke gebieden te stroomlijnen:
- Threat en vulnerability management
- Incident response
- Automatisering van beveiligingswerkzaamheden.

Dankzij SOAR kunnen organisaties zelf gecoördineerd en geautomatiseerd beveiligingstaken laten uitvoeren.

SOC
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

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.

Gerelateerde termen:

Source code
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Broncode

Spam
Spam is een bericht dat je ongevraagd ontvangt. Bijvoorbeeld via e-mail, mobiele telefoon of vaste telefoon.

Spam- en virusfilter
Een computerprogramma dat e-mailberichten analyseert en bepaalt of er sprake is van spam of virussen. De e-mail kan vervolgens automatisch direct of na een bepaalde tijd worden verwijderd.

Spearphishing
Een phishingaanval die gericht is op een bepaald persoon. Soms is de aanval ook speciaal aangepast voor deze persoon. Daardoor 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 echte e-mails van phishingmails of spam kunnen onderscheiden.

DNS

Spoofing
Iemand misleiden door te doen alsof je iemand anders bent. Er zijn veel soorten spoofing. Een aanvaller kan zich in een e-mail 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.

SRAM
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

SURF Research Access Management

SSL
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Secure Sockets Layer

Gerelateerde termen:

SSO
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Single sign on

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

Cybersabotage

State-sponsored attack
Cyberaanval die door een staat wordt gefinancierd of op een andere manier ondersteund.

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

Storing
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Uitval

Supercomputer
De term supercomputer wordt gebruikt voor systemen die tenminste 10.000 tot 100.000 keer sneller zijn dan een gewone pc. Met de rekencapaciteit van een supercomputer is het mogelijk om complexe problemen op te lossen op het gebied van wetenschappelijk onderzoek en technologische ontwikkeling.

Snellius
HPC

Supply chain attack
Bij een supplychain-aanval valt een aanvaller een organisatie niet rechtstreeks aan, maar via één van de leveranciers. Hierdoor is het mogelijk om organisaties die zelf een goede beveiliging hebben, toch succesvol aan te vallen.

SURF Research Access Management
SURF Research Access Management (SRAM) is een platform waar je als instelling toegang tot onderzoeksdiensten delegeert aan onderzoekers. Deze dienst is ontwikkeld op basis van bestaande en bewezen internationale afspraken voor autorisatie en authenticatie binnen onderwijs en onderzoek.

SURF Research Cloud
SURF Research Cloud is een portaal waarin je eenvoudig een virtuele onderzoeksomgeving bouwt.

Virtuele onderzoeksomgeving

Gerelateerde termen:

SURF Security & Privacy Conferentie

Tweedaagse conferentie voor security- en privacyprofessionals in het mbo, hbo en wo. Mede georganiseerd door de beveiligingscommunity's SCIPR & SCIRT.

SCIPR
SCIRT

SURF Summit

Jaarlijks evenement voor bestuurders en beslissers van SURF-leden waar digitalisering en innovatie op strategisch niveau op de agenda staan.

SURF Vendor Compliance

Dienst die namens instellingen gezamenlijk privacy- en securityrisicoanalyses uitvoert op leveranciers.

DPIA
DTIA

SURFaudit

Met SURFaudit krijg je inzicht in en overzicht van je governance, risk en compliance (GRC). Het bestaat uit een toetsingskader, benchmark, GRC-applicatie, dreigingsbeeld, en toolkit voor risicomanagement.

Toetsingskader
Informatie-beveiliging
Privacy

SURFcert

SURFcert is het CERT (Computer Emergency Response Team) voor de onderwijs en onderzoekssector. Het biedt 24 uur per dag, 7 dagen per week ondersteuning bij beveiligingsincidenten. Ook biedt SURFcert diverse security-oplossingen waarmee instellingen de beveiliging kunnen optimaliseren.

CERT

SURFcertificaten

Via SURF kunnen instellingen tegen relatief lage kosten digitale certificaten aanvragen. Certificaten zijn belangrijk voor een goede ict-beveiliging van je instelling: ze versleutelen informatie en kunnen e-mail, documenten en/of software van een digitale handtekening voorzien. Ook kun je ze gebruiken voor authenticatie.

Certificaten

SURFconext

Met SURFconext kunnen gebruikers met één gebruikersnaam en wachtwoord inloggen bij alle clouddiensten die een instelling gebruikt. Dat geldt voor zowel diensten die iedereen gebruikt als diensten voor kleine specialistische teams. Veilig, makkelijk en privacyvriendelijk.

SURFcumulus

Met SURFcumulus kies je uit verschillende cloudaanbieders van binnen en buiten Europa voor gebruik bij jouw onderwijs-of onderzoeksinstelling.

Gerelateerde termen:

SURFdomeinen
Als ict-beheerder in onderwijs- en onderzoek registreer en verhuis je internetdomeinen gemakkelijk via SURFdomeinen. Ook het beheer van het DNS gaat eenvoudig, via de online portal.

SURFdrive
SURFdrive is een persoonlijke cloudopslagdienst voor het Nederlandse hoger onderwijs en onderzoek, waarmee medewerkers, onderzoekers en studenten gemakkelijk bestanden kunnen opslaan, synchroniseren en delen.

Onderzoeks-(data)

SURFfilesender
Met SURFfilesender verstuur je veilig grote bestanden, zoals onderzoeksdata. De bestanden zijn in Nederland opgeslagen en voorzien van versleuteling. SURFfilesender is te gebruiken door medewerkers en studenten van onderwijs- en onderzoeksinstellingen.

Onderzoeks-(data)

SURFfirewall
SURFfirewall neemt aanbesteding en beheer van de firewall uit handen voor onderwijs- en onderzoeksinstellingen. Voor een vast tarief per maand krijg je een firewall die SURF beheert en schaalbaar is in capaciteit en functionaliteit.

Firewall

SURF-netwerk
Het SURF-netwerk is een landelijk glasvezelnetwerk voor het onderzoek en onderwijs in Nederland. Het biedt snelle en goed beveiligde connectiviteit met het internet, en daarnaast tal van specifieke diensten.

SURFsecureID
SURFsecureID is de centrale dienst voor MFA bij instellingen. SURFsecure-ID voegt aan het inloggen een extra stap toe: de gebruiker logt in met een gebruikersnaam, wachtwoord én een tweede factor, zoals bijvoorbeeld een mobiele app (zoals Tiqr).

SURFconext
MFA

SURFsoc
SURFsoc monitort, onder andere via een SIEM-systeem, cyberdreigingen en mogelijke aanvallen op de infrastructuur van instellingen. Zo wordt de detectiecapaciteit van instellingen vergroot.

SIEM
SOC

SURFwireless
SURFwireless helpt instellingen met het aanleggen en onderhouden van een veilig en betrouwbaar wifi-netwerk.

Gerelateerde termen:

Swag
Goodies die hackers krijgen om ze te bedanken voor hun gratis hulp om een informatiesysteem te beveiligen. T-shirt met de tekst 'I hacked (...) and all I got was this lousy T-shirt'.

Symmetrische versleuteling
Informatie - zoals een tekstbestand of netwerkverkeer - beveiligen met een sleutel. Dit wordt gedaan met één sleutel, in tegenstelling tot asymmetrische versleuteling waarbij twee sleutels worden gebruikt. De ontvanger en verzender hebben dus allebei dezelfde sleutel. De informatie wordt onleesbaar gemaakt door de zender waarna de ontvanger deze weer leesbaar maakt, beide dus met dezelfde sleutel. Ze moeten deze sleutel op een vertrouwelijke manier met elkaar delen (bijvoorbeeld met behulp van asymmetrische versleuteling).

Versleutelen
Cryptografie
Public Key

T

Tabletop-cybercrisisoefening
In een tabletop-crisisoefening doorloop je met je team de crisisplannen en de onderlinge afstemming aan de hand van een fictief scenario. Dit is relatief rustig omdat het geen crisissimulatie is.

(N)OZON

Tailgating
Een techniek die social engineers gebruiken om ongeautoriseerd toegang te krijgen tot een beveiligde ruimte.

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 je testen kan doen. In het Nederlands noemen we dit een experimenteeromgeving of proeftuin.

MFA

Gerelateerde termen:

Threat
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Dreiging

Threat actor
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Actor

Threat hunting
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Hunting

Threat intell
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Threat intelligence

Threat intelligence
Verzamelde, verrijkte en geanalyseerde informatie over dreigingen in het digitale domein, die als doel heeft deze dreigingen tijdig te identificeren en de weerbaarheid van de ontvangers te verhogen.

Dreigings-informatie

Threat management
Een aanpak om bekende en onbekende dreigingen op te sporen en tegen te gaan. Hierbij gebruik je een combinatie van opsporingstechnieken.

Threat modeling
Een methode om zwakheden in computersystemen snel te herkennen, zodat hierop kan worden ingespeeld.

Timebox
Een vaste tijd waarin je bepaalde geplande activiteiten uitvoert. Is de tijd om, dan stopt het. Ook als de activiteiten nog niet klaar zijn.

Tiqr
Een open source smartphone-app die kan worden gebruikt voor multifactorauthenticatie.

TLP
Traffic Light Protocol. Dit is een methode, ontwikkeld door first.org, om data of informatie in te delen in klasses. Hoe je dit indeelt, hangt af van met wie je de informatie mag delen. De klasses zijn rood, oranje, groen en wit en de bijbehorende kleurcoderingen zijn TLP:RED, TLP:AMBER, TLP:GREEN en TLP:CLEAR. Kijk voor meer informatie op www.first.org/tlp/docs/v2/tlp-v2-nl.pdf

SCIRT

Gerelateerde termen:

TLS
Transport Layer Security

Transport Layer Security

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

Authenticatie

Toetsingskader
Een toetsingskader beschrijft wat de vereisten zijn om aan een bepaald volwassenheidsniveau te voldoen en vormen de basis van de self-assessments en (externe) audits.

Volwassen-heidsniveau
SURFaudit
Toetsingskader Informatie-beveiliging

Toetsingskader Informatiebeveiliging
Het SURFaudit Toetsingskader informatiebeveiliging beschrijft wat de vereisten zijn om aan een bepaald volwassenheidsniveau te voldoen en vormen de basis van de self-assessment en (externe) audits.

SURFaudit
Toetsingskader

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

Tokenisatie
Het proces waarbij je een document met kwetsbare gegevens vervangt door andere gegevens die minder kwetsbaar zijn. Zo kun je bijvoorbeeld privacy beter garanderen.

TOR (The Onion Router)
Een open netwerk om anoniemer op het internet te surfen. TOR biedt ook toegang tot het darkweb.

Darkweb

TPM
1. Third Party Memorandum/Mededeling. Verklaring van een onafhankelijk onderzoeksbureau waarin staat hoe goed de ict-dienstverlening en ict-kennis van een organisatie zijn.
2. Trusted Platform Module. Internationale standaardeisen voor een veilige cryptoprocessor. De TPM is ontworpen om hardware te gebruiken in het beveiligen van sleutels en cijfercodes. Dit security model zorgt ervoor dat de sleutels niet gestolen kunnen worden.

Traceback
Het proces om iets terug te voeren naar de bron.

Gerelateerde termen:

Tracken

Tracking is het verzamelen en analyseren van gegevens over de online activiteiten van individuen. Dit kan variëren van het volgen van websitebezoeken en klikgedrag tot interacties op sociale media. Dit staat op gespannen voet met privacy en security.

Gerelateerde termen: edu.nl

TRANSITS

Training voor incidentmanagement, grotendeels gemaakt met expertise vanuit de onderwijs- en onderzoeksector. SURF organiseert dit binnen Nederland.

Transport Layer Security (TLS)

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

Gerelateerde termen: Cryptografie, Authenticatie, SSL

Triple extortion

Bestanden of systemen van het slachtoffer zijn versleuteld; de sleutel wordt tegen betaling aangeboden. Voor extra pressie wordt gedreigd geëxfiltreerde informatie te openbaren. Hieraan worden ook nog eens DDoS-aanvallen toegevoegd.

Gerelateerde termen: Single extortion, Double extortion, Quadrupel extortion

Trojan

Type kwaadaardige software waarmee een aanvaller via een geheime ingang in een systeem kan komen. Vaak is deze verhuld in software die een gebruiker graag wil hebben en zelf installeert. Ook wel Trojan horse (paard van Troje).

Gerelateerde termen: Malware

True negative

De situatie dat een beveiligingssysteem niets opmerkt en er is daadwerkelijk niks aan de hand.

Gerelateerde termen: False negative

True positive

De situatie dat een beveiligingssysteem opmerkt dat er iets aan de hand is en er inderdaad sprake is van een aanval of afwijking.

Gerelateerde termen: False positive

Trust framework

Een verzameling partijen (deelnemers aan een identiteitsfederatie) die een zelfde set afspraken onderschrijven. Hierdoor ontstaat onderling vertrouwen.

Trusted third party

Een onafhankelijke partij die ondersteunt bij de uitwisseling van privacy-gevoelige informatie tussen partijen.

Gerelateerde termen: TPM

Gerelateerde termen:

TTP
Tactics, Techniques and Procedures: tactieken, technieken en processen die een aanvaller gebruikt. TTP's worden gebruikt om de manier van werken van aanvallers te bepalen. Een Red teamoefening is hier een voorbeeld van.

Adversary simulation

Tweestapsauthenticatie
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Meerfactor-authenticatie

Two-factor authentication
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Meerfactor-authenticatie

Typosquatting
Een vorm van misbruik van het internet. Hier wordt misbruik gemaakt van de situatie dat mensen kleine fouten in een URL vaak niet zien. Bijvoorbeeld het gebruik van een domeinnaam, die maar 1 letter verschilt van de domeinnaam van de website die de bezoeker wil bezoeken.

U

U-CISO
Overleg waar alle CISO's van de universiteiten in zijn vertegenwoordigd.

Uitval
De situatie waarin gebruikers niet meer in een digitaal systeem kunnen werken.

Universiteit van Harderwijk
Fictieve universiteit die regelmatig wordt ingezet bij diverse oefeningen.

OZON

Gerelateerde termen:

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

UNL
Universiteiten van Nederland is de kbrancheorganisatie van de veertien publieke universiteiten van Nederland. De leden van deze vereniging zijn drie bijzondere universiteiten, tien bekostigde, en de Open Universiteit.

Update
Patch

Aanpassing van een bestaande versie van hard- of software. Deze repareert bekende zwakke plekken en zorgt eventueel voor nieuwe beveiliging en extra functies.

Upgrade
Nieuwe (geactualiseerde) versie van software, hardware of firmware.

URL-shortening
edu.nl

Verkorten van de URL-link om het makkelijker te gebruiken. Met een URL-shortener kun je voor lange URLs een korte link aanmaken. Daarbij wordt de oorspronkelijke URL minder zichtbaar en dit kan een beveiligingsrisico met zich meebrengen. Zo kan een (kwaadaardige) link worden verhuld door een verkorte link.

USB-sleutel
SURFsecureID

Een USB-drive die wordt gebruikt om een gebruiker te identificeren en te authenticeren.

Username
Gebruikersnaam

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

V

Gerelateerde termen:

Versleutelen
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Cryptografie
Ontsleutelen
SURFcertificaten

Vertrouwelijkheid
Vertrouwelijke informatie is niet voor iedereen toegankelijk. Alleen geautoriseerde personen hebben toegang tot vertrouwelijke informatie. Vertrouwelijkheid is één van de kwaliteitskenmerken van gegevens. Persoonsgegevens zijn bijvoorbeeld vertrouwelijke gegevens.

BIV
Autorisatie

Verwerker (processor)
De partij die (als leverancier) persoonsgegevens verwerkt in opdracht en ten behoeve van de verwerkingsverantwoordelijke (diens klant).

Verwerkersovereenkomst
Een verwerkersovereenkomst regelt de afspraken bij de verwerking van persoonsgegevens tussen verwerker en de verwerkingsverantwoordelijke.

Verwerkingsverantwoordelijke (controller)
Degene die het doel en de middelen van de verwerking van persoonsgegevens bepaalt en opdracht geeft voor de verwerking.

VH
Vereniging Hogescholen is de brancheorganisatie van het hbo in Nederland. Alle bekostigde hogescholen in Nederland zijn lid van deze vereniging. Vereniging Hogescholen zet zich in voor goed onderwijs en onderzoek. Zij doen dit door in gesprek te gaan met de overheid en maatschappelijke organisaties.

Virtual machine (VM)
Virtual machine, een computer binnen een computer.

Virtual private network (VPN)

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.

Virtual private server (VPS)

Een virtuele machine die als dienst wordt verkocht door een hostingpartij. Dit wordt ook wel een virtual dedicated server genoemd. Een VPS wordt doorgaans aangeboden met een geïnstalleerde kopie van een besturingssysteem, zoals Windows of Linux. Daarbij krijg je een account met systeemrechten op de VPS, zodat je kunt inloggen op de VPS. Een VPS vertoont veel overeenkomsten met een fysieke server met het belangrijkste verschil dat de onderdelen van de VPS virtueel (softwarematig) zijn en daardoor makkelijker aan te passen. Een VPS is daardoor vele malen goedkoper dan een fysieke server.

Virtuele onderzoeksomgeving

SURF Research Cloud

De virtuele onderzoeksomgeving is een virtuele werkomgeving in de cloud waar onderzoekers makkelijk en veilig kunnen samenwerken aan data-analyse.

Virus

Malware

Een computervirus of virus is een vorm van schadelijke software (malware). Virussen worden vaak verspreid via bijlagen in e-mail. Deze schadelijke software wordt op een computersysteem gezet met als doel het systeem uit te schakelen, te beschadigen of gegevens te stelen. Het virus wordt zo ontworpen dat het zichzelf probeert te verspreiden naar andere digitale systemen.

Vishing

Voicephishing

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Vitale infrastructuur

Kritieke infrastructuur

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

VM

Virtual machine

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Voicephishing

Phishing

Vorm van phishing waarbij een aanvaller belt met een gebruiker om vertrouwelijke informatie te krijgen, om vervolgens met deze informatie te proberen in een digitaal systeem te komen.

Gerelateerde termen:

Volwassenheidsniveau

Het volwassenheidsniveau van informatiebeveiliging geeft aan hoe gestructureerd en effectief een organisatie omgaat met digitale veiligheid. Een hoger volwassenheidsniveau voor informatiebeveiliging betekent een meer volwassen, proactieve en weerbare organisatie.

SURFaudit
Toetsingskader Informatiebeveiliging

VPN

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Virtual private network

VPS

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Virtual private server

Vriend-in-nood-fraude

Vorm van oplichting waarbij het slachtoffer denkt een bekende (vaak zoon of dochter) te helpen met een betaling.

WhatsApp-fraude

Vrijwaringsverklaring

Verklaring waarin men toestemming geeft een beveiligingsonderzoek te doen waarbij de onderzoeker gevrijwaard wordt van schade die hij mogelijk veroorzaakt. Er staat ook in waar het onderzoek aan moet voldoen. Deze verklaring gebruikt men bijvoorbeeld voor een penetratietest.

Vulnerability

Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Kwetsbaarheid

Vulnerability assessment

Handmatige controle waarbij je zwakke plekken in een systeem opspoort. Vooraf bepaal je hoe je dat doet. Bij een vulnerability assessment probeer je alle zwakke plekken te vinden in een klein gebied. Dat is anders dan bij een penetratietest waarbij je zo diep mogelijk in een systeem wil komen.

Vulnerability management

Het geheel van maatregelen die een organisatie uitvoert om zwakke plekken in de eigen digitale systemen op te sporen en te herstellen.

Vulnerability scan

Een geautomatiseerde scan die zwakke plekken in een systeem opspoort.

Gerelateerde termen:

W

Wachtwoord

Reeks van letters, cijfers 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

Wachtwoordkluis

Een wachtwoordmanager slaat al jouw wachtwoorden op in een veilige wachtwoordkluis.

Wachtwoord-manager

Wachtwoordmanager

Software waarin een gebruiker combinaties van wachtwoorden en gebruikersnamen kan opslaan, in een soort digitale kluis. Vaak kan de software ook zelf wachtwoorden aanmaken, websites herkennen en automatisch invullen. Ook geeft de wachtwoordmanager vaak aan of een wachtwoord sterk genoeg is, en of je het al eerder hebt gebruikt.

WYAF (Where You Are From)

Een pagina waarop gebruikers selecteren van welke instelling (identity provider) zij zijn. Wordt gebruikt binnen een federatieve authenticatie- en autorisatieinfrastructuur.

Authenticatie

SURFconext

Wbni

De Wet beveiliging netwerk- en informatiesystemen is een Nederlandse wet die bepaalt aan welke eisen aanbieders van essentiële diensten (AED's) en digitale diensten (DSP's) moeten voldoen. Deze wet voert uit wat er staat in de Europese Netwerk- en Informatiebeveiligingsrichtlijn (NIB). De wet Wbni wordt vervangen door de Cyberbeveiligingswet (Cbw).

Cyber-beveiligingswet

Webbrowser

Een browser is een programma dat het mogelijk maakt om websites op internet te bezoeken.

SURFfilesender

Gerelateerde termen:

Wetenschappelijk Technische Raad
De Wetenschappelijk Technische Raad (WTR) adviseert de coöperatie SURF, gevraagd en ongevraagd, over strategische, wetenschappelijke en technische kwesties van de coöperatie.

Whaling
Manier om vertrouwelijke informatie (zoals persoonlijke data van werknemers) of geld van een organisatie te stelen. Meestal gebeurt dit door een valse e-mail te sturen uit naam van iemand die de werknemer vertrouwt. Via deze e-mail wordt de werknemer verleid om bedrijfsgegevens te onthullen of een grote betaling te autoriseren.

Gerelateerde termen: **CEO-/CFO-/CxO-fraude**, **Business e-mail compromise (BEC)**

WhatsApp-fraude
Vorm van oplichting via WhatsApp waarbij het slachtoffer denkt een bekende, vaak een zoon of dochter, te helpen met een betaling.

Gerelateerde termen: **Vriend-in-nood-fraude**

White team/white teaming
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Gerelateerde termen: **Adversary simulation**

Whitebox test
Kijk voor de toelichting bij de gerelateerde term(en) in het oranje kader. →

Gerelateerde termen: **Crystalbox 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 cowboy-films waarin de held altijd een witte hoed droeg. Een whitehat hacker wordt ook wel een ethische hacker genoemd.

Gerelateerde termen: **Hacker**, **Greyhat hacker**, **Blackhat hacker**

Whitelisting
Whitelisting wordt ook wel allow listing genoemd. Bij whitelisting beschrijf je wie of wat er toegestaan is om te gebruiken. Dit wordt technisch ingericht. Het tegenovergestelde is blacklisting of deny listing.

Gerelateerde termen: **Allow listing**, **Blacklisting**, **Blocklisting**, **Deny listing**

Wifi-calling
Bij wifi-calling loopt je telefoongesprek via wifi in plaats van je telefoonprovider.

Gerelateerde termen: **SURFwireless**

Wifi-netwerk
Draadloze internetverbinding

Gerelateerde termen: **eduroam**

Gerelateerde termen:

Worm

Malware

Kwaadaardige code die zichzelf, zonder tussenkomst van een mens, vermenigvuldigt en verspreidt over verschillende digitale systemen. Bekende voorbeelden van wormen zijn WannaCry en NotPetya.

X

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).

XDR (Extended Detection and Response)

XDR maakt het makkelijker om incidenten te detecteren en erop te reageren door Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), Endpoint Detection and Repsonse (EDR) en Network traffic Analysis (NTA) te combineren.

XSS

Cross site scripting

Cross site scripting

Z

Zero trust

Model met strenge regels over hoe binnen een intern netwerk, onderling vertrouwen is ingericht. Het uitgangspunt luidt: vertrouw niets of niemand, controleer altijd of een gebruiker of computer wel is wie hij zegt te zijn. Een gebruiker mag alleen in een digitaal systeem, als het systeem heeft gecontroleerd wie hij is en waar hij is.

Zero Trust Architecture (ZTA)

Een model voor security-architectuur met een aantal leidende principapparaat geen verhoogde toegang (het netwerk wordt niet vertrouwd). Naast gebruikers, moeten ook apparaten geauthenticeerd worden. En door meerlaagse securitychecks wordt vertrouwen zo veel mogelijk vervangen door controles. Informatie wordt altijd versleuteld uitgewisseld.

Zero-click-aanval

Gerelateerde termen: **Worm**

Aanval waarbij de gebruiker niet hoeft te klikken voordat hij begint. Anders dan veelvoorkomende aanvallen zoals phishing, waarbij de gebruiker eerst iets moet doen.

Zero-day

Gerelateerde termen: **0-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 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 speciale exploit omdat de zwakke plek die wordt misbruikt nog niet bij de leverancier bekend is en dus ook 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 deze voor veel geld verkopen aan criminelen of inlichtingendiensten.

Zombiecomputer

Gerelateerde termen: **Bot** **Botnet**

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.

Gerelateerde termen:

Zone
Een samenstel van apparatuur waaraan dezelfde beveiligingseisen worden gesteld.

Zonering
Het in kleinere onderdelen opdelen van netwerken waardoor ze beter worden beheerd, beveiligd en beheerst. Elke zone heeft een eigen beveiligingsniveau en bijpassende beveiligingsmaatregelen.

Netwerk-segmentatie
Segmentering

Zorgplicht
De plicht die organisaties die onder de Cyberbeveligingswet vallen 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 aanval te verkleinen als die er toch komt.

Cyber-beveiligingswet

Gerelateerde termen:

Colofon

Auteurs
Rosanne Pouw
Thijs Kinkhorst

Redactie
Maureen van Althuis

Vormgeving
Vrije Stijl, Utrecht

Dit is een uitgave van SURF en Cybersave Yourself.
Gebaseerd op het Cyberwoordenboek van Cyberveilig Nederland i.s.m. ECP, Platform voor de Informatiesamenleving.

Oktober 2025


CSY