Debat voorbereiding Firewall Force

ATIX Cybersecurity Fundamentals 2025-26 P3

Groepsnummer: **10**

Groepsnaam: **Firewall Force**

Groepsleden: **Bavli, Jonas, Lucas, Vo**

Inhoudsopgave

1. Gevolgen van incidenten

1a. Welke impact hebben incidenten op individuen (privacy, financiële schade, reputatie)?

- **Privacy:** Persoonsgegevens kunnen uitlekken of misbruikt worden (bijvoorbeeld reserveringsgegevens, inloggegevens of gezondheidsgegevens). Dit kan leiden tot identiteitsfraude of gerichte oplichting.
- **Financiële schade:** Slachtoffers kunnen direct geld verliezen door fraude of indirecte kosten krijgen (bijvoorbeeld door het blokkeren van accounts, nieuwe documenten aanvragen of extra beveiligingsmaatregelen).
- **Reputatie:** Bij incidenten kunnen mensen reputatieschade ervaren als hun gegevens in verkeerde handen vallen of als zij als “slachtoffer” herkenbaar worden.
- **Indirecte effecten (psychologisch):** Stress, schaamte, angst en wantrouwen richting digitale communicatie komen vaak voor, vooral wanneer incidenten persoonlijk raken of gevoelig zijn (zoals zorggegevens).

1b. Welke impact op organisaties (continuïteit, juridische claims, reputatieverlies)?

- **Continuïteit:** Systemen en processen kunnen uitvallen, waardoor dienstverlening stopt of vertraagt. Dit leidt tot workarounds, backlogs en productiviteitsverlies.
- **Financiële impact:** Kosten door herstelwerk, incident response, externe specialisten, compensatie, omzetverlies en eventuele boetes.
- **Juridisch:** Mogelijke gevolgen rond privacywetgeving (bijvoorbeeld AVG), meldplichten, contractbreuk, claims of aansprakelijkheid.
- **Reputatieverlies:** Verlies aan vertrouwen bij klanten, partners en medewerkers; reputatieschade kan langer doorwerken dan de technische storing.

1c. Welke impact op de maatschappij (vertrouwen in digitale systemen, afhankelijkheid van technologie, publieke veiligheid)?

- **Vertrouwen in digitale systemen:** Incidenten zorgen voor afnemend vertrouwen in e-mail, digitale dienstverlening en online transacties.
- **Afhankelijkheid van technologie:** Grote incidenten laten zien dat veel sectoren afhankelijk zijn van digitale ketens en leveranciers; uitval bij één partij kan breed doorwerken.
- **Publieke veiligheid:** In kritieke sectoren (zoals zorg) kan digitale verstoring maatschappelijke ontwrichting veroorzaken, omdat dienstverlening direct raakt aan welzijn en veiligheid.
- **Indirecte effecten:** Normalisering van cybercrime (mensen verwachten fraude), hogere maatschappelijke kosten (extra controles, verzekeringen, herstel) en meer druk op organisaties om “digitaal weerbaar” te worden.

1d. Opdracht: minimaal drie echte incidenten (actualiteit) en analyseer gevolgen op drie niveaus (incl. indirecte effecten)

Incident 1: Van der Valk (Nederland, september 2025) – phishing bij medewerkers en klantfraude

Wat gebeurde er

- Medewerkers trapten in phishing via een nagemaakte inlogpagina.
- Aanvallers gebruikten reserverings- en klantgegevens om gasten gericht te benaderen.
- Doel was het stelen van betaalgegevens en het plegen van fraude.

Gevolgen voor individuen

- Financieel: slachtoffers kunnen geld verliezen door gerichte fraude.
- Privacy: reserveringsgegevens en persoonsgegevens worden misbruikt voor geloofwaardige oplichting.
- Indirect: stress, schaamte en wantrouwen richting “officiële” berichten.

Gevolgen voor organisaties

- Continuïteit: extra werkdruk door veel klantcontact en herstelacties.
- Reputatie: vertrouwen is cruciaal in hospitality; reputatieschade kan blijven hangen.
- Juridisch: mogelijke verplichtingen/risico’s onder de AVG, afhankelijk van aard en omvang.

Gevolgen voor maatschappij

- Digitale fraude wordt normaler en geloofwaardiger door misbruik van echte gegevens.
- Algemeen vertrouwen in digitale communicatie daalt.

Incident 2: Change Healthcare (Verenigde Staten, februari 2024) – ransomware en zorgketenstoring

Wat gebeurde er

- Een ransomware-aanval legde systemen van een grote zorg-IT ketenpartij plat.
- Processen zoals declaraties en farmaceutische dienstverlening werden verstoord.
- De verstoring werkte door naar veel zorgverleners en apotheken.

Gevolgen voor individuen

- Zorgimpact: vertragingen bij recepten en zorgprocessen.
- Privacyrisico: mogelijk risico op uitlek van gevoelige gezondheidsgegevens.
- Indirect: angst en stress omdat zorg direct raakt aan welzijn.

Gevolgen voor organisaties

- Continuïteit: handmatige workarounds en backlogs.
- Financieel: declaraties en cashflow komen onder druk.
- Reputatie/vervolgschade: losgeld, lekdreiging en langdurige verstoring vergroten schade.

Gevolgen voor maatschappij

- Zorg is een kritieke sector; uitval van één schakel kan brede ontwrichting geven.
- Vertrouwen in digitale zorgprocessen en ketens daalt.

Incident 3: CrowdStrike update-incident (wereldwijd, 19 juli 2024) – fout in update en massale IT-uitval

Wat gebeurde er

- Een fout in een beveiligingsupdate veroorzaakte wereldwijd Windows-crashes.
- Veel organisaties vielen tegelijk uit, zonder dat er een 'hack' nodig was.
- Microsoft schatte dat ongeveer 8,5 miljoen apparaten getroffen waren.

Gevolgen voor individuen

- Indirecte schade: diensten vallen weg (bijvoorbeeld reizen, zorg, betalingen), waardoor stress en onzekerheid ontstaan.

Gevolgen voor organisaties

- Continuïteit: downtime door tooling-update; medewerkers en systemen kunnen niet werken.
- Herstelkosten: massaal herstelwerk, noodprocedures en reputatieschade.

Gevolgen voor maatschappij

- Dit laat zien dat beschikbaarheid ook onderdeel is van security; één fout kan wereldwijd ontwrichten.
- Vertrouwen in digitale infrastructuur en grote leveranciers kan dalen.

---

2. Maatregelen

2a. Onderzoek welke soorten maatregelen zijn er (technisch, organisatorisch, procesmatig, mensgericht).

- **Technische maatregelen:** Multi-factor authenticatie, patching, endpoint-detectie, netwerksegmentatie, back-ups, logging en monitoring.
- **Organisatorische maatregelen:** Beleid, rollen en verantwoordelijkheden, leveranciersmanagement, awareness-programma.
- **Procesmatige maatregelen:** Incident response plan, change management, periodieke toegangsevaluaties.
- **Mensgerichte maatregelen:** Training, securitycultuur, heldere communicatie, melden zonder schaamte.

2b. Weeg af: welke kosten, beperkingen of weerstand kunnen maatregelen oproepen? Waarom kiezen organisaties soms niet voor de veiligste optie?

- **Kosten:** Monitoring, redundantie, tooling (zoals EDR/SIEM), training en beheer kosten geld en capaciteit.
- **Beperkingen en gebruiksgemak:** Extra inlogstappen, strengere toegangsrechten en beperkingen (bijv. minder flexibiliteit) kunnen als hinderlijk worden ervaren.
- **Weerstand en cultuur:** Medewerkers kunnen security zien als "lastig" of "tijdrovend", vooral als het nut niet zichtbaar is of als maatregelen niet aansluiten bij het werk.
- **Complexiteit en legacy:** Oude systemen, afhankelijkheden en integraties maken verbetering lastig en risicovol om te wijzigen.
- **Waarom niet de veiligste optie:** Organisaties kiezen soms voor een middenweg omdat ze balans zoeken tussen veiligheid en bedrijfsvoering. Als maatregelen te veel frictie geven, is de kans groter dat ze worden omzeild en ontstaat schijnveiligheid.

2c. Welke maatregelen zijn effectief tegen jullie gekozen incidenten?

- **Tegen phishing en klantfraude (Van der Valk):**
    - Sterke inlogbeveiliging (phishing-resistente multi-factor authenticatie, conditionele toegang).
    - Bewustwordingstraining, phishing-simulaties, meldknop en meldcultuur.
- **Tegen ransomware en ketenstoring (Change Healthcare):**
    - Segmentatie, streng rechtenbeheer en privileged access management.
    - Back-ups en herstel-oefeningen, bij voorkeur offline of onveranderbaar waar mogelijk.
- **Tegen uitval door foutieve updates (CrowdStrike):**
    - Gefaseerd uitrollen van updates met testgroepen (canary testing).
    - Business continuity plan met fallback procedures en waar nodig redundantie.

2d. Opdracht: kies per incident minimaal 2 maatregelen, leg uit waarom passend, en welke trade-offs er zijn (kosten, gebruiksgemak, cultuur).

Incident 1: Van der Valk – twee maatregelen en trade-offs

Maatregel 1: Phishing-resistente multi-factor authenticatie en conditionele toegang

- Waarom passend: account-overname wordt veel moeilijker, ook als iemand toch op een phishinglink klikt.
- Trade-offs: extra inlogstappen en beheerlast; weerstand mogelijk omdat het “tijd kost”.

Maatregel 2: Awareness, phishing-simulaties, meldknop en meldcultuur

- Waarom passend: de aanval start bij menselijk gedrag en social engineering; sneller melden beperkt schade.
- Trade-offs: tijdsinvestering; irritatie of training-moeheid als het niet praktisch en kort wordt ingericht.

Incident 2: Change Healthcare – twee maatregelen en trade-offs

Maatregel 1: Netwerksegmentatie, streng rechtenbeheer en privileged access management

- Waarom passend: ransomware verspreidt minder makkelijk; de schadezone wordt kleiner.
- Trade-offs: complexere inrichting en beheer; processen kunnen trager worden door strengere toegang.

Maatregel 2: Back-ups en herstel-oefeningen (bij voorkeur offline of onveranderbaar)

- Waarom passend: herstel zonder losgeld wordt realistischer; downtime en impact worden kleiner.
- Trade-offs: kosten voor opslag en beheer; discipline en tijd nodig om hersteltests serieus uit te voeren.

Incident 3: CrowdStrike update-incident – twee maatregelen en trade-offs

Maatregel 1: Gefaseerd uitrollen van updates met testgroepen (canary testing)

- Waarom passend: een fout wordt eerst bij een kleine groep zichtbaar; je voorkomt massale uitval.
- Trade-offs: uitrol gaat langzamer; extra proces en monitoring zijn nodig.

Maatregel 2: Business continuity plan met fallback procedures en waar nodig redundantie

- Waarom passend: kritieke processen kunnen doorgaan als IT tijdelijk uitvalt; schade door downtime wordt kleiner.
- Trade-offs: redundantie kost geld; noodprocedures vragen onderhoud en oefening en voelen “extra” tot het misgaat.

3. Cybersecurity governance

A. Organisatie van Cybersecurity

Drie lijnen model

1e lijn = dagelijks beheer (IT'ers, systeembeheerders)

2e lijn = risico & compliance (CISO, security officers)

3e lijn = onafhankelijke controle (interne/externe audit)

Kernprocessen (wat doe je continu?)

- **Asset- en dataclassificatie:** wat hebben we, wat is kritisch/gevoelig?
- **Risicomanagement:** risico's identificeren, beoordelen, behandelen en rest-risico vastleggen.
- **Beheer van maatregelen:** organisatorisch (procedures/rollen) en technisch (controls).
- **Incidentrespons:** detectie, melding, containment, herstel, evaluatie/lessons learned.
- **Awareness en gedrag:** onboarding, periodieke training, phishing-oefeningen.
- **Continu verbeteren:** audits, management review, verbeteracties.

B. Beleid, Normen, Wetgeving & ISMS

De belangrijkste dingen:

Beleid	Bestuurlijke afspraken en richting: *wat vinden we verplicht en waarom?*
ISO 27001	Internationale norm voor het opzetten van een **ISMS** (managementsysteem)
ISO 27005	Richtlijn/methode voor **informatiebeveiligingsrisicomanagement**
AVG/GDPR	Privacywetgeving: bescherming van **persoonsgegevens**
NIS2 (2024)	EU-richtlijn voor hogere cyberweerbaarheid bij aangewezen sectoren/organisaties
ISMS	Het **systeem** waarmee je security bestuurt en continu verbetert (PDCA)

C. Hoe governance helpt om maatregelen breed geaccepteerd en ingebed te krijgen

Governance maakt maatregelen **legitiem, uitvoerbaar en duurzaam**. Concreet:

1. **Duidelijk eigenaarschap:** proceseigenaren zijn verantwoordelijk voor risico's; security adviseert; bestuur stelt kaders en escaleert waar nodig. Hierdoor is het niet "IT die iets oplegt".
2. **Besluiten op basis van risico (niet op mening):** je koppelt maatregelen aan scenario's (bv. ransomware, account takeover) en aan impact op onderwijs/onderzoek/bedrijfsvoering.
3. **Prioritering en budget:** security wordt onderdeel van jaarplannen/portfolio's, met tijd en middelen. Dat vergroot haalbaarheid en acceptatie.
4. **Standaarden + uitzonderingsproces:** duidelijke baselines (bv. MFA, patch-SLA) met een gecontroleerd "exception"-proces (motivatie, tijdelijke looptijd, goedkeuring). Dit voorkomt wildgroei.
5. **Meten en rapporteren:** KPI's/KRI's maken voortgang zichtbaar (bv. MFA-dekking, patch compliance, restore tests). Transparantie per afdeling stimuleert eigenaarschap.

6. **Verankering in processen:** security-by-design in projecten, security-eisen in inkoop, autorisatieprocessen via HR/inschrijving. Dan wordt security “normaal werk”.

D. Korte schets: hoe Avans Hogeschool cybersecurity governance kan verbeteren

1) Governance Board (structureel)
Richt een **Cybersecurity Governance Board** in (maandelijks/2-maandelijks) met: CvB-portefeuillehouder, CIO/IT-manager, CISO, FG/Privacy Officer en vertegenwoordigers van faculteiten/diensten. Taken:

- security-roadmap prioriteren en budget bewaken;
- besluiten over risicoacceptaties boven een drempel;
- KPI-dashboard bespreken en blokkades oplossen.

2) “Avans Security Baselines” (simpel en meetbaar)
Stel 6–10 niet-onderhandelbare baselines vast, bijvoorbeeld:

- **MFA verplicht** voor alle accounts (zeker extern en admin).
- **Patch-SLA** voor kritieke kwetsbaarheden (binnen X dagen) + rapportage.
- **Back-up & hersteltests** per kwartaal voor kernsystemen (aantoonbaar).
- **Centrale logging/monitoring** voor kernplatformen + alerting op verdachte logins.
- **Identity lifecycle:** snelle onboarding/offboarding, least privilege, periodieke review.
- **Leveranciersbaseline:** minimale security-eisen voor SaaS (contract, verwerker, incidentmeldingen, security-rapportages).

3) Risicomanagement per domein, centraal ondersteund
Laat faculteiten/diensten hun belangrijkste risico’s beoordelen met een vaste methode (ISO27005-achtig) en standaard scenario’s (ransomware, account takeover, datalek via delen, uitval LMS). Proceseigenaren kiezen maatregelen of accepteren rest-risico expliciet; CISO-team levert templates en begeleiding.

4) Security verankeren in projecten en inkoop

- In projecten: verplichte security-check (classificatie, DPIA indien nodig, architectuurreview).
- In inkoop: security-eisen standaard onderdeel van selectie en contract (ketenrisico’s).

5) Compact KPI-dashboard per faculteit/dienst
Bijv. % MFA, patch compliance, # high findings open > 90 dagen, phishing click/report rate, hersteltest-succes, incident doorlooptijd. Dit maakt sturing en accountability concreet.

Conclusie
Door heldere rollen, baselines, risicogedreven besluiten en een werkend ISMS kan Avans cybersecurity van “losse maatregelen” naar **bestuurbare, aantoonbare en breed gedragen** beveiliging brengen.

4. Weerstand en Acceptatie

Hoewel mensen langzaamaan wel weten wat het belang van cybersecurity is, wordt het toch nog vaak gezien als iets dat lastig is of beperkend werkt voor de gebruiker. Waarom accepteren medewerkers, het management of klanten bepaalde maatregelen niet altijd meteen?

Waarom is er weerstand? De belangrijkste factoren:

- **Gemak vs. veiligheid:** Mensen willen snel hun werk doen. Elke extra stap (zoals een lange wachtwoordzin of een extra code invullen) voelt als vertraging (vooral als het dan ook nog mis gaat). Doordat gebruikers bijvoorbeeld snel willen inloggen voeren ze een verkeerde 2FA code in. Nu moeten ze opnieuw een code opvragen en duurt het allemaal nog langer. Dit zorgt voor frustratie en uiteindelijk heeft de gebruiker een negatief gevoel bij 2FA, terwijl 2FA eigenlijk een hele toegankelijke en sterke vorm van beveiliging is.
- **Kosten:** Voor het management is cybersecurity vaak een kostenpost. Ze betalen voor software of trainingen, maar zien niet direct resultaat. Pas als het misgaat, snappen ze de waarde.
- **Gebrek aan urgentiebesef:** Veel mensen denken: "Waarom zouden hackers ons willen hebben? We zijn maar een klein bedrijf" of "Ik heb toch niks te verbergen".
- **Communicatie:** Als de IT-afdeling alleen maar in vage, technische termen praat, haakt de rest van de organisatie af omdat ze het niet interessant vinden en simpelweg ook niet begrijpen.
- **Cultuur:** Als er een cultuur is van “fouten maken mag niet” durven mensen niet toe te geven dat ze op een foute link hebben geklikt. Of mensen voelen zich juist heel onzeker om met systemen te werken als ze eigenlijk niet weten hoe ze er veilig mee om moeten gaan.

Praktijkvoorbeelden:

1. **Bijbaan in de logistiek (Gemak vs. Veiligheid):** Ik werk in een magazijn van een kleding webshop. Als ik bestellingen moet inpakken zie ik op het computerscherm bij mijn station welke artikelen bij de bestelling horen. Ik scan een artikel en dan wordt dat artikel op het scherm afgevinkt. Als ik een korte tijd niks scan springt het scherm op slot en moet er een wachtwoord van 12 tekens ingevoerd worden (door een teamleider). Althans, het is de bedoeling dat de teamleider dit doet. Omdat er targets gehaald moeten worden (snelheid is belangrijk), staat het wachtwoord inmiddels op een stukje schilderstape vastgeplakt op het scherm, zodat iedereen snel het wachtwoord in kan voeren en door kan werken. De cybersecuritymaatregel werkt hier averechts, omdat het telkens invoeren van een wachtwoord ten koste gaat van het werkproces.
2. **Studenten op Avans (Gebrek aan urgentie & Gemak):** We kennen allemaal de irritatie: je hebt over 5 minuten de deadline voor een verslag op Brightspace, en precies dan moet je inloggen met de Authenticator app op je telefoon. Je telefoon ligt beneden, of is leeg. De veiligheidsmaatregel roept frustratie op omdat het studenten in de weg zit op stressvolle momenten. Dit kan ervoor zorgen dat ze de tweestapsverificatie op andere platformen gewoon uitschakelen omdat ze er zo een negatief gevoel bij hebben.

5. Acceptatie

Hoe kunnen we de weerstand die we hierboven beschreven verminderen en zorgen dat mensen cybersecurity wel omarmen en maatregelen toepassen?

Strategieën om acceptatie te vergroten:

- **Strategie 1: Security Awareness & Gamification (Bewustwording trainen):** In plaats van saaie e-learnings en dikke handboeken, maak je veiligheid onderdeel van de dagelijkse routine op een leuke manier. Denk aan het sturen van nep-phishingmails. Klikt een medewerker? Dan krijgt die een korte, grappige video met uitleg. Meldt een medewerker de mail netjes bij de IT-helpdesk? Dan krijgen ze punten of een kleine beloning (gamification).
- **Strategie 2: Security by Design/ User Experience (UX) verbeteren:** Dit betekent dat je het veilige gedrag de standaard of de “makkelijkste optie” maakt. In plaats van mensen te dwingen elke maand een nieuw, ingewikkeld wachtwoord te bedenken, stap je over op "Single Sign-On" (SSO) of biometrisch inloggen (vingerafdruk, FaceID, of een pasje scannen). De techniek lost het probleem op de achtergrond op, zodat de gebruiker er zo min mogelijk last van heeft.

Beoordeling: Welke is het meest effectief?

Strategie 2 (UX verbeteren & Security by Design) zou het meest effectief zijn. Mensen zijn van nature geneigd om de weg van de minste weerstand te kiezen. Je kunt medewerkers nog zo veel trainen (Strategie 1), maar als een veiligheidsproces irritant blijft, zullen ze in stressvolle situaties toch proberen het systeem te omzeilen zoals bij het voorbeeld uit het magazijn.

Natuurlijk is bewustwording (Strategie 1) altijd nodig omdat menselijke fouten blijven bestaan, maar de basis moet zijn dat veilig werken geen extra moeite mag kosten. Maak veiligheid onzichtbaar en makkelijk, dan verdwijnt de weerstand vanzelf. Dit toont aan dat cybersecurity geen bijzaak of belemmering hoeft te zijn, maar gewoon bij het proces hoort.

6. Bedreigingen & kansen

a. Welke actuele dreigingen zijn er?

Actuele dreigingen die structureel terugkomen: Phishing & social engineering (spearphishing, smishing, nep-loginpagina’s, CEO-fraude).Gestolen inloggegevens / identity attacks (password spray, credential stuffing, token theft).Ransomware & afpersing (encryptie + datadiefstal/double extortion).Misbruik van kwetsbaarheden (vooral internet-facing systemen).Edge devices als doelwit (VPN/firewalls/gateways) omdat ze direct aan het internet hangen. Supply chain/third-party risico (leveranciers, SaaS, IT-dienstverleners).DDoS/beschikbaarheidsaanvallen (verstoring van websites/portalen).Insider threats (opzettelijk of per ongeluk: verkeerd delen, misconfiguraties).AI-misbruik (snellere/realistischere phishing, meer automatisering).ENISA noemt in het EU-dreigingsbeeld dat threats against availability bovenaan staan en dat ransomware en datagerelateerde dreigingen daarna volgen.

b. Hoe groot is de kans dat een organisatie geraakt wordt, hoe kan je die kans reduceren?

Kans is hoog als:

veel medewerkersaccounts en cloudapps bestaan zonder sterke MFA, patching traag is op internet-facing systemen, leveranciers kritieke processen draaien (ketenafhankelijkheid), logging/monitoring beperkt is (aanvallen blijven langer onopgemerkt), back-ups niet getest zijn (herstel duurt lang of faalt).

Kans reduceren doe je door (1) initial access te blokkeren en (2) impact te beperken als het toch misgaat:

1. Identity harden: phishing-resistente MFA (FIDO2/WebAuthn), least privilege, conditional access.
2. Patch & hardening: focus op internet-facing systemen en edge devices; snelle patch-SLA's.
3. Detectie/response: centrale logging + EDR/XDR, incident playbooks en oefenen.
4. Resilience: segmentatie en immutable/offline back-ups + periodieke restore-tests.

c. Drie dreigingen: inschatting waarschijnlijkheid & impact (met incidenten)

Dreiging 1 — Phishing & gestolen inloggegevens (Identity attacks)

Wat is het?
Medewerkers worden misleid om te klikken/in te loggen, of aanvallers misbruiken gelekte wachtwoorden en proberen op schaal accounts (password spray). Vaak de start van fraude, datadiefstal of ransomware.

Onderbouwing: Microsoft geeft aan dat 97% van de aanvallen spray attacks zijn op wachtwoord

Waarschijnlijkheid: Zeer hoog
Impact: Middel → Hoog (van mailboxmisbruik tot datalek/fraude/toegang tot kernsystemen)

Incidentvoorbeeld (NL) – Van der Valk (sept 2025)
Bij twee Van der Valk-hotels klikten medewerkers op een phishinglink; daarna werden gasten met reserveringsinformatie gericht opgelicht. Dit laat zien dat phishing niet alleen "IT-schade" is, maar direct leidt tot financiële schade en reputatieverlies.

Hoe reduceer je de kans? 1. Phishing-resistente MFA (FIDO2/WebAuthn) en legacy auth uitschakelen. 2. Conditional access + least privilege (risicovolle logins blokkeren, minimale rechten). 3. Awareness met simulaties + meldknop + snelle opvolging (gedragsverandering meetbaar maken).

Dreiging 2 — Ransomware (afpersing + verstoring)

Wat is het?
Ransomware is vaak "double extortion": versleuteling én datadiefstal. De grootste schade is doorgaans beschikbaarheid: processen vallen uit (onderwijs, planning, HR/financiën).

Onderbouwing: ENISA plaatst ransomware hoog in het dreigingslandschap en koppelt dit aan "threats against availability".
In Nederland noemt NCSC in het Cybersecuritybeeld 2025 dat Project Melissa in 2024 minimaal 121 unieke ransomware-incidenten registreerde.

Waarschijnlijkheid: Hoog
Impact: Zeer hoog (uitval, herstelkosten, mogelijk AVG-meldingen, reputatie)

Incidentvoorbeeld (NL/onderwijs-keten) – Iddink (april 2024)
Iddink getroffen door een cyberaanval; er is gesproken over ransomware en mogelijk zijn persoonsgegevens buitgemaakt. Dit is relevant als ketenincident: één leverancier kan veel scholen/leerlingen raken.

Hoe reduceer je kans/impact? 1. 3-2-1 back-ups, bij voorkeur offline/immutable, plus restore-tests (werkt herstel echt?). 2. Segmentatie + beperken adminrechten + EDR/XDR (laterale beweging beperken, sneller detecteren). 3. Patchmanagement met prioriteit op internet-facing systemen/remote access.

Dreiging 3 — Kwetsbaarheden/edge devices & supply chain (third-party)

Wat is het?
Aanvallers misbruiken kwetsbaarheden in internet-facing systemen (servers, VPN, firewalls) of komen via leveranciers binnen. Edge devices zijn extra aantrekkelijk omdat ze direct bereikbaar zijn vanaf externe netwerken.

Onderbouwing: NCSC legt uit dat edge devices aantrekkelijke doelwitten zijn omdat ze direct bereikbaar zijn.
ENISA positioneert kwetsbaarheden en ketenrisico's als belangrijke componenten in het dreigingslandschap.

Waarschijnlijkheid: Middel → Hoog (afhankelijk van patchdiscipline/asset-inzicht/leveranciers)
Impact: Hoog (snelle escalatie, brede compromittering, moeilijk te detecteren)

TU Eindhoven (jan 2025): *TU Eindhoven haalde het netwerk offline na een cyberaanval; er was geen onderwijs mogelijk en mail/studiemateriaal was beperkt toegankelijk. Latere berichtgeving meldde dat een hacker dagenlang toegang had gehad, en dat onderwijs een week grotendeels plat lag.*

Hoe reduceer je de kans? 1. Asset & exposure management: weten wat internet-facing is, hardening, lifecycle management. 2. Vulnerability management met SLA's: kritieke patches snel + compensating controls (isolatie/WAF). 3. Third-party risk management: eisen in contracten (logging, meldplicht, assurance), leveranciersreview, exit/fallback plan.