WHITEPAPER 2026

ACADEMIE NEDERLAND

Cyberweerbaarheid begint bij medewerkers

10 praktische maatregelen en een uitgebreide checklist voor een digitaal veilige organisatie



10 maatregelen

30 controlepunten

90 dagen actieplan

ACADEMIE NEDERLAND

Waarom cyberweerbaarheid begint bij medewerkers

Een praktische gids voor medewerkers, leidinggevenden en organisaties.



Een sterke digitale organisatie begint bij veilig gedrag.

Techniek is onmisbaar, maar medewerkers moeten dreigingen herkennen, veilig handelen en zonder drempels kunnen melden.

DIT VINDT U IN DE WHITEPAPER

01 Risco's en herkenbare voorbeelden

02 Tien maatregelen voor dagelijks gebruik

03 Praktijkcasussen en incidentrespons

04 Checklist, scoremodel en 90-dagenplan

De mens, de techniek en het proces

Waarom kleine handelingen grote gevolgen kunnen hebben.

- Een medewerker ontvangt een geloofwaardige factuur,
- een onverwacht inlogverzoek of een document met
- te ruime deelrechten. Zulke situaties vragen niet
- alleen om software, maar ook om duidelijke afspraken.



VIJF BASISPRINCIPES VAN DIGITALE WEERBAARHEID

1. Breng de belangrijkste risico's in kaart
2. Bevorder veilig gedrag en een open meldcultuur
3. Bescherm systemen, applicaties en apparaten
4. Beheer toegangsbrechten zorgvuldig
5. Bereid de organisatie voor op incidenten

CYBERDREIGINGEN

Welke digitale risico’s moet u herkennen?

Vijf veelvoorkomende dreigingen op de werkvloer.



01 **Phishing en zakelijke e-mailfraude**
Controleer onverwachte betaalverzoeken via een bekend kanaal.

02 **Social engineering via telefoon en chat**
Deel nooit zomaar wachtwoorden, codes of toegang.

03 **Onveilig inloggen en MFA-verzoeken**
Keur nooit een inlogverzoek goed dat u niet zelf startte.

04 **Datalekken en verkeerd delen**
Controleer ontvangers, toegang en gevoeligheid van bestanden.

05 **Ransomware en schadelijke bestanden**
Meld verdachte downloads of afwijkend systeemgedrag.

DE AANPAK

10 maatregelen voor veilig gedrag

Maatregelen 1 tot en met 5 – van inzicht naar actie.



01 **Maak risico's concreet**
Gebruik voorbeelden uit uw eigen processen, zoals facturen en personeelsgegevens.

02 **Train medewerkers per functie**
Een finance-team loopt andere risico's dan de servicedesk of HR.

03 **Controleer onverwachte verzoeken**
Verifeer betalingen en gevoelige informatie via een onafhankelijk kanaal.

04 **Gebruik veilige authenticatie**
Pas unieke wachtwoorden, passkeys, wachtwoordmanagers en MFA toe.

05 **Maak melden laagdrempelig**
Stimuleer snelle meldingen en reageer zonder schuldtoewijzing.

10 maatregelen voor veilig gedrag

Maatregelen 6 tot en met 10 — van beleid naar gewoonte.



06 Deel informatie zorgvuldig
Gebruik goedgekeurde tools en controleer gedeelde toegangsrechten.

07 Beveilig apparaten en werkplekken
Vergrendel schermen en meld verloren apparaten onmiddellijk.

08 Oefen realistische scenario's
Doe phishingoefeningen en bespreek hoe medewerkers reageren.

09 Maak leiderschap zichtbaar
Geef zelf het goede voorbeeld en stimuleer een veilige meldcultuur.

10 Meet en verbeter periodiek
Evalueer oefeningen, incidentmeldingen en openstaande acties.

PRAKTIJKCASES

Drie situaties om met uw team te oefenen

Gebruik de casussen om gedrag, werkspraken en procedures te bespreken.



A De dringende factuur

SITUATIE Een medewerker krijgt vlak voor sluitingstijd een verzoek voor een spoedbetaling.

ACTIE Stop, verifeer via een bekend nummer en meld het verdachte bericht.

B Het gedeelde HR-document

SITUATIE Een personeelsbestand wordt met te ruime deelrechten verstuurd.

ACTIE Trek toegang zo mogelijk in en meld het mogelijke datalek direct.

C Het onverwachte MFA-verzoek

SITUATIE Een medewerker ontvangt inlogmeldingen zonder zelf in te loggen.

ACTIE Keur niets goed en volg onmiddellijk de instructies van IT.

INCIDENTRESPONS

Wat te doen bij een cyberincident?

Een helder stappenplan voor medewerkers — snel melden maakt het verschil.



1 Herken en stop
Klik niet verder en onderneem geen eigen herstelactie.

2 Meld direct
Gebruik het afgesproken interne meldkanaal.

3 Beschrijf feitelijk
Noem tijdstip, betrokken systemen en wat u zag.

4 Bewaar relevante informatie
Verwijder geen bestanden of berichten zonder instructie.

5 Werk mee aan opvolging
IT, security en privacy bepalen de vervolgstappen.

BELANGRIJK Een melding is geen schuldbekentenis. Bij twijfel: meld toch.

VERANTWOORDELIJKHEDEN

Cyberveiligheid is teamwork

Iedereen speelt een rol. Maak afspraken zichtbaar en uitvoerbaar.



01

BESTUUR & DIRECTIE

Stellen prioriteiten, maken budget vrij en volgen de voortgang.

02

IT & SECURITY

Beheren toegang, beveiliging, incidentrespons en technische maatregelen.

03

HR & LEIDINGGEVENDEN

Borgen onboarding, trainingen, werkafspraken en een open meldcultuur.

04

MEDEWERKERS

Controleren afwijkende verzoeken, beschermen gegevens en melden signalen.

KERNBOODSCHAP

Maak de veilige keuze de makkelijkste keuze.

ZELFEVALUATIE • 30 CONTROLEPUNTEN

Checklist: Mens & bewustwording

Vink aan wat aantoonbaar geregeld is binnen uw organisatie.

ONDERDEEL 1 VAN 3

10 controlepunten • score: ____ / 10

- ☐ 01 Riscovolle gegevens en processen zijn bekend bij medewerkers.
- ☐ 02 Nieuwe medewerkers krijgen uitleg tijdens hun onboarding.
- ☐ 03 Riscovolle functies krijgen aanvullende cybertraining.
- ☐ 04 Medewerkers herkennen phishing en social engineering.
- ☐ 05 Betalingsverzoeken worden onafhankelijk geverifieerd.
- ☐ 06 Onverwachte MFA-verzoeken worden nooit goedgekeurd.
- ☐ 07 Iedereen kent het interne meldpunt voor cyberincidenten.
- ☐ 08 Vergissingen kunnen zonder angst worden gemeld.
- ☐ 09 Leidinggevenden bespreken veiligheid met hun team.
- ☐ 10 Trainingen worden geëvalueerd en regelmatig verbeterd.

Tip: Bewaar bewijs zoals instructies, registraties of oefenverslagen.

ZELFEVALUATIE • 30 CONTROLEPUNTEN

Checklist: Systemen & gegevens

Vink aan wat aantoonbaar geregeld is binnen uw organisatie.

ONDERDEEL 2 VAN 3

10 controlepunten • score: ____ / 10

- ☐ 01 Passende multifactorauthenticatie is actief.
- ☐ 02 Er zijn veilige wachtwoord- en passkeyrichtlijnen.
- ☐ 03 Toegang tot systemen past bij ieders functie.
- ☐ 04 Rechten worden aangepast bij vertrek of functiewissel.
- ☐ 05 Apparaten en software krijgen tijdig updates.
- ☐ 06 Gevoelige bestanden worden alleen veilig gedeeld.
- ☐ 07 Er zijn duidelijke afspraken voor hybride werken.
- ☐ 08 Verlies van apparaten wordt onmiddellijk gemeld.
- ☐ 09 Leveranciers met systeemtoegang zijn in beeld.
- ☐ 10 Back-ups worden gemaakt én herstel wordt getest.

Tip: Bewaar bewijs zoals instructies, registraties of oefenverslagen.

ZELFEVALUATIE • 30 CONTROLEPUNTEN

Checklist: Incidenten & verbetering

Vink aan wat aantoonbaar geregeld is binnen uw organisatie.

ONDERDEEL 3 VAN 3

10 controlepunten • score: ____ / 10

- ☐ 01 Het incidentresponsplan heeft duidelijke eigenaars.
- ☐ 02 Een bereikbaar meldkanaal is intern bekend.
- ☐ 03 Phishing- en ransomware-scenario's zijn geoefend.
- ☐ 04 Medewerkers weten welke feiten zij moeten melden.
- ☐ 05 IT, HR, privacy en management kennen hun rol.
- ☐ 06 Een mogelijk datelek wordt beoordeeld en vastgelegd.
- ☐ 07 Kritieke processen en afhankelijkheden zijn bekend.
- ☐ 08 Cyberrisico's worden periodiek opnieuw beoordeeld.
- ☐ 09 Verbeteracties hebben een eigenaar en einddatum.
- ☐ 10 Het management bespreekt de verbeteringen.

Tip: Bewaar bewijs zoals instructies, registraties of oefenverslagen.

RESULTAAT

Hoe cyberweerbaar is uw organisatie?

Tel uw vinkjes en bepaal welke risico's eerst aandacht verdienen.



01	Mens & bewustwording	___ / 10
02	Systemen & gegevens	___ / 10
03	Incidenten & verbetering	___ / 10

TOTAALSCORE ___ / 30

Score is een indicatie, geen audit of wettelijke toets.

0-10 Start met de basis

11-20 Borg bestaande maatregelen

21–26 Controleer de uitvoering

27–30 Blijf toetsen en verbeteren

IMPLEMENTATIE

Uw actieplan voor de eerste 30 dagen

Van nulmeting tot concrete verbeteringen: vier overzichtelijke weken.



WEEK 1

Nulmeting en eigenaarschap

Vul de checklist in, benoem kritieke processen en wijs eigenaren aan.

WEEK 2

Beperk directe risico's

Controleer MFA, meldprocedures en betalingsverificatie; los urgente hiaten op.

WEEK 3

Training en oefening

Oefen een phishing- of fraudegeval en bespreek wat medewerkers nodig hebben.

WEEK 4

Evaluatie en vervolg

Controleer de voortgang, actualiseer de checklist en rapporteer besluiten.

DUURZAAM VERBETEREN

Van 30 naar 90 dagen

Veilig werken is geen eenmalige actie maar een continu verbeterproces.



01

DAG 31–60 • VERDIEPEN

Ontwikkel functiegerichte trainingen, verbeter toegangsbewer en oefen samenwerking tussen IT, HR en privacy.

02

DAG 61–90 • BORGEN

Actualiseer procedures, evalueer oefeningen en neem een beperkt aantal indicatoren op in de managementrapportage.

BLIJVEND RITME

Herhaal de checklist ieder kwartaal of na grote veranderingen.

VERDER LEREN

Samen bouwen aan cyberweerbaarheid

Ontwikkel kennis en vaardigheden met Academie Nederland.



ISO 27001 Foundation

De basis van informatiebeveiliging en risicobeheersing.

ISO 27001 Professional

Verdieping voor security- en beleidsprofessionals.

NIS2 Professional

Cybersecurityverplichtingen vertalen naar maatregelen.

Privacy & Data Protection

Bewust omgaan met persoonsgegevens en privacy.

KLAAR VOOR DE VOLGENDE STAP?

Bespreek een incompany training op maat.

www.academie-nederland.nl