Auteur: Peter H.M.P. Roelofsma Full Professor Risk Management en Cybersecurity The Hague University of Applied Sciences

Tussen regel en realiteit

Cybersecurity is cruciaal voor het beschermen van infrastructuur, data en maatschappelijke systemen. Cyberrisico's, zoals datalekken en ransomware, kunnen grote schade veroorzaken. Een groeiende uitdaging is het cascade-cyberrisico, waarbij één incident een kettingreactie veroorzaakt binnen onderling verbonden systemen en organisaties.

Opmerkelijke voorbeelden van cascadecyberrisico's zijn waar te nemen in real world scenario's met wijdverbreide verstoringen veroorzaakt door ransomware-aanvallen zoals WannaCry en NotPetya, waarbij het falen van één systeem zich verspreidde over netwerken en industrieën. Dit leidde tot aanzienlijke economische en operationele schade. De SolarWinds-aanval, de Ledger-inbreuk en de Kaseya-ransomware-aanval zijn andere goede voorbeelden van dergelijke cascade-incidenten (Kruti et al., 2023; ENISA, 2023b; Oxford Analytica, 2021).

De toenemende digitalisering van activiteiten in sectoren zoals financiën, gezondheidszorg, defensie, energietransitie, stedelijke ontwikkeling en transport verergert het risicolandschap verder. Organisaties moeten de dynamische aard van deze risico's begrijpen om proactieve en effectieve cyberbeveiligingsstrategieën te ontwikkelen.

Sectie 1. Overzicht van dit document

In sectie 2 worden de tien gemeenschappelijke componenten van supplychain of cascadecyberrisico's geschetst. Sectie 3 legt de noodzaak uit van verhoogde maatschappelijke waakzaamheid met betrekking tot dit fenomeen. Sectie 4 bespreekt het 'Toren van Babel'-effect in Cascade Cyber Risk Management die een belangrijk achterliggend probleem vormt voor cascade cyber risicomanagement. Sectie 5 identificeert de vijf belangrijkste hiaten tussen regel en realiteit in cascadecyberrisicobeheer die verband houden met dit effect. Sectie 6 bespreekt de theoretische en computationele achtergrond voor het aanpakken van deze hiaten. Hierbij wordt de innovatieve AI-gebaseerde cascade-cyberrisicobeoordelingsmethode met behulp van computationele shared mental models beschreven. Sectie 7 beschrijft de methodologische benadering voor gegevensverzameling via het Cybersecurity Living Lab als de optimale uitwerking van deze aanpak. Sectie 8 schetst een narrative of change voor de toekomst van Cascade Cyber Risk Management die nodig is om de aanpak te laten slagen. Sectie 9 geeft de conclusie van dit document.

Sectie 2. Cascadecyberrisico's: componenten en implicaties

Cascadecyberrisico's verwijzen naar het domino-effect waarbij een cyberaanval op één systeem leidt tot daaropvolgende storingen in onderling verbonden systemen, met name in kritieke infrastructuur. Het Agentschap van de Europese Unie voor cyberbeveiliging ENISA (ENISA, 2023a) voorspelt dat cascade-aanvallen op de toeleveringsketen

Een groeiende uitdaging is het cascade-cyberrisico, waarbij één incident een kettingreactie veroorzaakt

in 2030 de belangrijkste cyberdreiging voor organisaties zullen worden. Recente literatuur identificeert tien belangrijke componenten van toeleveringsketen- of cascade-cyberrisico's, die elk bijdragen aan de potentiële ernst van dergelijke incidenten (Ghadge et al., 2019; Daniel et al., 2022; Paletti et al., 2021).

2.1 Onderling verbondenheid van systemen

Onderling verbonden systemen beïnvloeden elkaar, waarbij het falen van één component kan leiden tot het falen van andere. Deze onderlinge afhankelijkheid en interoperabiliteit creëert een netwerk van risico's dat snel kan escaleren. Naarmate systemen meer geïntegreerd raken, neemt de kans op systemische storingen toe.

2.2 Gedeelde kwetsbaarheden

Onderling verbonden systemen kunnen gemeenschappelijke kwetsbaarheden delen, wat betekent dat één enkele exploit meerdere systemen tegelijkertijd kan compromitteren. Het identificeren van gedeelde kwetsbaarheden is cruciaal voor organisaties om uitgebreide beveiligingsmaatregelen te implementeren.

2.3 Verschillende verspreidingsmechanismen

Risico's kunnen zich verspreiden via meerdere paden, waaronder gegevensstromen, gedeelde bronnen en services van derden. Hierdoor is het lastig om de volledige omvang van een risicogebeurtenis te voorspellen. Het begrijpen van deze mechanismen is cruciaal voor het ontwikkelen van effectieve mitigatiestrategieën. Organisaties moeten hun onderlinge afhankelijkheden in kaart brengen om potentiële verspreidingspaden beter te kunnen anticiperen.

2.4 Feedbacklussen

Feedbacklussen kunnen risico's verergeren. Deze lussen kunnen herstelpogingen belemmeren en de duur van een incident verlengen. Het herkennen van feedbackmechanismen is essentieel bij cascadecyberrisicomanagement om de veerkracht in onderling verbonden systemen te verbeteren.

2.5 Niet-lineaire effecten

De relatie tussen systeemcomponenten is vaak niet-lineair, wat betekent dat storingen kunnen leiden tot onevenredig grote gevolgen, wat risicobeoordeling en -beheer compliceert. Effectieve modelleringstechnieken zijn essentieel om deze dynamiek te begrijpen en te beperken.

2.6 Vertraagde effecten

De gevolgen van een cyberbeveiligingsincident zijn mogelijk niet direct merkbaar en leidt vaak tot vertraagde reacties die de situatie kunnen verergeren. Organisaties moeten mogelijk gevoeligere bewakingssystemen implementeren om problemen vroegtijdig te detecteren en effectiever te reageren. Het begrijpen van mogelijke vertragingen is essentieel voor het plannen van strategieën voor respons op incidenten en voor het vermijden van overreactie in het risicomanagement.

2.7 Afhankelijkheid van vertrouwen

Suboptimaal vertrouwen in andere componenten of systemen kan ertoe leiden dat organisaties potentiële kwetsbaarheden over het hoofd zien of juist overschatten. Hierdoor neemt de kans op opeenvolgende fouten toe. Het creëren van een just culture, d.i. een cultuur waarin potentiële risico's regelmatig kunnen worden beoordeeld, kan organisaties helpen deze afhankelijkheid te verminderen. Vertrouwen moet continu worden geëvalueerd in onderling verbonden omgevingen.

2.8 Complexiteit

De complexiteit van onderling verbonden systemen kan potentiële kwetsbaarheden verhullen en het moeilijk maken

om risico's effectief te identificeren en aan te pakken. Naarmate systemen evolueren, neemt de complexiteit toe, waarbij toenemende complexiteit deze uitdagingen versterkt.

2.9 Dynamische aard

De onderlinge verbondenheid van systemen verandert in de loop van de tijd, met nieuwe integraties en afhankelijkheden die zich vormen, die het risicolandschap kunnen veranderen. Continue monitoring en adaptieve governance-frameworks zijn nodig om te reageren op deze evoluerende risico's. Organisaties moeten wendbaar blijven om nieuwe uitdagingen aan te pakken zodra ze zich voordoen. De dynamische aard van onderling verbonden systemen, met evoluerende integraties en afhankelijkheden, kan het risicolandschap plotseling veranderen. Hierdoor zijn continue monitoring en adaptief bestuur noodzakelijk om opkomende risico's effectief te beheren.

2.10 Onzichtbaarheid van risico's

Cascadecyberrisico's kunnen verborgen blijven totdat ze zich manifesteren, waardoor proactief risicomanagement een uitdaging wordt. Organisaties moeten proactieve risicobeoordelingstechnieken toepassen om potentiële kwetsbaarheden te identificeren voordat ze tot incidenten leiden. Meer transparantie kan helpen bij het herkennen en aanpakken van deze onzichtbare risico's. De onzichtbaarheid van cascadecyberrisico's compliceert proactief risicomanagement, waardoor de invoering van proactieve risicobeoordelingstechnieken en meer transparantie noodzakelijk is om potentiële kwetsbaarheden te identificeren en aan te pakken.

Sectie 3. Op weg naar een geïntegreerde aanpak

De toenemende complexiteit en onderlinge verbondenheid van systemen vereisen verhoogde waakzaamheid en innovatieve technieken voor risicobeoordeling. Edward Tenner (1996) betoogt dat technologische vooruitgang risico's vaak transformeert in plaats van uitroeit, wat leidt tot onvoorziene negatieve gevolgen. Hij noemt dit het 'revenge-effect van technologische innovatie'. Dit concept van technologische wraakeffecten benadrukt de noodzaak van aanhoudende waakzaamheid bij het beschermen van de samenleving tegen de chronische en subtiele problemen die worden veroorzaakt door technologische innovatie (Tenner, 1996). Een geïntegreerde aanpak van cascade-cyberrisicomanagement is essentieel. Het revenge-effect wordt steeds belangrijker voor cyber risk management. Jazairy (2024) benadrukt het actuele belang hiervan door het integreren van cybersecurityrisicomanagement in strategisch management, waarbij cybersecurity-inspanningen worden afgestemd op bredere organisatiestrategieën om digitale activa en infrastructuur te beschermen tegen evoluerende cyberdreigingen. Melaku (2023) stelt voor om een dynamisch en adaptief cybersecurity-governancekader op te nemen om ervoor te zorgen dat beveiligingsrisico's op de juiste manier worden beheerd en organisatorische middelen worden geoptimaliseerd.

Sectie 4. Het 'Toren van Babel'-effect

De onderlinge verbondenheid van systemen vereist een gemeenschappelijke taal en verhaal om transparantie en samenwerking in de hele toeleveringsketen te bevorderen. Het ontbreken van een uniforme taal in cyberbeveiliging creëert echter aanzienlijke barrières voor effectieve communicatie, wat leidt tot het 'Toren van Babel'-effect (Dijkstra et al., 2024; ENISA, 2023b). Dit effect beschrijft de uitdagingen die worden veroorzaakt door uiteenlopende en onverenigbare terminologieën, richtlijnen, kaders en methodologieën tussen verschillende belanghebbenden, wat resulteert in miscommunicatie, inconsistente risicobeoordelingen en onsamenhangende mitigatie-inspanningen.

4.1 Behoefte aan een gemeenschappelijke taal

Het vaststellen van een gemeenschappelijke taal is essentieel om het 'Toren van Babel'-effect te overwinnen. Organisatieleiders en bestuurders dragen de verantwoordelijkheid om complexe concepten te vereenvoudigen en terminologie te gebruiken die bij alle werknemers aanslaat, ongeacht hun technische expertise. Deze aanpak verbetert het situationele bewustzijn en stelt werknemers in staat om op zinvolle wijze bij te dragen aan de cascadecyberresilience-inspanningen van de organisatie (World Economic Forum, 2017).

4.2 De rol van leiders en besturen

Leiders en bestuurders moeten ervoor zorgen dat cybersecurity is ingebed in de gehele organisatiecultuur en dat er een gemeenschappelijke taal en verhaallijn wordt vastgesteld. Zij moeten dit verhaal ook actief uitdragen. Door cybersecurity-inspanningen af te stemmen op bredere organisatiestrategieën, kunnen leiders een gedeeld begrip van de betrokken risico's en de collectieve verantwoordelijkheid voor het beperken ervan bevorderen.

Sectie 5. Misalignment tussen regels en realiteiten

Er zijn verschillende misalignments tussen regels en de realiteit in cascadecyberrisicomanagement, die effectieve cascade risicobeperking in de weg staat. Hieronder worden de vijf belangrijkste genoemd.

5.1 Rule based versus Risk based management

Cyberrisicomanagement in Nederland en de EU is sterk afhankelijk van verschillende risicokaders, wat leidt tot verwarring vanwege verschillende terminologieën en definities. Zo kan de term 'risico' meerdere interpretaties hebben, wat de afstemming van cyberbeveiligingsmaatregelen bemoeilijkt. Daarnaast kan er verwarring ontstaan over wat 'risicobereidheid' inhoudt en het benodigde niveau van veerkracht. Volgens Dijkstra et al. (2024) worstelen veel organisaties nog steeds met hun cyberrisico-identiteit en -bereidheid. De overvloed aan richtlijnen en kaders, zoals NIST, ISO en ITSRM2, verergert deze verwarring nog verder, wat vaak resulteert in een checkboxmentaliteit waarbij risicomanagers zich richten op vormen van naleving van regels in plaats van analyse van daadwerkelijke risico's in de actuele realiteit. Dijkstra en Veen stellen voor om een op risico's gebaseerde aanpak te hanteren en een routekaart voor cyberrisicobeheer te delen om deze kaders beter af te stemmen op risico's van de realiteit. Afstemming is noodzakelijk voor effectief cyberrisicobeheer en vereist gecoördineerde communicatie tussen verschillende organisatieniveaus, van CERT/CSIRT-teams tot senior management, risico-eigenaren, toezichthoudende instanties en nationale cyberbeveiligingsautoriteiten. Er is echter vaak sprake van onvoldoende afstemming in het verzamelen van informatie tussen managementteams, wat leidt tot geïsoleerde inspanningen en ineffectief risicobeheer. Het Agentschap van de Europese Unie voor cyberbeveiliging (ENISA, 2024) benadrukt het belang van gecoördineerde communicatie voor gedeeld situationeel bewustzijn, dat momenteel onderontwikkeld is.

5.2 Usability versus Cybersecurity

Er bestaat een aanzienlijk probleem in afstemming tussen cyberbeveiligingsmaatregelen en bruikbaarheid, waardoor er spanning ontstaat tussen beveiliging en gebruiksgemak. Gebruikers vinden bijvoorbeeld complexe authenticatieprocessen vaak belastend, belemmerend of stressvol, wat leidt tot frustratie en mogelijke beveiligingslekken. Onderzoek door Furnell (2024) benadrukt de uitdagingen van het bruikbaar maken van cyberbeveiliging zonder de beveiliging in gevaar te brengen. Reuter et al. (2022) benadrukken de noodzaak van transparantie en aanpasbaarheid in beveiligingsmaatregelen om de acceptatie en effectiviteit van gebruikers te verbeteren. Grobler et al. (2021) pleiten voor een mensgerichte benadering van cyberbeveiliging, met de nadruk op gebruikersgedrag en cognitieve percepties om de kloof tussen beveiliging en bruikbaarheid te dichten. Afstemming is hier ook noodzakelijk. Discrepanties tussen bruikbaarheid en beveiliging kunnen een bron van kwetsbaarheden voor systemische risico's zijn in de supplychain.

5.3 Academische opleiding versus Behoeften van de industrie

Er is een opvallende discrepantie tussen cyberbeveiligingsonderwijs en de vereisten van de industrie. Huidige onderwijsprogramma's voorzien studenten vaak niet in de praktische vaardigheden die nodig zijn op de arbeidsmarkt. Yusuf (2024) betoogt dat cyberbeveiligingscurricula moeten worden bijgewerkt om aan de eisen van de industrie te voldoen, zodat afgestudeerden vanaf dag één klaar zijn voor een baan. AlDaajeh et al. (2022) stellen voor om onderwijsprogramma's af te stemmen op nationale cyberbeveiligingsstrategieën om de vaardigheidskloof te dichten. Towhidi en Pridmore (2023) presenteren een model voor het ontwerpen van cursussen die aansluiten bij de behoeften van de industrie en benadrukken daarbij het belang van praktische, hands-on ervaring. Het is cruciaal om deze discrepantie in het veld op te lossen. Hier is afstemming nodig. Er is bovendien een groot tekort aan personeel voor cascade-cyberrisico's en zij moeten adequaat zijn uitgerust om hun missie uit te voeren.

5.4 Misalignments in de cascade supplychain

ENISA (2023b) identificeerde vier categorieën van veelvoorkomende organisatorische misalignments tussen regels en realiteit met betrekking tot supply chain risk management. Ze benadrukten verschillende kennishiaten en relateerden deze aan een supply chain risk management. Deze hiaten werden gecategoriseerd in vier opeenvolgende gebieden met 'to do'-stappen, waarbij de nadruk werd gelegd op de misalignments tussen theoretische regels en praktische realiteiten:

a) Supply Chain Risk Management:

- Begrijp de supplychain; identificeer leveranciers en aanbieders
- Begrijp de potentiële risico's voor de organisatie en voor eindklanten.

  Misalignment: Organisaties slagen er vaak niet in hun

toeleveringsketen volledig in kaart te brengen, wat leidt tot hiaten in de identificatie en het beheer van risico's

b) Beheer van relaties in de toeleveringsketen:

- Beheer de toeleveringsketen; zorg voor beleid en overeenkomsten; definieer cyberbeveiligingsvereisten
- Monitor de prestaties van leveranciers en dienstverleners; beheer wijzigingen

  Misalignment: Beleid en overeenkomsten kunnen op papier bestaan, maar de implementatie en handhaving ervan zijn vaak inconsistent, waardoor kwetsbaarheden niet worden aangepakt

c) Omgaan met kwetsbaarheden:

- Beheer kwetsbaarheden; ken uw activa; begrijp de risico's van kwetsbaarheden
- Monitor kwetsbaarheden; patch kwetsbaarheden; zorg voor een gedefinieerd onderhoudsbeleid

  Misalignment: Ondanks dat ze kwetsbaarheidsbeheerprocessen hebben, worstelen veel organisaties met tijdige patching en asset management, wat leidt tot exploiteerbare hiaten

d) Kwaliteit van producten en diensten:

- Bied veilige producten en diensten; bescherm de infrastructuur; zorg voor veilige processen
- Implementeer technische maatregelen; creëer transparantie in de toeleveringsketen; meet de kwaliteit van producten en diensten

  Misalignment: De kwaliteit en veiligheid van producten en diensten schieten vaak tekort aan de normen vanwege ontoereikende technische maatregelen en gebrek aan transparantie in de toeleveringsketen

5.5 Misalignment van theoretische kaders

Hubbard (2020) en Cremer et al. (2022) betogen dat traditionele methoden en kaders voor risicobeheer voornamelijk falen vanwege hun afhankelijkheid van kwalitatieve beoordelingen en gebrek aan kwantitatief empirisch bewijs. Kwantitatieve benaderingen zijn nodig om zich aan te passen aan de dynamische aard van cascade cyberdreigingen, waar deze tekortkomingen bijzonder uitgesproken zijn. Cascadecyberrisico-onderzoek is bovendien vaak gebaseerd op ex post facto-gegevens, verzameld nadat een incident heeft plaatsgevonden. Wat nodig is, is uitgebreide gegevensverzameling in de hele toeleveringsketen – vóór, tijdens en na cyberincidenten. Er is ook een mismatch in het begrip van wat data is. Voor wetenschappelijke doeleinden moeten kwantitatieve gegevens meetbaar, herhaalbaar en toegankelijk zijn. Om deze mismatches tussen theoretische kaders en empirische gegevensverzameling aan te pakken, is een gezamenlijke inspanning vereist om cybersecuritypraktijken voortdurend te evalueren en te verbeteren op basis van empirische systemische gegevens. Het is bijvoorbeeld cruciaal om op basis van gegevens te voorspellen welke bedrijven binnen een toeleveringsketen waarschijnlijk worden aangevallen wanneer een leverancier binnen de keten wordt gecompromitteerd. Deze voorspellende capaciteit zou betere voorbereidings- en responsstrategieën mogelijk maken, waardoor de algehele veerkracht van de toeleveringsketen tegen cascade cyberbedreigingen wordt verbeterd. Samenvattend benadrukt de huidige stand van zaken van cascade cyber risk management verschillende belangrijke kwesties:

1) De noodzaak van verhoogde waakzaamheid tegen cascade threats
2) Verwarring en inadequate afstemming tussen regels en realiteit in meerdere domeinen in dit veld
3) een gebrek aan adequate empirische gegevens

Secties 6 en 7 zullen deze uitdagingen aanpakken door oplossingen te bieden voor de vijf geïdentificeerde verkeerde afstemmingen. In sectie 6 introduceren we de theorie van het computationele gedeelde mentale modellen dat AI-gebaseerde risicobeoordelingen van cascade-risico's faciliteert. Sectie 7 schetst de onderzoeksmethodologie van de Cybersecurity Living Lab-benadering, als oplossing voor bovengenoemde problematiek, en die uitgebreide gegevensverzameling voor cascadecyberrisico's mogelijk maakt.

Sectie 6. Computationele gedeelde mentale modellen voor cascadecyberrisicobeheer

De theorie van gedeelde mentale modellen biedt een aanpak voor het aanpakken van misalignments in cascadecyberrisicobeheer. Kenneth Craik (1943) introduceerde het concept van mentale modellen als interne representaties van de externe wereld die individuen helpen om door hun omgeving te navigeren. Deze modellen zijn dynamisch en kunnen in de loop van de tijd evolueren, wat zorgt voor een betere aanpassing aan nieuwe uitdagingen (Craik, 1943).

6.1 Organisatorisch leren

Organisatorisch leren begint met individuen die hun mentale modellen aanpassen als reactie op nieuwe ervaringen. Deze kennis kan worden gedeeld via discussies, evaluaties van fouten en best practices, games of andere sociale interacties, wat leidt tot collectief leren.

Feedbackloops stellen organisaties in staat om van individuen te leren en vice versa, wat de algehele aanpassingsvermogen verbetert (Canbaloglu et al., 2022; Roelofsma et al, 2024).

6.2 Netwerkmodellering van complexe systemen

Adaptieve netwerkmodellen kunnen de complexiteit van gezamenlijk mentale modellen en organisatorisch leren weergeven. Deze modellen leggen relaties vast tussen staten en hun dynamiek, wat zorgt voor realistischere representaties van leer- en vergeetprocessen. Deze aanpak ondersteunt een beter begrip en modellering van hoe organisaties leren en zich aanpassen in de loop van de tijd (Treur, 2020; Roelofsma et al., 2024).

6.3 What-if-analyse voor cascaderisicobeoordeling

De what-if-analyse evalueert verschillende cascadecyberaanvalscenario's en hun potentiële impact op de beveiligingshouding van een organisatie en de samenleving. Met behulp van AI-technieken helpt deze analyse mogelijke toekomstige gevolgen te beoordelen onder verschillende contextuele kenmerken, waardoor het vermogen van een organisatie om zich systematisch aan te passen aan cyberrisico's en deze te beperken, wordt verbeterd (Mestour et al., 2024; Roelofsma et al 2024).

Sectie 7. De Cybersecurity Living Lab (CSyLL)-methode

Het Cybersecurity Living Lab (CSyLL)-initiatief speelt in op de behoefte aan meer afstemming in cyberbeveiliging en bovenstaande problematiek aan te pakken door gebruik te maken van het Quadruple Helix- raamwerk (Carayannis et al., 2009, 2012). Dit raamwerk integreert de academische wereld, de industrie, de overheid en het maatschappelijk middenveld om veerkrachtige beveiligingspaden samen te creëren en te ontwerpen. De Living Lab-methode omvat een adaptief kennisdelingsproces om samenwerking en innovatie te bevorderen, zodat de unieke perspectieven en expertise van elke sector bijdragen aan uitgebreide cybersecurityoplossingen.

De Living Lab-benadering integreert gedeelde mentale modellen en theorieën over organisatorisch leren om samenwerking en innovatie te verbeteren. Door gedeeld begrip en continu leren te bevorderen, streeft het Lab ernaar de effectiviteit van zijn gezamenlijke inspanningen te verbeteren (Lupp, 2021; Roelofsma et al., 2024).
Het Cybersecurity Living Lab is een experimentele werkomgeving waar studenten, onderzoekers, bedrijven, publieke instellingen en eindgebruikers samenwerken om nieuwe ideeën, producten en diensten op het gebied van cybersecurity te ontwikkelen, testen en evalueren in de praktijk. Door middel van innovatieve experimenten en onderzoek leren deelnemers effectief te reageren op cyberdreigingen en risico's te beheren.

7.1. Doelstellingen van het Cybersecurity Living Lab

Het CSyLL-initiatief heeft tot doel:

- Gegevens verzamelen: empirische gegevens verzamelen voor op bewijs gebaseerd cascade-risicobeheer
- Oplossingen samen creëren: veerkrachtige beveiligingspaden ontwikkelen met meerdere belanghebbenden
- Onderwijs verbeteren: studenten praktische ervaring bieden in cybersecurityrisicobeheer
- Onderzoek faciliteren: onderzoekssamenwerkingen mogelijk maken om innovatieve benaderingen van cybersecurity te verkennen

Het proces in het Living Lab is iteratief, met voortdurend feedback verzamelen en verbeteringen aanbrengen. Hierdoor kan het Lab innovaties ontwikkelen die aansluiten bij de behoeften en het gedrag van gebruikers in hun dagelijks leven. Living Labs richten zich op complexe maatschappelijke uitdagingen, waarbij onderzoek en duurzaamheid centraal staan. Ze bevorderen realtime leren en dichten de kloof tussen theoretisch onderzoek en praktische toepassing. Innovaties zijn hierdoor gericht op daadwerkelijke bruikbaarheid en acceptatie door de gebruiker. In het Cybersecurity Living Lab creëren de deelnemers met deze visie een leergemeenschap voor cybersecurity.

7.2 Wat gebeurt er in het Cybersecurity Living Lab?

De belangrijkste onderdelen van het Lab zijn:
Cybersecuritywerkplaats. In de cybersecuritywerkplaats werken de deelnemers met het Living Lab-concept aan de toekomst van cyberveiligheid. Zij ontwikkelen nieuwe technologieën, leermodules, AI-hulpmiddelen en meer. Realtime dreigingsmonitoring en incidentrespons. Studenten en professionals leren hoe ze effectief kunnen
reageren op cyberaanvallen met realtime dreigingsdetectie, incidentrespons en cyberrisicomanagement.
Security Operations Center (SOC). In het lab zetten de deelnemers een SOC op waar studenten en onderzoekers leren hoe ze cyberdreigingen kunnen identificeren, analyseren en aanpakken, vergelijkbaar met hoe professionele cybersecurityteams dat doen. Dit biedt hen niet alleen

praktijkervaring, maar ook de mogelijkheid om onderzoek te doen naar risicomanagementmethoden.
Onderwijs en training. Studenten en andere deelnemers doen praktijkervaring op met cybersecuritytools, zoals risicomanagementraamwerken, beveiligingssoftware, procedures voor incidentrespons en cyberwargaming. Ze leren hoe ze risico's kunnen beoordelen, monitoren en beheren, en hoe ze kunnen reageren op cyberdreigingen. Het lab biedt ook mogelijkheden voor stages, afstudeerprojecten en postdoctoraal onderzoek. In samenwerking met docenten en het bedrijfsleven streeft het Living Lab ernaar onderwijsvernieuwingen te realiseren die beter aansluiten bij de praktijk.

Toegepast onderzoek. Samen met bedrijven, onderzoekers en studenten doen we onderzoek naar innovatieve oplossingen voor cybersecurity. De onderzoeksthema's variëren van het optimaliseren van cyberrisicomanagement en het bestuderen van biases en kennisoverdracht tot het ontwikkelen van gezamenlijke mentale modellen. Daarnaast onderzoeken we het co-creatieproces met eindgebruikers, bijvoorbeeld bij systeemontwerp en authenticatie. Tot slot richten we ons op onderzoek naar beslisondersteuning, de rol van cyber management games en de inzet van kunstmatige intelligentie als hulpmiddel bij cyberrisicomanagement.

Cyber Security simulatielab. Dit is een belangrijk onderdeel van het Living Lab. In het Cyber Security simulatielab ontwikkelen de deelnemers specifieke simulaties voor cyberrisicomanagement met behulp van AI- modellen. Deze simulaties worden gebruikt voor onderwijs, productontwikkeling en onderzoek. Verbinding tussen onderwijs en bedrijfsleven. Het Living lab werkt nauw samen met bedrijven om ervoor te zorgen dat de activiteiten aansluiten bij de nieuwste security- en veiligheidsnormen, regelgeving en technologische trends. Hierdoor blijft het onderwijs relevant en up-to-date, en kunnen studenten werken met tools en gegevens die in de praktijk worden gebruikt.

Sectie 8. Een 'Narrative of Change'

In een tijdperk van toenemende cyberdreigingen realiseren organisaties zich dat ware cyberveerkracht niet in isolatie kan worden bereikt. De onderlinge verbondenheid van de digitale wereld betekent dat één kwetsbaarheid kan leiden tot cascadecyberrisico's, waarbij één inbreuk meerdere storingen veroorzaakt. Het cyberbeveiligingslandschap vereist samenwerking, gedeeld begrip en collectieve actie. Net zoals de mensen van Babel een monumentaal project begonnen, moeten wij een maatschappelijke transitie naar verbeterde cyberbeveiliging ondernemen, ondersteund door een positieve en omarmde mindset.

Het verhaal van de Toren van Babel herinnert ons aan de gevolgen van verdeeldheid en ambitie zonder gedeelde verantwoordelijkheid. De mensen van Babel wilden een grote stad en toren bouwen om roem te vergaren, maar hun gebrek aan samenwerking leidde tot verwarring en mislukking. Dit principe geldt ook voor cyberbeveiliging: echte prestaties liggen in samenwerking, niet in concurrentie. Wanneer organisaties individuele onderscheidingen boven collectieve verantwoordelijkheid stellen, volgen verwarring en fragmentatie. Cascadecyberrisicomanagement is zowel een technische als maatschappelijke uitdaging. We moeten een gedeeld mentaal model bevorderen dat organisatorische grenzen overstijgt. Door een cultuur van samenwerking en effectieve communicatie te creëren, kunnen we veerkrachtige systemen bouwen die bestand zijn tegen cyberdreigingen. Dit vereist een positieve benadering van verandermanagement en een gedeeld gevoel van doel en verantwoordelijkheid.

Sectie 9. Conclusie

Cascadecyberrisico's vormen aanzienlijke uitdagingen voor moderne organisaties, met name in kritieke infrastructuur. De onderlinge verbondenheid van systemen, gedeelde kwetsbaarheden en niet-lineaire effecten compliceren risicobeoordeling en -beheer. Een geïntegreerde aanpak, ondersteund door gedeelde mentale modellen en organisatorisch leren, is essentieel voor het verbeteren van de veerkracht tegen cascadecyberdreigingen. Het Cybersecurity Living Lab-initiatief biedt een veelbelovend raamwerk voor het aanpakken van deze uitdagingen door samenwerking tussen de academische wereld, de industrie, de overheid en het maatschappelijk middenveld te bevorderen. Door adaptieve netwerkmodellering en empirische gegevensverzameling te benutten, kunnen organisaties beter anticiperen op cascade cyberrisico's en deze beperken, wat zorgt voor een veiliger en veerkrachtiger digitaal ecosysteem.

Voor een complete lijst van referenties, kun je het artikel raadplegen dat vanaf eind april op de site van PvIB staat.