
Essentiële Woordenlijst Cyberbeveiliging (NL)

- | | | | |
|----|---|----|--|
| 01 | Fundamenten en Preventie | 04 | Fase 2: Detectie, Monitoring en Analyse |
| 02 | Fase 1 — Fundamenten en Preventieve Beveiliging | 05 | Fase 2: Detectie en Monitoring |
| 03 | Fase 1: Preventie en Grondslagen | 06 | Fase 3: Respons, Herstel en Continuïteit |
| | | 07 | Fase 3: Incidentrespons en Herstel |

Fundamenten en Preventie

1 Aanvalsoppervlak (Attack Surface)

Het geheel van alle kwetsbare punten, interfaces en diensten waarlangs een aanvaller toegang kan zoeken tot een netwerk of systeem.

| Minimaliseer blootgestelde poorten en deactiveer overbodige services tijdens hardening-sessies.

2 Vertrouwelijkheid (Confidentiality)

Het principe dat data en communicatie alleen toegankelijk zijn voor expliciet geautoriseerde personen, processen of systemen.

| Pas sterke versleuteling toe tijdens opslag en transport om ongeoorloofde inzage te verhinderen.

3 Integriteit (Integrity)

De waarborg dat data en configuraties nauwkeurig, volledig en aantoonbaar ongewijzigd blijven door onbevoegden.

| Gebruik cryptografische hashes en digitale handtekeningen voor actieve bestands- en vertrouwenscontrole.

4 Beschikbaarheid (Availability)

De garantie dat operationele IT-systemen en bedrijfskritische informatie tijdig bereikbaar blijven voor bevoegde gebruikers.

| Richt redundantie en periodiek beproefde back-upsystemen in tegen storingen en ransomware.

5 Zero Trust Architectuur

Een beveiligingsmodel dat structureel uitgaat van nul impliciet vertrouwen, ongeacht de locatie binnen het netwerk.

| Dwing continue authenticatie en strikte microsegmentatie af op ieder netwerkknooppunt.

Fase 1 — Fundamenten en Preventieve Beveiliging

6 Meervoudige Verificatie (MFA)

Een authenticatiemethode die ten minste twee verschillende factoren vereist om iemands identiteit te bewijzen.

| Verplicht MFA voor alle beheeraccounts en externe toegangspunten.

7 Principe van Minste Bevoegdheid (Least Privilege)

Het beleid waarbij gebruikers en processen uitsluitend de minimale toegangsrechten krijgen die strikt noodzakelijk zijn.

| Voorkom standaard administratorrechten op werkstations om laterale verplaatsing in te perken.

8 Netwerksegmentatie

Het fysiek of logisch opdelen van een netwerk in kleinere, afzonderlijk beheerde subnetwerken of zones.

| Isoleer kritieke servers van algemene kantoornetwerken met firewalls en VLANs.

9 Patchbeheer (Patch Management)

Het systematisch identificeren, testen en installeren van software-updates om beveiligingslekken te dichten.

| Hanteer een strakke testcyclus voor beveiligingspatches op internetgerichte servers.

10 Symmetrische Versleuteling

Een cryptografische techniek waarbij dezelfde geheime sleutel wordt gebruikt voor zowel versleuteling als ontsleuteling.

| Gebruik AES-256 voor snelle en robuuste bulkversleuteling van databases.

11 Asymmetrische Versleuteling

Een cryptografische methode die gebruikmaakt van een sleutelpaar: een openbare sleutel en een strikt geheime privésleutel.

| Zet asymmetrische cryptografie in voor sleuteluitwisseling bij TLS-verbindingen.

12 Hashing

Een mathematische eenrichtingsfunctie die willekeurige gegevens omzet in een unieke tekenreeks van vaste lengte.

| Sla wachtwoorden nooit plat op, maar hasj ze met een willekeurige salt.

13 Toegangscontrole op Basis van Rollen (RBAC)

Een autorisatiemodel waarbij permissies worden toegekend aan functierollen in plaats van individuele accounts.

| Wijs gebruikersrollen toe in directoryservices om autorisaties schaalbaar te beheren.

14 Hardening

Het beveiligen van systemen door onnodige software, poorten, protocollen en standaardwachtwoorden te verwijderen.

| Pas standaarden zoals CIS Benchmarks toe op pas geïnstalleerde besturingssystemen.

15 End-to-End Encryptie (E2EE)

Een versleutelingsmethode waarbij alleen de communicerende eindgebruikers de berichten kunnen ontcijferen en tussenliggende servers niet.

| Gebruik E2EE bij interne communicatie-apps voor vertrouwelijke directiegesprekken.

16 Phishing

Een vorm van social engineering waarbij aanvallers zich voordoen als betrouwbare entiteiten om inloggegevens of gevoelige data te ontfutselen.

| Train personeel met periodieke simulaties en hanteer duidelijke meldingsknoppen in e-mailclients.

17 Social Engineering

Het psychologisch manipuleren van mensen om vertrouwelijke handelingen uit te voeren of geheime gegevens prijs te geven.

| Stel verificatieprocedures in voor ongebruikelijke betalingsverzoeken per telefoon of e-mail.

18 Kwetsbaarheidenscan (Vulnerability Scan)

Een geautomatiseerde audit die netwerken en systemen controleert op bekende beveiligingsfouten en misconfiguraties.

| Draai wekelijkse kwetsbaarheidsscans om ontbrekende patches direct in kaart te brengen.

19 Penetratietest (Pentest)

Een geautoriseerde en gesimuleerde cyberaanval om de operationele effectiviteit van beveiligingsmaatregelen diepgaand te testen.

| Laat jaarlijks een onafhankelijke pentest uitvoeren op publiek toegankelijke webapplicaties.

20 Gegevensclassificatie

Het categoriseren van organisatiedata op basis van gevoeligheid en het potentiële risico bij ongeautoriseerde openbaarmaking.

| Label documenten als openbaar, intern of vertrouwelijk om passende bescherming af te dwingen.

21 Firewall (Netwerkbeveiliging)

Systeem dat inkomend en uitgaand netwerkverkeer inspecteert en filtert volgens ingestelde beveiligingsregels.

| Plaats aan de netwerkperimeter en tussen interne zones om ongeautoriseerde verbindingen direct te blokkeren.

22 Virtueel Privaat Netwerk (VPN)

Versleutelde verbinding over een openbaar netwerk die communicatie tussen apparaat en bedrijfsnetwerk beveiligt.

| Verplicht stellen voor externe medewerkers om afluisteren op openbare netwerken te verhinderen.

23 Publieke Sleutel Infrastructuur (PKI)

Raamwerk van beleid, technologie en procedures voor het uitgeven en beheren van digitale certificaten.

| Inzetten voor betrouwbare server-identificatie en veilige TLS-gecodeerde communicatie via vertrouwde certificaatautoriteiten.

24 Digitaal Certificaat (TLS/SSL)

Elektronisch bestand dat een publieke sleutel bindt aan een geverifieerde identiteit via cryptografische ondertekening.

| Toepassen op webservern om HTTPS-verkeer te versleutelen en man-in-the-middle-aanvallen af te slaan.

25 Gegevensverliespreventie (DLP)

Software die voorkomt dat gevoelige gegevens ongeautoriseerd het bedrijfsnetwerk verlaten of gekopieerd worden.

| Monitoren van e-mailbijlagen en usb-poorten op aanwezigheid van persoonsgegevens of intellectueel eigendom.

Fase 1: Preventie en Grondslagen

26 Web Application Firewall (WAF)

Specifieke filterlaag die HTTP-verkeer naar webtoepassingen inspecteert op applicatie-aanvallen zoals injecties.

| Plaatsen vóór publieke webapplicaties om SQLi en XSS direct te detecteren en blokkeren.

27 Air Gapping

Beveiligingsmaatregel waarbij een computernetwerk fysiek volledig is ontkoppeld van externe en onveilige netwerken.

| Gebruiken voor kritieke back-uparchieven en operationele systemen om remote besmettingen onmogelijk te maken.

28 Eindpuntbeveiliging (Endpoint Protection)

Centraal beheerde beveiligingslaag op individuele apparaten tegen schadelijke software en ongeautoriseerd gebruik.

| Installeren op laptops en servers ter bescherming tegen kwaadaardige downloads en procesinjecties.

29 Geleide Toegangscontrole (MAC)

Beveiligingsmodel waarin een centrale autoriteit toegangsrechten oplegt via strikte vertrouwelijkheidslabels.

| Toepassen in militaire of hoogbeveiligde omgevingen om ongeautoriseerde informatiedoorstroom absoluut te verhinderen.

30 Wachtwoordbeheerder (Password Manager)

Versleutelde kluisapplicatie voor het genereren en veilig opslaan van unieke, complexe inloggegevens.

| Organisatiebreed invoeren om wachtwoordhergebruik en zwakke combinaties effectief uit te bannen.

Fase 2: Detectie, Monitoring en Analyse

31 Inbraakdetectiesysteem (IDS)

Monitoringsysteem dat verdacht netwerkverkeer analyseert en waarschuwingen genereert bij geconstateerde dreigingen.

| Gebruiken om passief netwerkafwijkingen en bekende aanvalspatronen vroegtijdig te signaleren.

32 Inbraakpreventiesysteem (IPS)

Actieve netwerklaag die verdacht dataverkeer niet alleen herkent, maar direct geautomatiseerd stopt.

| Plaatsen in de verkeersstroom om kwaadaardige pakketten realtime af te breken vóór endpoints worden geraakt.

33 Security Information and Event Management (SIEM)

Platform voor centrale verzameling, normalisatie en geautomatiseerde correlatie van logbestanden uit diverse systemen.

| Inrichten in het SOC om verspreide logdata om te zetten in bruikbare beveiligingsmeldingen.

34 Security Operations Center (SOC)

Gespecialiseerd team en commandocentrum verantwoordelijk voor 24/7 monitoring, detectie en incidentafhandeling.

| Aanstellen voor continue waakzaamheid en triage van prioritaire beveiligingsincidenten.

35 Endpoint Detection and Response (EDR)

Agentsoftware die endpointactiviteit registreert, verdacht gedrag analyseert en direct reacties mogelijk maakt.

| Inzetten om verdachte procesuitvoeringen op laptops te detecteren en geïnfecteerde hosts direct netwerktechnisch te isoleren.

36 Extended Detection and Response (XDR)

Platform dat detectiegegevens over endpoints, netwerken, e-mail en clouddiensten automatisch koppelt en analyseert.

| Toepassen voor een alomvattend overzicht van complexe, meervoudige aanvalsvectoren binnen de gehele organisatie.

37 Dreigingsinformatie (Threat Intelligence)

Gestructureerde informatie over tactieken, technieken en aanvalskennmerken van actieve cybercriminelen en statelijke actoren.

| Logsystemen en firewalls verrijken met indicators of compromise (IoC's) om actuele campagnes af te vangen.

38 Dreigingsjacht (Threat Hunting)

Handmatig en analytisch proces om proactief naar niet-gedetecteerde aanvallers in het netwerk te zoeken.

| Periodiek hypothesen formuleren en data analyseren om geruisloze infiltraties op te sporen.

39 Indicator van Inbreuk (IoC)

Digitaal spoor dat duidt op een beveiligingsinbreuk, zoals specifieke bestandshashes of kwaadaardige IP-adressen.

| Laden in SIEM- en EDR-systemen om besmette apparaten direct geautomatiseerd te identificeren.

40 Indicator van Aanval (IoA)

Signaal dat wijst op de intentie en lopende actie van een aanvaller, ongeacht de gebruikte malwareversie.

| Monitoren op afwijkend gedrag zoals verdachte PowerShell-opdrachten om aanvallen in real-time te stoppen.

Fase 2: Detectie en Monitoring

41 Honeypot (Lokaas)

Een opzettelijk kwetsbaar opgesteld doelsysteem ontworpen om aanvallers aan te trekken, te misleiden en hun gedrag te analyseren zonder risico voor productiedata.

| Plaats een virtuele server in een DMZ om vroege verkenningsactiviteiten te signaleren.

42 Gedragsanalyse (UEBA)

User and Entity Behavior Analytics detecteert afwijkingen van normale activiteitspatronen van accounts en apparaten met machine learning.

| Signaleer gecompromitteerde inloggegevens wanneer een account plotseling 's nachts bulkdata downloadt.

43 Logbeheer (Log Management)

Het gestructureerd verzamelen, aggregeren, normaliseren en veilig bewaren van systeem- en applicatielogs ter ondersteuning van toezicht en compliance.

| Centraliseer firewall- en serverlogs met onveranderbare opslag voor auditdoeleinden.

44 Netwerkstroomanalyse (NetFlow)

Statistische analyse van netwerkverkeersstromen (bron, doel, poort en volume) zonder inspectie van de volledige pakketinhoud.

| Detecteer verdachte data-exfiltratie naar onbekende externe IP-adressen op basis van verkeerspieken.

45 SOAR (Security Orchestration, Automation and Response)

Technologie die beveiligingstaken automatiseert en workflows tussen verschillende beveiligingsoplossingen stroomlijnt via gestandaardiseerde playbooks.

| Blokkeer automatisch kwaadaardige IP-adressen op firewalls direct na een waarschuwing melding.

46 Diepe Pakketinspectie (DPI)

Geavanceerde filtertechniek die zowel de metadata als de daadwerkelijke inhoud van passerende datapakketten diepgaand inspecteert.

| Herken verborgen malwarepayloads en verboden applicatieprotocollen binnen goedgekeurd poortverkeer.

47 Verkeersafspiegeling (Port Mirroring / SPAN)

Een switchfunctie die een kopie van netwerkverkeer van specifieke poorten doorstuurt naar een monitoringpoort voor analyse.

| Voed een passief IDS-sensornetwerk met continu realtime netwerkverkeer.

48 Bastion Host (Sprongserver)

Een speciaal geharde server die dient als enige gecontroleerde en gemonitorde toegangspoort tot interne netwerkomgevingen.

| Verleen systeembeheerders uitsluitend via deze server en MFA toegang tot productiedatabases.

49 Synthetische Monitoring

Het periodiek uitvoeren van gesimuleerde gebruikerstransacties om de beschikbaarheid en integriteit van diensten proactief te testen.

| Voer continue inlogtests uit om onbeschikbaarheid op te merken vóór gebruikers klagen.

50 Bestandsintegriteitsbewaking (FIM)

Een beveiligingsmechanisme dat wijzigingen in kritieke systeembestanden, configuraties en registers controleert en valideert tegen hash-baselines.

| Detecteer ongeautoriseerde wijzigingen in systeembestanden direct na een mogelijke inbraak.

Fase 3: Respons, Herstel en Continuïteit

51 Incident Respons Plan (IRP)

Een gedocumenteerd draaiboek met procedures, rollen en communicatielijnen om gestructureerd te reageren op beveiligingsincidenten.

| Stuur het responsteam aan tijdens een actieve aanval om schade direct te beperken.

52 Insluiting (Containment)

De fase in incidentrespons waarin verdere verspreiding van een cyberaanval of malwarebesmetting actief wordt gestopt.

| Isoleer besmette werkstations direct van het lokale netwerk om laterale verplaatsing te blokkeren.

53 Uitroeiing (Eradication)

Het volledig verwijderen van alle sporen van een aanvaller, inclusief malware, achterdeurtjes en gecompromitteerde accounts.

| Verwijder kwaadaardige cronjobs en herstel aangetaste systeembestanden naar een schone staat.

54 Herstel (Recovery)

Het gecontroleerd terugbrengen van getroffen systemen en gegevens naar normale productiecondities na verificatie van veiligheid.

| Zet geverifieerde schone back-ups terug en hervat gefaseerd de kritieke bedrijfsprocessen.

55 Evaluatie en Geleerde Lessen (Lessons Learned)

Een gestructureerde evaluatie na een incident om te bepalen wat er gebeurde, wat werkte en hoe processen verbeterd moeten worden.

| Update verdedigingsregels en procedures op basis van concrete tekortkomingen uit de evaluatie.

56 Digitale Forensica (Forensics)

Het wettig en methodisch verzamelen, veiligstellen en analyseren van digitaal bewijsmateriaal na een cyberincident.

| Maak een bit-voor-bit schijfkopie van een gecompromitteerde server voor forensische analyse.

57 Keten van Bewaring (Chain of Custody)

Nauwkeurige chronologische documentatie die aantoont wie forensisch bewijs heeft verzameld, beheerd en geanalyseerd zonder manipulatie.

| Registreer elke fysieke en digitale overdracht van forensische bewijsdragers in een logboek.

58 Ransomware (Gijzelsoftware)

Schadelijke software die bestanden of systemen versleutelt en losgeld eist in ruil voor de decoderingssleutel.

| Voorkom betaling door te vertrouwen op geteste, offline opgeslagen back-ups voor snel herstel.

59 Bedrijfscontinuïteitsplan (BCP)

Een integraal strategisch plan dat waarborgt dat kritieke bedrijfsprocessen doordraaien tijdens en direct na een ernstige calamiteit.

| Activeer alternatieve werklocaties en handmatige werkprocessen tijdens langdurige IT-uitval.

60 Rampenherstelplan (Disaster Recovery Plan)

Een specifiek technisch plan gericht op het herstellen van vitale IT-infrastructuur, servers en dataopslag na een catastrofe.

| Voer failover-procedures uit naar een secundair datacenter bij uitval van de primaire site.

Fase 3: Incidentrespons en Herstel

61 DDoS-mitigatie (Distributed Denial of Service)

DDoS-mitigatie omvat technieken om grootschalige, gedistribueerde netwerkaanvallen te absorberen of te filteren, zodat diensten operationeel blijven.

| Inzetten van scrubbing centers en anycast-routing bij volumetrische netwerkaanvallen.

62 Geheugenanalyse (RAM Forensics)

Geheugenanalyse is het veiligstellen en onderzoeken van vluchtig RAM-geheugen om actieve malware, injecties en niet-opgeslagen gegevens te identificeren.

| RAM-dump analyseren tijdens actieve besmettingen om encryptiesleutels of injecties te achterhalen.

63 Tijdlijnreconstructie (Timeline Analysis)

Tijdlijnreconstructie ordent systeemgebeurtenissen chronologisch op basis van tijdstempels om aanvalsvectoren en acties nauwkeurig te herleiden.

| Logboeken correleren om de exacte inbraaksequentie en laterale verplaatsing vast te stellen.

64 Draaiboek (Incident Playbook)

Een incident playbook biedt een vooraf gedefinieerd, stapsgewijs stappenplan voor het snel en uniform afhandelen van specifieke dreigingstypen.

| Het ransomware-draaiboek direct activeren om isolatie en communicatie foutloos te sturen.

65 Back-up Onveranderlijkheid (Immutable Backup)

Onveranderlijke back-ups kunnen gedurende een vastgestelde periode door niemand worden gewijzigd of verwijderd, zelfs niet door beheerders.

| Bescherming tegen ransomware die schaduwkopieën en back-ups tracht te vernietigen.

66 Quarantaine (Netwerkisolatie)

Netwerkisolatie verbreekt alle reguliere verbindingen van een verdacht eindpunt, met uitzondering van een beveiligd beheerkanaal voor onderzoek.

| Een besmet werkstation direct afsluiten van het bedrijfsnetwerk via EDR-opdrachten.

67 Ransomware Onderhandeling en Beleid

Het beleid rond losgeldonderhandelingen definieert wettelijke, ethische en operationele richtlijnen over het al dan niet communiceren met aanvallers.

| Direct inschakelen van bevoegde autoriteiten en crisisteams conform het bedrijfsbeleid.

68 Communicatiematrix bij Incidenten

Een communicatiematrix specificeert wie, wanneer en via welke beveiligde kanalen geïnformeerd wordt tijdens een ernstig informatiebeveiligingsincident.

| Gebruikmaken van out-of-band communicatiekanalen wanneer de primaire e-mailinfrastructuur gecompromitteerd is.

69 Hersteltijd Doelstelling (RTO)

Recovery Time Objective (RTO) is de maximaal toelaatbare tijdsduur waarin een bedrijfsproces of IT-systeem na een storing hersteld moet zijn.

| Prioriteren van herstelvolgorde van kritieke databases tijdens systeemuitval.

70 Herstelpunt Doelstelling (RPO)

Recovery Point Objective (RPO) definieert de maximaal aanvaardbare periode van dataverlies, gemeten in tijd vanaf het moment van uitval.

| Bepalen van de vereiste back-upfrequentie en datareplicatieschema's voor financiële data.

71 Forensisch Kopieerproces (Bit-stream Image)

Een bit-stream image is een exacte, bit-voor-bit replica van een fysiek opslagmedium, inclusief vrije ruimte en verwijderde gegevens.

| Veiligstellen van bewijsmateriaal op een write-blocker voorafgaand aan diepgaand schijfonderzoek.

72 Root Cause Analysis (Oorzaakanalyse)

Root Cause Analysis is een gestructureerde methode om de fundamentele kwetsbaarheid of procesfout te identificeren die het incident mogelijk maakte.

| Voorkomen van herhaalde inbraken door de initiële toegangsmethode definitief te verhelpen.

73 Post-Mortem Vergadering

Een post-mortem is een multidisciplinaire bespreking na een incident om responsprestaties te analyseren en verbeterpunten vast te leggen.

| Beveiligingsprocedures en detectieregels aanscherpen op basis van waargenomen tekortkomingen.

74 Datalek Notificatieplicht (AVG / GDPR)

De wettelijke verplichting om ernstige inbreuken op persoonsgegevens binnen 72 uur te melden aan de toezichthouder en eventueel betrokkenen.

| Tijdig inschakelen van de Functionaris Gegevensbescherming bij gecompromitteerde klantgegevens.

75 Crisisbeheerteam (Crisis Management Team)

Het orgaan op directieniveau dat strategische beslissingen neemt omtrent reputatie, financiën, continuïteit en juridische stappen tijdens een crisis.

| Besluiten over externe persberichten en noodfinanciering tijdens een aanhoudende cyberaanval.

76 Failover en Redundantie

Failover is het geautomatiseerd of handmatig overschakelen naar een standby-systeem bij het falen van de primaire server of netwerkverbinding.

| Verkeer naadloos routeren naar een secundair datacenter bij hardwarematige storingen.

77 Clean Room Herstelomgeving

Een geïsoleerde, schone infrastructuur waarin back-ups veilig worden teruggezet en gevalideerd op persistente malware voordat productie start.

| Herstellen en scannen van back-upbestanden zonder risico op herinfectie van het netwerk.

78 Compromise Assessment

Een grondig onderzoek van de gehele IT-omgeving om vast te stellen of aanvallers onopgemerkt aanwezig zijn of recent actief zijn geweest.

| Uitvoeren na fusies of vermoedelijke netwerkinbreuken om slapende achterdeurtjes op te sporen.

79 Forensisch Verslag (Forensic Report)

Een formeel document waarin forensische bevindingen, methoden en feitelijke conclusies helder worden gerapporteerd voor juridisch of intern gebruik.

| Aanbieden van bewijsmateriaal aan opsporingsdiensten of verzekeraars na een ransomware-inbraak.

80 Cyberverzekering (Cyber Insurance Claims)

Een verzekering die financiële verliezen, herstelkosten en aansprakelijkheid compenseert die voortvloeien uit cyberaanvallen en gegevensinbreuken.

| Direct contact opnemen met de verzekeringsexpert ter goedkeuring van ingeschakelde herstelbedrijven.
