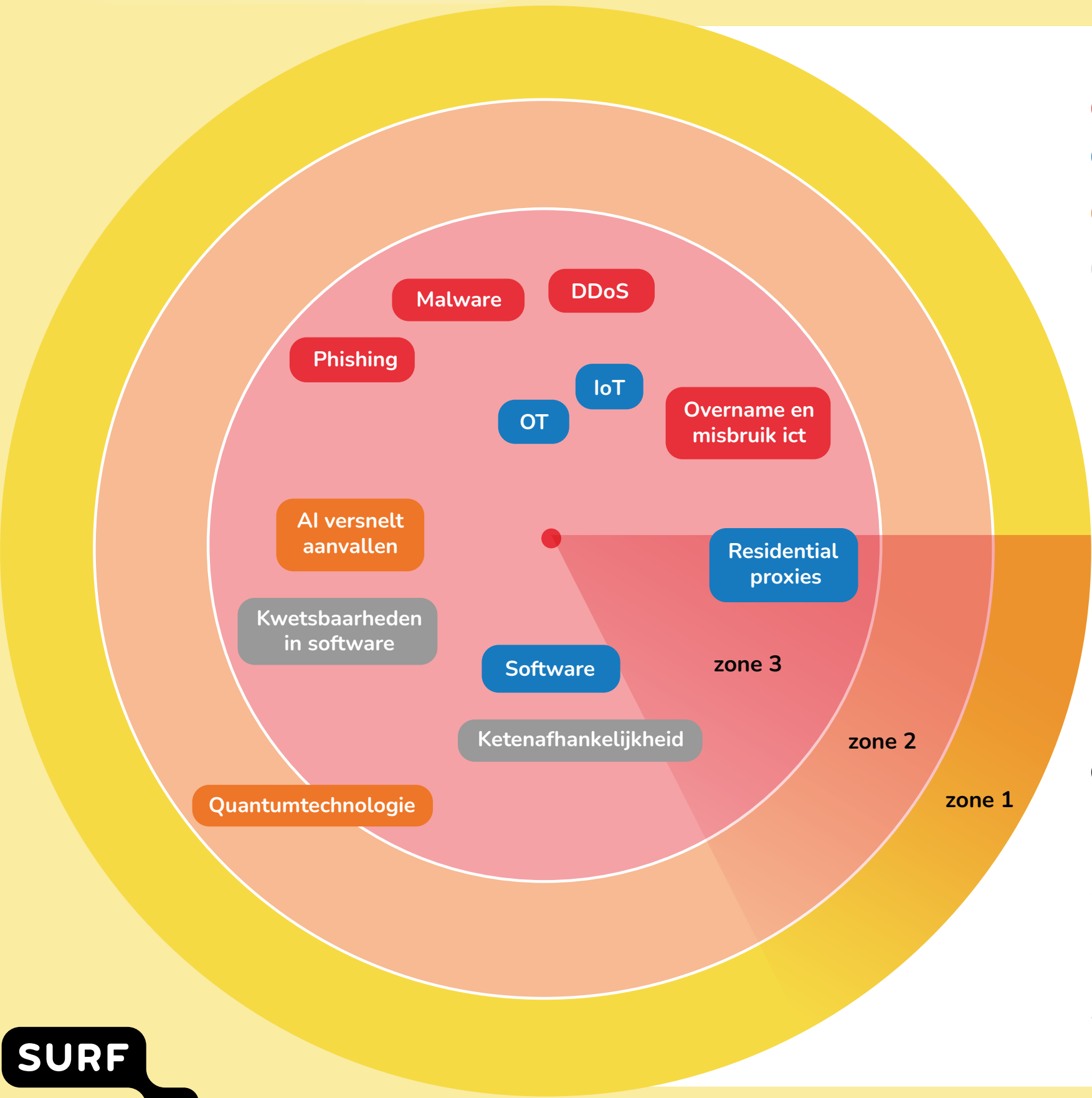


CYBERDREIGINGSBEEELD 2026

De belangrijkste
cybersecuritytrends
in onderwijs
en onderzoek





- Dreiging
- Meer aandacht nodig
- Trend, invloed
- Wat ons kwetsbaar maakt

TOELICHTING TRENDS

Zoals elk jaar blijven de trends uit voorgaande jaren relevant. Zo zijn de trends van 2025 ook in 2026 actueel. Dit dreigingsbeeld beschrijft de belangrijkste veranderingen en accenten binnen deze dreigingen:

1. Kwetsbaarheden worden steeds sneller misbruikt

De ontwikkelingen in AI veranderen het beeld ten opzichte van 2025. Waar het in 2018 gemiddeld 771 dagen duurde voordat een kwetsbaarheid werd misbruikt, is dat in 2026 nog slechts 1,54 dag. Instellingen moeten daarom niet alleen sneller, maar vooral slimmer gaan patchen.

ZONES

- Zone 3: Acuut**
dagelijks te zien, nu actie nemen.
- Zone 2. Belangrijk**
dit gebeurt al, bereid je voor.
- Zone 1: Opletten**
kunnen belangrijk gaan worden in toekomst of vaker voorkomen.

2. Voorbereiding op quantum-technologie blijft achter

Uit een peiling van SURF onder security-professionals in 2026 blijkt dat quantum-technologie bij bijna een derde van de instellingen nauwelijks bekend is, ook niet op directie- of bestuursniveau. Toch is het risico actueel: aanvallers stelen nu al versleutelde gegevens om die later met quantumtechnologie te kunnen ontsleutelen (*store now, decrypt later*).

3. Kwetsbaarheden in de softwareketen vergroten het aanvalsoppervlak

Aanvallers richten zich steeds vaker op de softwareketen in plaats van op individuele organisaties. Vrijwel elke organisatie gebruikt honderden tot duizenden opensource-library's en -componenten. Door misbruik van een kwetsbaarheid in een veelgebruikt component kan een aanvaller in één klap duizenden organisaties raken.

4. Niet-Europese technologie vergroot de kwetsbaarheid

De afhankelijkheid van niet-Europese technologie brengt steeds grotere risico's met zich mee voor continuïteit, veiligheid en privacy. Door die afhankelijkheid kunnen verstoringen en geopolitieke ontwikkelingen ertoe leiden dat instellingen geen toegang meer hebben tot essentiële technologie en digitale diensten.

Actueel overzicht trends en dreigingen

Zie voor een actueel overzicht van van deze en andere trends en dreigingen het cybersecurity-dashboard.

► [Naar het SURF cybersecurity-dashboard](#)
(inloggen met SURFconext)

5. Cyber-fysieke systemen (OT) onvoldoende in beeld

Cyber-fysieke systemen die gebruikmaken van operationele technologie (OT) – zoals systemen die gebouwen, energievoorzieningen, onderzoekopstellingen en klimaatbeheersing op de campus aansturen – zijn steeds vaker verbonden met het internet, maar onvoldoende in beeld bij de IT-afdeling. Daardoor worden deze systemen niet goed gemonitord en onderhouden, en zijn ze kwetsbaarder voor cyberaanvallen en verstoringen.

6. Residential proxies maken kwaadaardig verkeer moeilijker herkenbaar

Aanvallers benaderen organisaties steeds vaker via residential proxies - diensten die internetverkeer omleiden via vertrouwde IP-adressen van onderwijsinstellingen. Daardoor is kwaadaardig verkeer moeilijker te herkennen en te blokkeren. Studenten en medewerkers kunnen hun apparaat zo onbedoeld onderdeel maken van een proxy-netwerk en daarmee een ingang bieden voor cybercriminaliteit.

Uit de praktijk

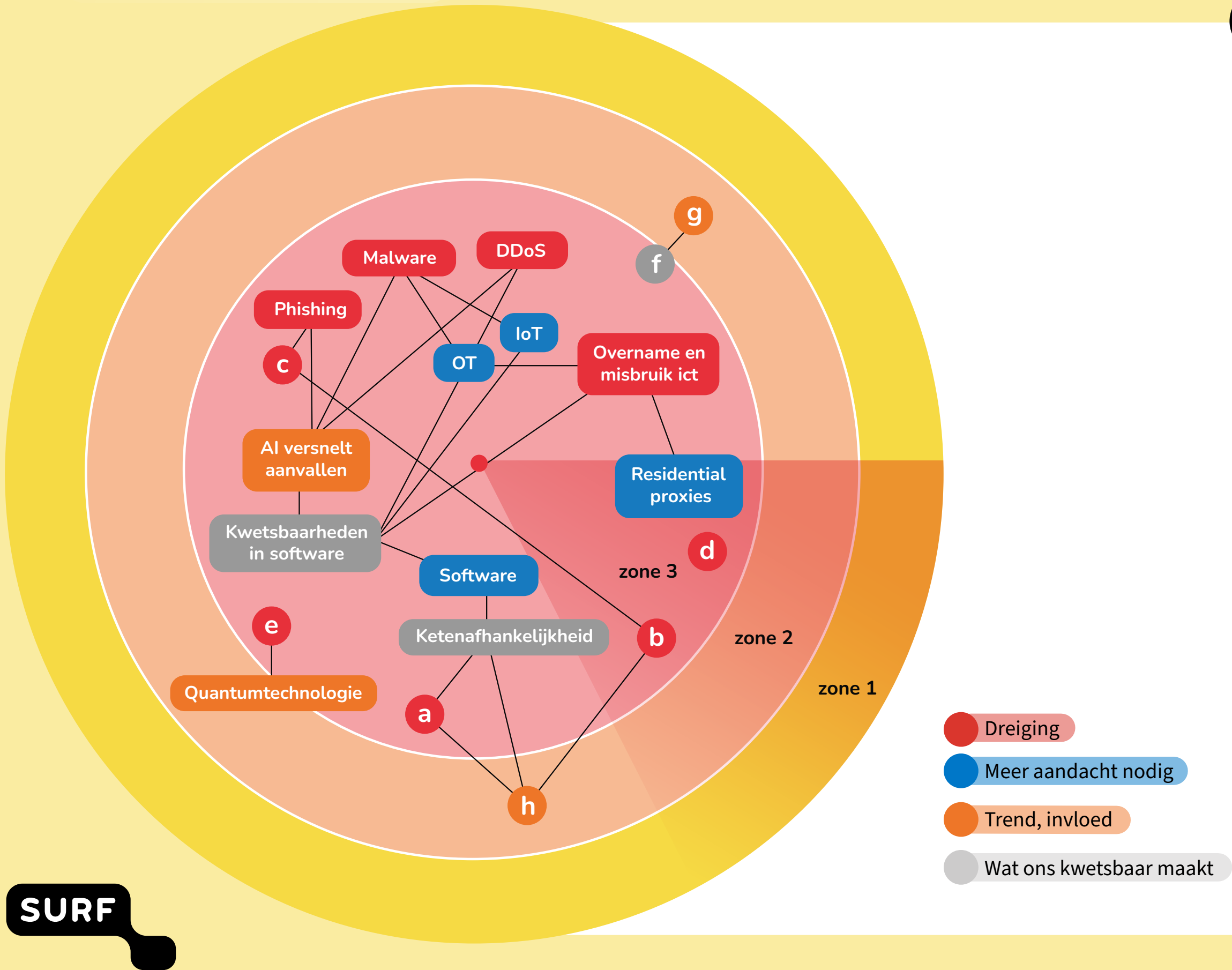
- ▶ AI versnelt het vinden van kwetsbaarheden, maar houden onderwijs en onderzoek het patchtempo bij?
- ▶ De onzichtbare kwetsbaarheid van cyber-fysieke systemen
- ▶ Quantumveiligheid in onderwijs en onderzoek: bewustzijn is er, actie blijft uit
- ▶ Residential proxies: aanvallers vermomd als gewone studenten

SAMENHANG DREIGINGEN

De uitgelichte trends staan niet op zichzelf, maar hangen vaak samen met andere dreigingen. In het figuur is met lijnen aangegeven welke dreigingen onderling samenhangen.

Andere dreigingen:

- a. Spionage
- b. Hacktivisme
- c. Identiteitsfraude
- d. Manipulatie van data
- e. Verkrijging en openbaarmaking van informatie
- f. Capaciteitstekort
- g. AI voor verdedigen
- h. Geopolitiek
- i. Awareness en gedrag



WAT KUN JE DOEN?

De basis op orde

De vijf algemene basisprincipes blijven essentieel om je te beschermen tegen de cyberdreigingen en de schade van incidenten te beperken.

► [Naar de vijf basisprincipes](#)

Direct aan de slag?

Op het SURF Security Expertise Centrum vind je praktische handreikingen en diverse templates waarmee je direct aan de slag kunt.

► [Naar het Security Expertise Centrum](#)

Specifieke maatregelen bij de trends in 2026

1. Patch je systemen sneller en gericht

Breng systemen en kwetsbaarheden in kaart en richt assetmanagement in om prioriteiten te bepalen. Gebruik een slim patchproces dat rekening houdt met de ernst van kwetsbaarheden en het belang van de systemen.

2. Bereid je encryptie voor op quantumcomputers

Inventariseer welke encryptietechnieken je instelling gebruikt en stap op basis van risico-afwegingen geleidelijk over naar versleutelingsmethoden die bestand zijn tegen toekomstige quantumcomputers (quantumveilige cryptografie).

3. Breng library's in de softwareketen in kaart

Inventariseer welke library's je instelling gebruikt, zodat je bij kwetsbaarheden snel kunt handelen. Een handig hulpmiddel hierbij is een Software Bill of Materials (SBOM), een ingrediëntenlijst van software.

4. Beveilig je cyber-fysieke systemen (OT)

Breng je cyber-fysieke systemen in kaart en breng ze onder in aparte netwerksegmenten. Gebruik bijvoorbeeld [dit template](#) om de beveiliging van je OT-systemen te beoordelen.

5. Versterk je digitale autonomie

Investeer tijd en geld in innovatieve projecten en alternatieven die de afhankelijkheid van niet-Europese technologie verkleinen en je digitale weerbaarheid versterken.

6. Detecteer en voorkom misbruik van residential proxies

Monitor je netwerk op residential proxies en gebruik de dreigingsinformatie van [SURFcert](#). Volg meldingen zo snel mogelijk op, installeer kosteloos [DNS Firewall](#) om malware-infecties te blokkeren en maak medewerkers en studenten bewust van dit risico.

VAN INDIVIDUELE NAAR GEZAMENLIJKE WEERBAARHEID

Cyberweerbaarheid stopt niet bij de grenzen van je instelling. Door binnen de sector samen te blijven werken en onze kennis, expertise en voorzieningen met elkaar te delen, kunnen we dreigingen sneller signaleren en effectiever reageren. Voorbeelden van gezamenlijke cyberweerbaarheidsvoorzieningen zijn SURFcert, SURFsoc, SURF Vendor Compliance, het Security Expertise Centrum en de beveiligings-community's SCIRT en SCIPR.

Verder slaat de sector de handen ineen met investeringen in de AI-fabriek en Nextcloud, wat bijdraagt aan digitale autonomie van de sector. De crisis rondom leerlingmanagementsysteem Canvas in 2026 liet zien dat de sector nog kan versterken op het gebied gezamenlijk crisismanagement. Verder werken we aan het uitbreiden van de SURF-dienstverlening met securitytoetsen en risicomanagement op sectorale- en ketenafhankelijkheden en op het gebied van technische weerbaarheid.

Zo versterken we samen de digitale weerbaarheid van onderwijs en onderzoek.



Copyright

Deze publicatie is beschikbaar onder de licentie
Creative Commons Naamsvermelding 4.0 Internationaal.
[Creativecommons.org/licenses/by/4.0/deed.nl](https://creativecommons.org/licenses/by/4.0/deed.nl)

Oktober 2026

SURF**SURF cybersecurity-dashboard**

Actueel overzicht trends en dreigingen

Op het SURF cybersecurity-dashboard vind je een actueel overzicht van dreigingen en trends in onderwijs en onderzoek. Het dashboard is alleen toegankelijk voor leden van de SURF Community voor Informatiebeveiliging en PRivacy (SCIPR).

► [Naar het SURF cybersecurity-dashboard](#)
(inloggen met SURFconext)

