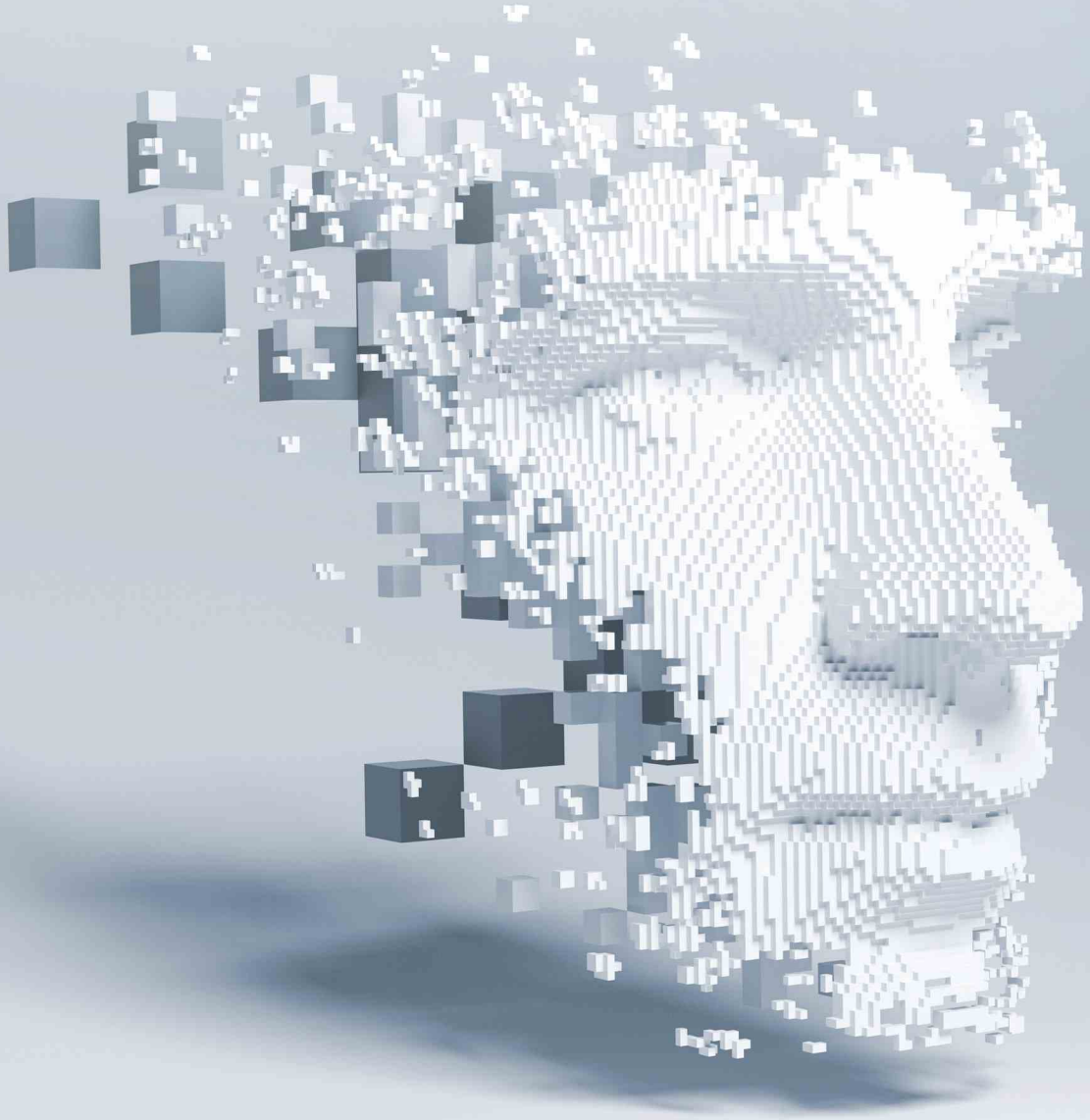
Cybercrime Trends 2024

De nieuwste bedreigingen en beveiliging best-practices



sosafe

Inhoudsopgave

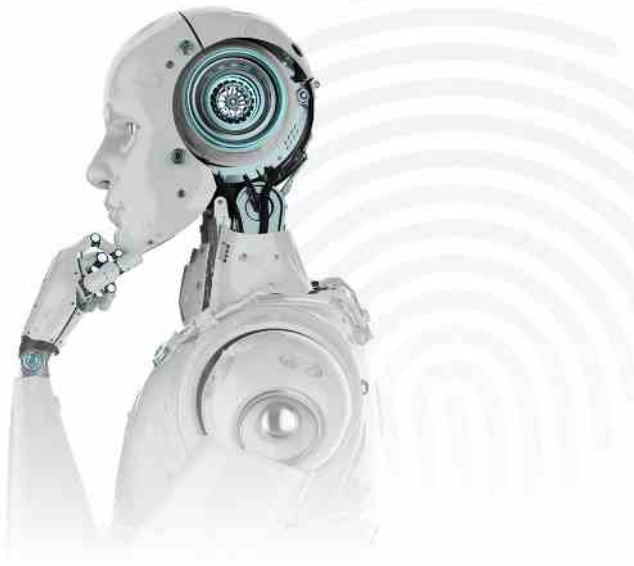
In 2023 veranderde alles. Het is tijd om je voor te bereiden op wat komen gaat.

Het jaar 2023 markeerde een keerpunt in ons wereldwijde verhaal. Sinds OpenAI de lancering van ChatGPT-3 aankondigde in november 2022, is er een golf van door AI gedreven innovatie ontstaan en heeft er een **diepgaande verschuiving plaatsgevonden in hoe we omgaan met technologie**. Deze evolutie is met name merkbaar op het gebied van informatiebeveiliging, waar AI niet alleen de verdediging van cybersecurity versterkt, maar ook de complexiteit van cyberaanvallen vergroot.

Naarmate we 2024 verder ingaan, staan we voor een opeenstapeling van uitdagingen die wordt aangedreven door een ongekend snelle technologische innovatie: de steeds grotere rol van AI in cyberaanvallen, de positieve en negatieve kanten van opkomende technologieën zoals 5G en quantum computing en de professionalisering van cybercriminaliteit tot een zeer gespecialiseerde industrie. Deze context wordt nog complexer door de opkomst van hacktivisme en cyberaanvallen te midden van mondiale politieke crises en de toename van desinformatiecampagnes. Dit alles maakt dreigingen complexer, met verstrekkende gevolgen. Tegelijkertijd strijden cybersecurityprofessionals tegen burn-out te midden van deze escalerende dreigingen.

Met de verwachting dat de kans op een **aanval als gevolg van menselijke fouten** toeneemt in dit dreigingslandschap, is een sterke beveiligingscultuur onze enige hoop. Daarom richt dit rapport zich op de acht cybercriminaliteitstrends voor 2024 en biedt het best-practice beveiligingsrichtlijnen om je beter voor te bereiden tegen een diversiteit aan cyberdreigingen.

1 Het groeiende aandeel van AI in cyberaanvallen: Een storm aan de horizon



Het wijdverbreide gebruik van AI, dat naar verwachting meer dan 300 miljoen gebruikers zal bereiken in 2024 en naar schatting 700 miljoen tegen 2030, benadrukt niet alleen de revolutie die gaande is, maar is ook aanleiding om je zorgen te maken over de bredere implicaties en veiligheidsrisico's.[1] Ook **deepfakes** en **stemklonen** passeren de revue waar het gaat om door AI getriggerde beveiligingsuitdagingen. Kwaadwillende actoren maken al enige tijd gebruik van beide technologieën, maar de recente snelle verspreiding van tools die in staat zijn om hoogwaardige deepfake-video's te produceren, maken deze technologie toegankelijker. Dat heeft op zijn beurt geleid tot een toename van het gebruik ervan, met name in **desinformatiecampagnes en sociale manipulatie**[2] (meer hierover lees je in de trend van desinformatie-as-a-service).

1 op de 4

mensen heeft **zelf een aanval met stemklonen meegemaakt** of kent iemand die hier slachtoffer van is geworden.

Bron: McAfee[3]

Ook het stemklonen neemt toe. Een recente studie bevestigt dat één op de vier mensen zelf een aanval met stemklonen heeft meegemaakt of iemand kent die hier slachtoffer van is geworden.[3] Ook het platform 'Opgelicht?!' besteedt aandacht aan voice-cloning door AI en de nieuwe mogelijkheden die dit online oplichters biedt.[4] Hoewel cybercriminelen stemklonen voornamelijk gebruiken voor financiële oplichting, waarbij sommigen zelfs een gekidnapte jonge vrouw hebben nagebootst[5], **ondermijnt men nu ook MFA-systemen op basis van stemherkenning**. Zo slaagde een journaliste er eerder dit jaar in om toegang te krijgen tot haar bankrekening met een opname van haar eigen gekloonde stem.[6] Hoewel het experiment van de journaliste geen persoonlijk risico met zich meebracht, is de bredere dreiging zeer reëel.

1 **Statista (2023).** Artificial Intelligence Worldwide.

2 **Rathenau (2022).** AI en manipulatie op sociale en digitale media.

3 **McAfee (2023).** Artificial Imposters—Cybercriminals Turn to AI Voice Cloning for a New Breed of Scam.

4 **Opgelicht?! (2023).** Voice cloning door AI geeft nieuwe mogelijkheden voor online oplichters.

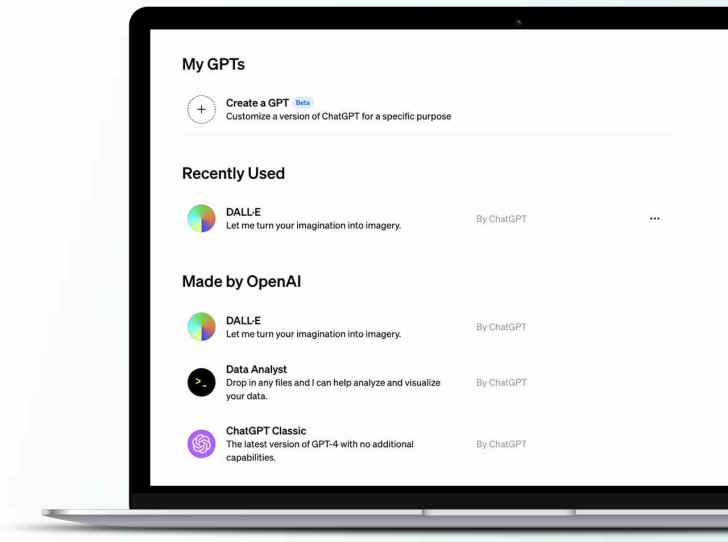
5 **CNN (2023).** 'Mom, these bad men have me': She believes scammers cloned her daughter's voice in a fake kidnapping.

Dit is echter verre van de enige manier waarop cybercriminelen AI gebruiken. Vooruitgang in generatieve AI het afgelopen jaar heeft geleid tot veel nieuwe mogelijkheden voor belangrijke tools. Sommige daarvan, zoals de recente mogelijkheid van ChatGPT om afbeeldingen te lezen, kunnen kwaadaardig worden gebruikt. Bijvoorbeeld de mogelijkheid van **promptinjectie**, wat betekent dat de tool de instructies of prompts in een afbeelding zal volgen in plaats van de instructies die de gebruiker aan de tool heeft gegeven bij het indienen van de afbeelding.[7] Hoewel dit in eerste instantie onschadelijk lijkt, zijn de mogelijkheden voor het manipuleren van gebruikers via deze tactiek oneindig.

Deze mogelijkheid om afbeeldingen te uploaden geeft ook aanleiding tot andere zorgen, zoals de mogelijkheid om **CAPTCHA-codes te omzeilen**, een van de meest bekende beveiligingen tegen oneerlijk gebruik van technologie. Tot voor kort konden hackers geen gebruikmaken van AI-technologie om CAPTCHA te lezen, voornamelijk vanwege de ethische beperkingen van de tools. Echter, Bing Chat heeft bewezen in staat te zijn deze codes te ontcijferen wanneer dit wordt gevraagd met een redelijk excuus of voorwendsel.[8] Dit is aanleiding tot zorgen bij bedrijven en websites wereldwijd over **de noodzaak om over te schakelen naar andere beveiligingsmethoden**. En naarmate de technologie vordert, **gebruiken hackers deze ook om hun eigen krachtige AI-tools te bouwen op basis van bestaande taalmodellen**. Zo verschenen kwaadaardige alternatieven voor ChatGPT, zoals FraudGPT en WormGPT.[9] Echter, tot het einde van 2023 was de creatie - niet het gebruik - van dergelijke tools beperkt tot degenen met technische kennis.

Recentelijk introduceerde OpenAI de mogelijkheid om zeer eenvoudig een GPT te creëren - een chatbot die je kunt trainen om je te helpen bij een specifieke taak op een nog toegankelijkere manier dan zijn tegenhangers op het dark web - zonder dat je enige codering of technische kennis nodig hebt. Gepersonaliseerde GPT's kunnen een waardevolle aanwinst zijn voor velen om hen te helpen bij dagelijkse werkzaamheden. Maar we kunnen er ook van uitgaan dat aanvallers **in 2024 gebruik zullen maken van de mogelijkheden om persoonlijke hackassistenten te creëren**[10] die gespecialiseerd zijn in het maken van zeer overtuigende smishing-teksten, spear phishing e-mails en polymorfe malware.[11]

Het risico dat gepaard gaat met AI kan ook voortkomen uit de **beperkingen** ervan in plaats van de mogelijkheden. De mogelijkheid van geavanceerde AI-modellen om code te schrijven is een significante vooruitgang, wijdverspreid overgenomen door tot wel 92% van de ontwikkelaars, zowel binnen als buiten de werkplek.[12] Er rijzen echter zorgen over



6 **The Wall Street Journal (2023).** I Cloned Myself With AI. She Fooled My Bank and My Family.

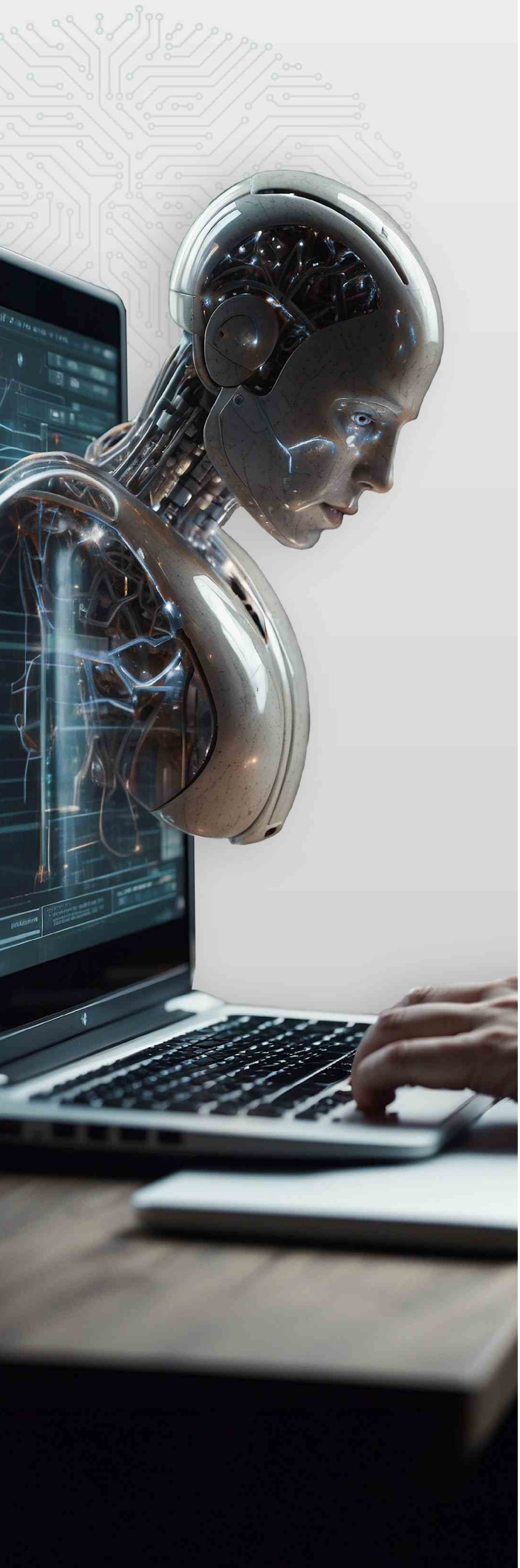
7 **Windows Central (2023).** GPT-4 Vision: A breakthrough in image deciphering unveils potential for 'prompt injection attacks'.

8 **AI Boom (2023).** Bing Chat misleid: Gebruiker omzeilt CAPTCHA met truc, onthult kwetsbaarheid in AI.

9 **Security Management (2023).** Check Point ziet eerste voorbeelden van door ChatGPT ontwikkelde schadelijke tools.

10 **Nu.nl (2023).** Ook criminelen gebruiken ChatGPT: 'Mogelijk begin van wapenwedloop'.

11 **HYAS (2023).** Blackmamba: Using AI to generate polymorphic malware.



de betrouwbaarheid van door AI gegenereerde code, waarbij experts wijzen op een neiging om functionaliteit boven beveiliging te plaatsen, wat resulteert in aanzienlijk verminderde betrouwbaarheid van code en de noodzaak om deze te controleren.[13] Enkele beveiligingsfouten omvatten kwetsbaarheid voor SQL-injecties, hard coded referenties en het gebruik van onveilige wachtwoord-hashing algoritmen.[14]

Maar misschien is de meest voorkomende beperking van AI een fenomeen dat **'hallucinaties'** wordt genoemd, waarbij AI valse of verzonnen informatie verstrekt. **Hackers maken nu misbruik van deze hallucinaties om toegang te krijgen tot kwaadaardige bestanden**.[15] Op verzoek van een gebruiker zal de tool 'hallucineren' en namen aanbevelen van niet-bestaande codebibliotheken. Hackers zullen vervolgens kwaadaardige codebibliotheken of pakketten maken onder die namen en ze uploaden naar openbare repositories. Op deze manier zal de volgende keer dat een van deze pakketten wordt aanbevolen, de gebruiker de kwaadaardige codebibliotheek downloaden die door de hacker is geüpload.

Gezien de opkomende bedreigingen van het gebruik van AI en het snelle tempo van technologische vooruitgang, **is het van cruciaal belang dat we robuuste methoden identificeren en implementeren om ons tegen deze bedreigingen te beschermen**. Een proactieve benadering van cybersecurity is essentieel om zowel bedrijven als individuen veilig te houden in een wereld die steeds meer door AI wordt gedreven.

12 **GitHub Blog (2023).** Survey reveals AI's impact on the developer experience.

13 **AG Connect (2023).** Na AI gegenereerde code komt AI gebaseerde check op AI codefouten.

14 **Nord Security (2023).** ChatGPT and secure coding: The good, the bad, and the dangerous.

15 **Infosecurity Magazine (2023).** New ChatGPT Attack Technique Spreads Malicious Packages.

CHECKLIST

Beveiliging best-practices

- **Controleer door AI gegenereerde code voordat je deze implementeert:** Zelfs als je de tool vraagt om veilige code te genereren, is het een goed idee om de betrouwbaarheid ervan te testen met geautomatiseerde code-reviewtools of door te werken met een gestandaardiseerde reeks beveiligingsbenchmarks.

- **Blijf op de hoogte van de laatste AI-trends en pas je beveiligingsstrategie hierop aan:** Sommige beveiligingsmaatregelen zijn mogelijk niet langer betrouwbaar naarmate de technologie zich verder ontwikkelt. Dat betekent dat je op zoek moet naar alternatieve oplossingen om je organisatie goed te blijven beschermen. Een toegewijd interventie- of intelligentieteam binnen je organisatie, gericht op het monitoren en analyseren van op AI gebaseerde aanvallen en hun impact op je beveiliging, kan een goede start zijn.

- **Gebruik AI-tools op een verantwoordelijke manier:** Vermijd het invoeren van persoonlijke gegevens en vertrouw niet uitsluitend op de informatie die AI-tools je verstrekken. Bedenk dat sommige antwoorden onjuist of verouderd kunnen zijn en het nooit verkeerd is om de integriteit van de informatie te controleren.

- **Maak gebruik van AI om je beveiliging te versterken:** Het werken met van op AI gebaseerde tools kan de analyse van grote hoeveelheden gegevens aanzienlijk verbeteren. Daarmee versterk je de detectie van afwijkingen en maak je identificatie van bedreigingen in realtime efficiënter. Door AI te integreren met SOAR (Security Orchestration, Automation and Response) kunnen we geautomatiseerde, intelligente besluitvorming en reactieve incidentafhandeling realiseren. Daarnaast is het gunstig om op AI gebaseerde geavanceerde authenticatiesystemen te implementeren, die voortdurend leren en beveiligingsmaatregelen verbeteren. Met consistente menselijke controle zorg je ervoor dat zij in lijn blijven met je beleid en ethische overwegingen.

- **Wees op je hoede voor verdachte spraak- of videoboodschappen:** Zelfs al lijken ze authentiek, als de boodschappen ongebruikelijke verzoeken of verdachte verklaringen bevatten, is het raadzaam om ze via alternatieve middelen te verifiëren.

- **Informeer je medewerkers over de beveiligingsdreigingen die AI kan veroorzaken:** Als je medewerkers weten hoe ze zichzelf en jouw organisatie tegen bedreigingen kunnen beschermen, dan zijn zij je beste verdedigingslinie. Leer ze ook hoe ze op verantwoorde wijze generatieve AI moeten gebruiken om gevoelige gegevens te beschermen.

2 Voorbij AI: Alle nieuwe technologieën worden uitgebuit door cybercriminelen

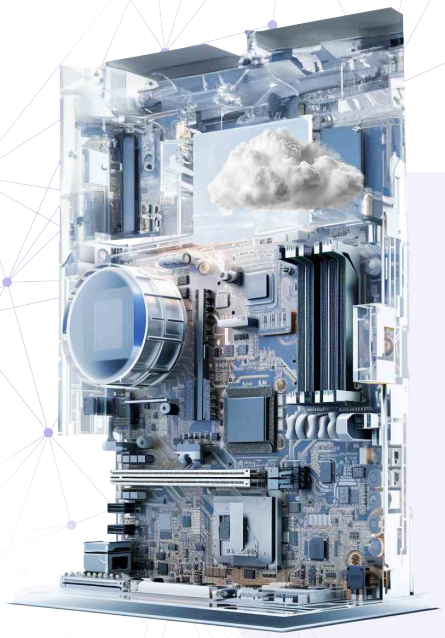
Ook al is het de innovatie van de eeuw, cybercriminelen richten zich niet alleen op kunstmatige intelligentie. Ze **verbreden hun horizon** om een scala aan opkomende technologieën uit te buiten. Het doel is om het aanvalsoppervlak te vergroten en hun bereik zo groot mogelijk te maken. Daarom wordt elke nieuwe **technologie zowel een hulpmiddel als een doelwit** voor geavanceerde cyberdreigingen.

Deze trend is echter niet helemaal nieuw, zoals we eerder hebben gezien met andere opkomende technologieën zoals **cloudtechnologie**. In de afgelopen jaren hebben bedrijven miljarden dollars geïnvesteerd in cloudopslag en zijn ze afgestapt van traditionele oplossingen voor opslag van gegevens. Natuurlijk is deze overgang niet onopgemerkt gebleven bij cybercriminelen. Volgens het CrowdStrike Global Threat Report zijn aanvallen gericht op cloudsystemen bijna verdubbeld in 2022.[1] En het aantal hackergroepen dat dergelijke aanvallen kan uitvoeren, zal verdrievoudigen.

De ransomware-aanval in Sri Lanka begin augustus 2023 was een duidelijke illustratie hiervan.[2] Kwaadwillende actoren drongen het cloudsysteem van de Sri Lankaanse overheid binnen door geïnfecteerde links onder overheidsmedewerkers te verspreiden. Met de aanval werd vier maanden aan overheidsgegevens uitgewist omdat het cloudsysteem van het land geen back-updiensten had.

En nu wacht opkomende technologieën zoals **quantum computing** een zelfde lot. Een belangrijk concept is 'nu oogsten, later decoderen' (harvest now, decrypt later - HNDL), waarbij cybercriminelen vandaag versleutelde gegevens verzamelen in de verwachting dat toekomstige ontwikkelingen in quantum computing hen in staat zullen stellen deze te decoderen, met mogelijk ongekende schendingen van de privacy, diefstal van intellectueel eigendom en onthulling van nationale veiligheidsgeheimen als gevolg.[3]

Het National Cyber Security Centre van het VK was zich in 2020 al bewust van dit probleem toen het een whitepaper met advies schreef over hoe over te stappen op quantum-bestendige algoritmen en het belang van het vroegtijdig starten van dit proces om beveiliging tegen potentiële dreigingen van quantum computing te waarborgen.[4] De onzekerheid over het tijdschema voor doorbraken in quantum computing creëert een complex risicolandschap.



1 **Dutch IT Channel (2023).** CrowdStrike Global Threat Report onthult opkomende dreigingsactoren.

2 **Infosecurity Magazine (2023).** Ransomware attack wipes out Sri Lankan government data.

3 **Security Management (2021).** Risico's en kansen van quantumcomputers: Nachtmerrie of droomscenario?

4 **National Cyber Security Centre (2020).** Preparing for quantum-safe cryptography.

Hierbij wegen organisaties de kosten van het vroegtijdig aannemen van quantum-bestendige maatregelen af tegen het risico onvoorbereid te zijn op een plotselinge vooruitgang in de mogelijkheden van quantum computing.

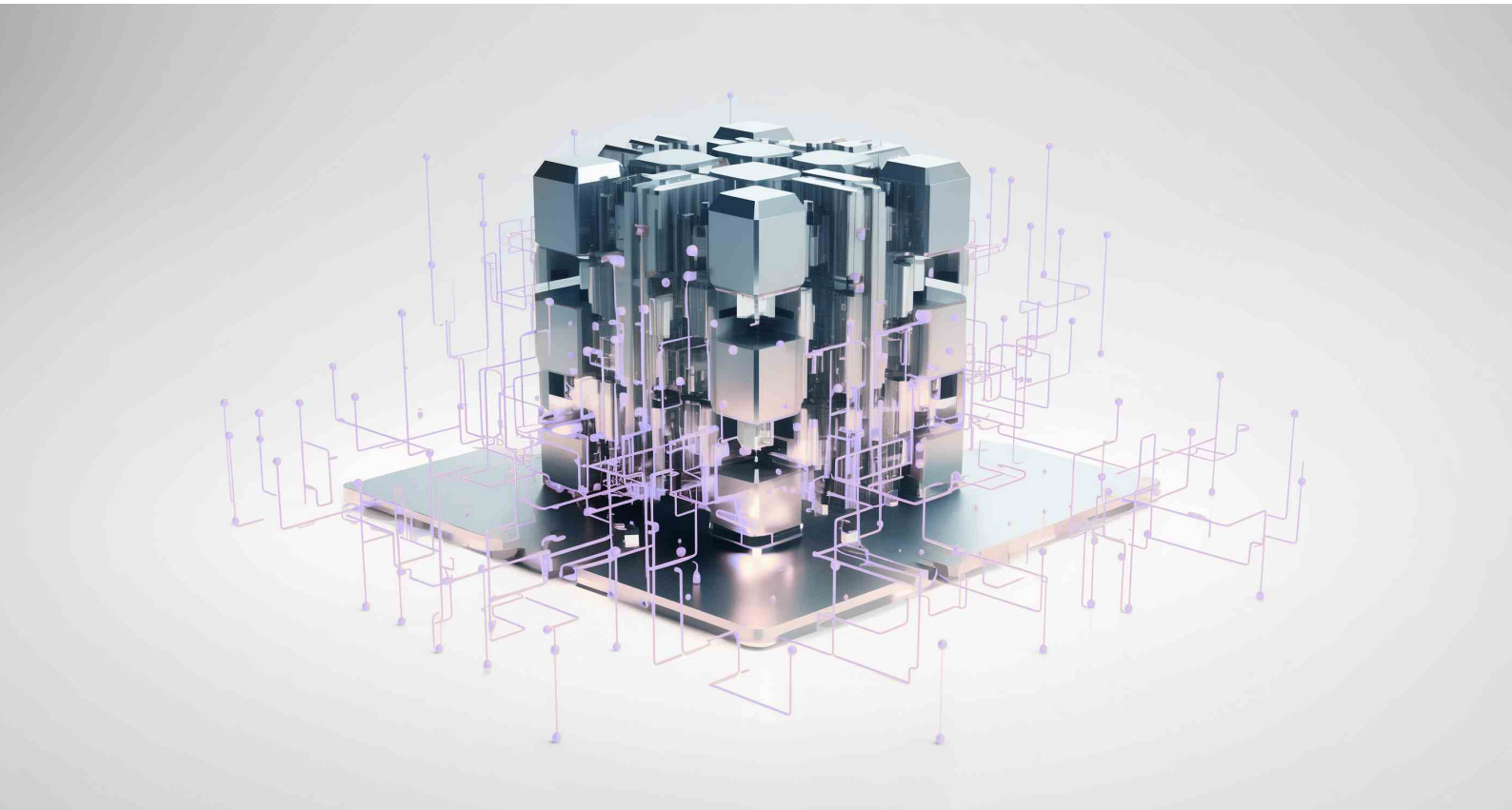
5G-technologie is een ander voorbeeld van hoe nieuwe technologieën een positieve en negatieve kant hebben. Er worden aan de ene kant ongekende connectiviteit en snelheid beloofd, maar tegelijkertijd kunnen deze nieuwe mogelijkheden ook door cybercriminelen worden uitgebuit. PriceWaterhouseCoopers identificeert de volgende cybersecurity uitdagingen van 5G: het ontstaan van nieuwe supply chains en grote afhankelijkheid van softwareleveranciers, een veelvoud aan devices en de data die gebruikmaken van 5G en vervanging van het 'core' netwerk om nieuwe functionaliteiten aan te bieden (network slicing).[5]

De Amerikaanse Cybersecurity and Infrastructure Security Agency (CISA) identificeert de volgende risico's in verband met 5G: verhoogde kwetsbaarheden als gevolg van complexe netwerkontwerpen en lokale 5G-implementaties; bedreigingen van de toeleveringsketen door kwaadaardige hardware en software; geërfde zwaktes van verouderde infrastructuur en onbetrouwbare componenten; beperkte marktconcurrentie wat leidt tot afhankelijkheid van mogelijk onveilige in eigen beheer ontwikkelde oplossingen en een uitgebreid aanvalsoppervlak met nieuwe kwetsbaarheden en een verhoogd risico op gegevensinbreuken als gevolg.[6]

Al deze vooruitgang maakt een ding duidelijk: naarmate **nieuwe technologieën blijven evolueren, doen de methoden en doelen van cybercriminelen dat ook**. Het is een constante race, waarbij elke nieuwe technologische ontwikkeling een nieuwe mogelijkheid biedt voor uitbuiting. Flexibele en adaptieve cybersecurity strategieën kunnen meebewegen met de technologische vooruitgang en op die manier de potentiële dreigingsrisico's die hierdoor ontstaan verminderen.

5 **PWC (2020).** Cybersecurity in een 5G-wereld is een probleem. Dit kunt u eraan doen.

6 **CISA (2023).** 5G Security and Resilience.



CHECKLIST

Beveiliging best-practices

- **Versterk cloudbeveiliging:** Investeer in uitgebreide back-up- en herstelsystemen voor cloudopslag en zorg voor een routine van regelmatige updates en patches om je te beschermen tegen veranderende dreigingen.
- **Minimaliseer het risico op datalekken:** Gebruik microsegmentatie om gegevens te beschermen, roteer versleutelingssleutels regelmatig op basis van gegevensclassificatie en zorg ervoor dat software en beveiligingsmaatregelen consequent worden bijgewerkt.
- **Ga voor een crypto-agile aanpak:** Wees bereid om snel over te schakelen naar algoritmes en cryptografische methoden wanneer nieuwe dreigingen zich voordoen.
- **Beveilig 5G-netwerken:** Pak kwetsbaarheden aan in complexe netwerkontwerpen en lokale implementaties en zorg voor de beveiliging van de toeleveringsketen, inclusief hardware- en softwarecomponenten.
- **Beperk kwetsbaarheden van verouderde infrastructuur:** Upgrade of vervang verouderde systemen die inherente beveiligingsfouten kunnen hebben en neem beveiligingsoverwegingen op in het ontwerp van nieuwe technologieën.
- **Hou opkomende dreigingen in de gaten en pas je hierop aan:** Blijf op de hoogte van opkomende cyberdreigingen, pas strategieën hierop aan en implementeer continue monitoring en realtime dreigingsanalyse.
- **Versterk de cyberbeveiligingsvaardigheden van je team:** Net als bij de AI trend, zal doorlopende training en bijscholing voor zowel je beveiligingsteam als de rest van je medewerkers hen voorbereiden zodat ze snel kunnen reageren en zich aan kunnen passen aan nieuwe bedreigingen.

3 Cybercriminaliteit zal zich ontwikkelen tot een nog professionelere en winstgevendere bedrijfstak

De professionalisering van cybercriminaliteit gaat gestaag door en zal in 2024 een nieuw niveau van volwassenheid bereiken. Deze groei wordt deels aangedreven door de beschikbaarheid en uitbreiding van **ransomware-as-a-service (RaaS)**-aanbiedingen. Vorig jaar hebben we laten zien hoe deze geavanceerde tools niet alleen de toetredingsdrempel voor potentiële cybercriminelen verlaagt, maar ook een aanzienlijke verschuiving in de complexiteit en impact van aanvallen teweegbrengt.

Het afgelopen jaar heeft het dreigingslandschap zich snel ontwikkeld, in die mate dat in 2023 **het aantal slachtoffers van ransomware is verdubbeld** in vergelijking met april van het jaar ervoor.[1] Deze verontrustende toename laat zien dat ransomware **de meest schadelijke, kostbare en wijdverbreide cyberdreiging blijft voor organisaties in EMEA**.[2]

Ook in Nederland vormen ransomware aanvallen een steeds groter wordende bedreiging voor instellingen en bedrijven. In een recent rapport gepubliceerd door het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC), komt naar voren dat Nederland op plek 12 staat als het gaat om hoe vaak organisaties in dit land slachtoffer worden van ransomware groepen.[3] Dat is hoger dan grote landen als China, Japan en Mexico. De industriesector en de financiële dienstverlening worden het meest getroffen. Opvallend is een verdubbeling van het aantal aangiftes van ransomware aanvallen uit de ICT-sector in 2021 ten opzichte van 2020.

Er is ook sprake van een toenemende gerichtheid van ransomware aanvallen. Zoals later in dit rapport wordt besproken, is er een duidelijke trend te zien in **gerichte aanvallen op de publieke sector en kritieke infrastructuur**, met name op het gebied van gezondheidszorg, onderwijs en overheidsorganisaties. De reden hiervoor is dat deze instanties vaak over onvoldoende beveiligingsmiddelen beschikken en eerder geneigd zijn om losgeld te betalen om essentiële diensten te behouden en gevoelige informatie te beschermen. Een verontrustend voorbeeld hiervan vond plaats in Maine in mei 2023, toen een ransomware groep een kwetsbaarheid in MOVEit uitbuitte, een programma voor bestandsoverdracht dat door deze Amerikaanse staat wordt gebruikt. De **aanvallers stalen gegevens van 1,3 miljoen mensen**, waaronder namen, geboortedata, verzekeringsnummers, rijbewijsnummers en andere staats- en belastingidentificatienummers.[4]

Maar deze sector is niet de enige die wordt getroffen. Neem het Amerikaanse MGM Resorts en de Nederlandse voetbalbond KNVB, ze waren eind vorig jaar beide doelwit van hackers. MGM Resorts, een van 's werelds toonaangevende casinohotelketens, was in september aan de beurt voor een aanval door hackers van de ALPHV-subgroep Scattered Spider.[5] De aanvallers gebruikten social engineering methodes door een medewerker te identificeren via LinkedIn en vervolgens de helpdesk te bellen. **Een gesprek van 10 minuten was genoeg om het miljardenbedrijf te compromitteren**. De cyberaanval op MGM Hotels leidde tot ernstige verstoringen, waardoor geld- en gokautomaten werden lamgelegd, en de website en boekingssystemen werden uitgeschakeld. De verwachting is dat de winst van MGM Resorts hierdoor in het derde kwartaal ongeveer $ 100 miljoen lager zal zijn, met nog eens $ 10 miljoen aan kosten voor herstel, waaronder technisch advies, juridische en andere externe consultancykosten. In dezelfde maand eist ransomware groep Lockbit meer dan een miljoen euro van de Nederlandse voetbalbond

1 **Black Kite (2023).** Ransomware threat landscape report.

2 **Gulf Business (2023).** Cybersecurity 2023: Threats proliferate but best practice still works.

3 **WODC (2023).** Wat weten we over ransomware aanvallen op instellingen en bedrijven in Nederland?

4 **Mashable (2023).** An entire state's population just had its data stolen by a ransomware group.

KNVB.[6] Op de getroffen schijf stonden belangrijke persoonlijke data van (oud)spelers, trainers en directieleden van de nationale teams, zoals kopieën van identiteitsbewijzen, contracten, medische gegevens en salarisstroken.

> **Gemiddeld duurt het ongeveer 23 dagen om basisprocessen na een verwoestende ransomware aanval te hervatten. Het herstellen van het totale systeem tot volledige functionaliteit kan maanden in beslag nemen.**

Inge van der Beijl
Human resilience enabler en expert in threat actor communications bij Northwave, tijdens de Human Firewall Conference 2023

De groeiende agressiviteit van cybercriminelen blijkt met name uit hun neiging om ransomware tactieken te intensiveren. Ze maken **steeds vaker gebruik van dubbele afpersingstactieken**, waarbij ze gegevens versleutelen en tegelijkertijd dreigen deze openbaar te maken. Hoewel niet nieuw, is deze methode de afgelopen maanden gangbaarder geworden.[7] Sommige hackers gaan zelfs over tot **drievoudige afpersing**, waarbij ze nog een andere laag van aanvallen toevoegen, zoals DDoS, en **viervoudige afpersing**, waarbij ze extra druk uitoefenen op klanten, leveranciers en werknemers van het aangevallen bedrijf. Na bijvoorbeeld het niet voldoen aan de losgeldeisen van de REvil-groep, richtten de aanvallers zich op Apple, een van de klanten van Quanta Computer, de hardware leverancier.[8] De groep dreigde niet alleen de vertrouwelijke productblauwdrukken van Apple, die bij de aanval waren buitgemaakt, vrij te geven. Zo probeerde bovendien de druk te verhogen door de onthulling te timen met de productlancering van Apple, waarbij ze de publieke en media-aandacht benutten om het effect te maximaliseren.

De professionalisering van cybercriminaliteit strekt zich uit tot verder dan RaaS, naar opkomende technologieën zoals stemkloning. **Stemkloning-as-a-service** (VCaaS) is een aanzienlijke bedreiging geworden, zoals we hebben gezien bij de AI trend. Hiermee kunnen zelfs weinig bekwame cybercriminelen aan de slag met geavanceerde imitatieschema's.[9] Met platforms zoals ElevenLabs, waarmee gebruikers aangepaste spraakvoorbeelden kunnen maken, blijft de toegangsdrempel voor cybercriminaliteit dalen. Gezien de opkomst van professionele, complexe cyberaanvallen is het belang van beveiliging van de toeleveringsketen duidelijker dan ooit. Het uitbesteden van diensten is steeds vaker noodzakelijk, maar het creëert ook nieuwe kwetsbaarheden doordat cybercriminelen **bedrijfsnetwerken infiltreren via partners of leveranciers**. Een voorbeeld hiervan gebeurde bij Airbus in 2023. Hackers compromitteerden een van hun klanten, Turkish Airlines, wat leidde tot een aanzienlijk verlies van gegevens van meer dan 3.000 leveranciers.[10] In deze context zijn we slechts zo sterk als onze zwakste schakel. Het negeren van de beveiliging van onze leveranciers, partners en klanten is niet langer een optie als we veilig willen blijven.

De prognose voor de toekomst is duidelijk: **cybercriminaliteit staat op het punt om een nog professionelere en winstgevendere bedrijfstak te worden**. Deze trend kan niet langer worden genegeerd of onderschat. Het is de hoogste tijd voor organisaties om te investeren in hun beveiliging. De ontwikkelingen van de afgelopen jaren vormen slechts het begin van een toekomst waarin cybercriminaliteit steeds geavanceerdere methoden zal ontwikkelen om haar doelen te bereiken.

5 **Techzine (2023).** Ransomware-aanval MGM Resorts verliep via bekende kwaal in Okta-platform.

6 **RTL Nieuws (2023).** KNVB betaalt losgeld aan cybercriminelen voor niet-publiceren paspoorten Oranjespelers.

7 **TechCrunch (2023).** Why extortion is the new ransomware threat.

8 **RTL Nieuws (2021).** Hackgroep eist 50 miljoen dollar voor gekaapte bestanden Apple.

9 **Recorded Future (2023).** I have no mouth, and I must do crime.

10 **The Register (2023).** Airbus suffers data leak turbulence to cybercrooks' delight.

CHECKLIST

Beveiliging best-practices

- **Bouw een weerbare infrastructuur tegen ransomware:** Ontwikkel een alomvattende beveiligingsaanpak die zowel preventieve maatregelen als goed doordachte reactieplannen omvat. Integreer geavanceerde dreigingsdetectiesystemen, zoals door AI aangestuurde anomaliedetectie. Ga voor een zero-trust architectuur om je beveiliging te verbeteren. Hierbij wordt geen enkele entiteit automatisch vertrouwd, zelfs niet wanneer deze zich binnen het eigen netwerk bevindt. Voer regelmatig beveiligingsaudits uit en ontwikkel effectieve rampherstelplannen. Herzie ook voortdurend back-upstrategieën en zorg ervoor dat je een getest incidentresponsplan hebt om effectief en snel te reageren in geval van een inbreuk.

- **Bescherming tegen social engineering en phishing aanvallen:** Train je medewerkers om hen bewust te maken van de risico's van social engineering aanvallen, met name de tactieken die worden gebruikt door ransomware groepen. Doorlopende training via micromodules en phishing simulaties kan het bewustzijn vergroten en medewerkers helpen potentiële dreigingen te herkennen. Het zorgen voor gegamificeerde en gepersonaliseerde leerervaringen zal de betrokkenheid en retentie van beveiligingskennis vergroten.

- **Omgaan met zero-day kwetsbaarheden:** Ontwikkel strategieën om snel te reageren op zero-day aanvallen. Dit omvat het opzetten van patchmanagement om software-updates efficiënt te distribueren en kwetsbaarheden snel te herstellen.

- **Versterk de beveiliging van de toeleveringsketen:** Evalueer en beveilig je toeleveringsketen. Dit omvat de beveiligingsprotocollen van je partners en leveranciers en het implementeren van strikte toegangscontroles en monitoringsystemen.

- **Verbeter gegevensbeveiliging en integriteit:** Implementeer geavanceerde versleutelingstechnieken en neem een gelaagde benadering van gegevensbescherming aan door te werken met data-centric security-frameworks en technologieën voor het voorkomen van gegevensverlies (DLP). Dit helpt het risico van datalekken en diefstal te minimaliseren.

- **Gebruik dreigingsinlichtingen en -analyses:** Gebruik dreigingsinlichtingen om huidige en opkomende dreigingen te identificeren en analyseren. Dit helpt je bij het nemen van preventieve maatregelen en het verbeteren van je reactievermogen in geval van een aanval.

INTERVIEW

Ralf Schneider

Senior Fellow bij Allianz en Hoofd Cybersecurity bij NextGenIT Think Tank

De indrukwekkende carrière van Ralf Schneider in IT en cybersecurity beslaat meer dan twee decennia. Het wordt gekenmerkt door zijn lange dienstverband bij Allianz, waar hij 13 jaar diende als Group CIO. Hij was ook bestuurslid van Allianz Managed Operations & Services en heeft onlangs de rol van Senior Fellow en Hoofd Cybersecurity op zich genomen bij de NextGenIT Think Tank. Ralf heeft een doctoraat in informatica behaald aan de Ludwig Maximilian University in München.

> Criminelen hebben steeds minder vaardigheden en organisatorisch vermogen nodig om een zeer effectieve aanval te lanceren en dat gaat een groot probleem voor ons worden.

Hoe ben je terechtgekomen in informatiebeveiliging?

Ik begon in dit vakgebied toen ik in januari 2011 werd benoemd tot Group CIO van Allianz. Met 3.000 kantoren en 63 bedrijfseenheden verspreid over de hele wereld, kwam ik er al snel achter dat we een communicatie-infrastructuur nodig hadden die videoconferenties omvatte. We moesten onze IT zó opbouwen dat we wereldwijd toegang konden krijgen tot IT-middelen met elk apparaat. Hiervoor heb je een aantal dingen nodig: een netwerkinfrastructuur, een geconsolideerd datacenter waarmee de toepassingen wereldwijd werken en een gevirtualiseerde eindwerkruimte, die allemaal veilig moeten zijn. Er bestond geen twijfel dat cyberbeveiliging een belangrijk onderwerp voor ons zou worden.

Toen de onthullingen van Snowden in 2013 naar buiten kwamen en de mobiele telefoon van mevrouw Merkel werd gehackt, zagen we dat cyberbeveiliging steeds meer een heikel punt werd. Naast de infrastructuur van netwerken, datacenters en virtuele werkruimten hebben we op mondiaal niveau in 2013 de Cyber Security Infrastructure, Global Identity and Access Management, Global Privilege Access Management en het Allianz Cyber Defense Center opgezet.

Hoe beoordeel je het huidige dreigingslandschap en hoe zal dit zich in de komende jaren ontwikkelen?

Sinds het begin van de oorlog in Oekraïne werd het duidelijk dat we midden in een cyberoorlog zitten. Op het gebied van cyberbeveiliging hebben we te maken met overheden, militaire en zeer geavanceerde criminele actoren. Cybercriminelen scherpen voortdurend hun vaardigheden aan en worden georganiseerder. Bovendien zetten ze de industrialisatie van cyberaanvallen om in een lucratieve business.

Dan is er een derde component. Cyberbeveiliging doorloopt doorgaans cycli. DDoS was een belangrijk probleem in 2013 voordat het verdween en nu is het weer terug. Het is te verwachten dat de focus terugkeert naar activisten en hackingkits, inclusief degene die worden aangedreven door AI. Criminelen hebben steeds minder vaardigheden en organisatorisch vermogen nodig om een zeer effectieve aanval te lanceren en dat gaat een groot probleem voor ons worden. In plaats van ons te concentreren op slechts een paar groepen, moeten we er honderden, zo niet duizenden in de gaten houden.

Het feit dat de kloof tussen rijk en arm groter wordt, maakt de situatie nog ernstiger. Je hoeft tegenwoordig geen professionele sporter te zijn om veel geld te verdienen. Je kunt ook hacker worden. Het goede nieuws is dat we steeds beter worden in zelfverdediging.

Je noemde de toename van generatieve AI. Denk je dat technologieën zoals deepfakes en stemklonen een massaprobleem zullen worden?

Stemklonen en vergelijkbare methoden zijn nu erg populair, maar ik denk dat er nog een ander risico aan verbonden is. Het gaat niet langer om het vinden van een beveiligingsfout of het identificeren van een individu als zwak punt. Het gaat om de respons: het uitschakelen en omzeilen van detectietools. Daar zal een grote toename te zien zijn in het gebruik van AI.

Ik zie op dit moment geen grote gevaren omdat AI nog te veel fouten maakt en op de juiste manier moet worden gebruikt. Maar we bevinden ons nog steeds in de beginfase en we moeten ons voorbereiden op het ergste scenario. Op dit moment profiteren we ervan dat een echt grootschalige inzet nog niet heeft plaatsgevonden. Met elke aanval - succesvol of niet - leren we en kunnen we onze verdediging verbeteren. Maar het risico zit niet alleen in de kwantiteit, maar ook in de gelijktijdigheid die AI mogelijk maakt. Gelijktijdige schaalvergroting van aanvallen kan een groot probleem worden.

Hoe denk je dat we gelijke tred kunnen houden met de snelle ontwikkelingen in het dreigingslandschap?

Kort gezegd, goede cyberhygiëne en op de hoogte blijven van de nieuwste dreigingen. Cyberhygiëne moet vanaf de basis worden opgebouwd, wat een grote uitdaging is. Ik denk niet dat je multifactorauthenticatie kunt omzeilen. Voordat je in je auto stapt, moet je je gordel omdoen. Voordat je op het internet gaat surfen, moet je een multifactorauthenticatie doorlopen. Bij Allianz hebben we tijdens de coronapandemie multifactorauthenticatie geïmplementeerd omdat de meeste mensen vanuit huis werkten.

De belangrijkste manier om gelijke tred te houden met de snelheid waarmee dreigingen zich ontwikkelen, is vanaf het begin goed en uitgebreid te werk gaan en vervolgens zorgen dat je bijblijft. We vernieuwen momenteel ons Cyber Defense Platform dat we hebben gekocht van marktleiders. Nu is de grote taak om het te integreren en het in de praktijk te gebruiken, maar daar investeren we in. Uiteindelijk komt het allemaal neer op de menselijke factor - de juiste mensen vinden en hen de mogelijkheid geven om zelfstandig te leren. Ontbreekt het je aan capaciteit of bewustzijn in je bedrijf, dan kom je ook met alle technologie ter wereld niet ver.

> **Uiteindelijk komt het allemaal neer op de menselijke factor. De juiste mensen vinden en hen de kans geven om zelfstandig te leren. Ontbreekt het aan capaciteit of bewustzijn in je bedrijf, dan kom je ook met alle technologie ter wereld niet ver.**

Een andere trend op het gebied van cybercriminaliteit is digitalisering, waarbij alles steeds meer met elkaar verbonden raakt. Welke risico's zie je hier met betrekking tot cybersecurity?

Het exploiteren van een website zonder bescherming tegen fundamentele dreigingen door een proxy shield is erg riskant. Elke onderneming heeft een goed proxy shield nodig en dat heeft zijn prijs. Alles is met elkaar verbonden en gaat als het ware met de snelheid van het licht. Bovendien wordt alles bediend door software die handelingen in milliseconden kan uitvoeren. Monitoring en controle zijn niet mogelijk zonder automatisering, maar we kunnen niet verwachten dat AI alles voor ons doet. We worden aangevallen door mensen die AI gebruiken, dus we hebben mensen nodig die AI gebruiken om ons te verdedigen. Deze mensen moeten worden opgeleid en de juiste inzichten en kennis hebben. Bovendien zijn de contactpunten voor de IT-systemen niet alleen machines, maar meestal mensen. Elk van deze contactpunten moet worden gemonitord en beveiligd.

De vraag is, moeten bedrijven eerst hun technische kwetsbaarheden dichten en zich dan op mensen richten of andersom? Heb jij een holistische strategie om de menselijke factor te betrekken?

Als je je met volle vaart in elke strijd stort, ga je verliezen. Als je je vijand kent, verlies je misschien de helft van de tijd. Maar als je zowel je vijand als jezelf kent, heb je een goede kans om elke keer te winnen. Cybersecurity is een spel van aanval en verdediging. We begonnen in 2013 met twee controles die we op uitgebreide schaal uitrolden. We begonnen met bewustzijn en grootschalige dekking tegen DDoS en het beveiligen van mobiele eindapparaten, gevolgd door alle lagen zoals de Protection Detection Layer, Response Layer en Recovery Layer.

Tweeduizend jaar wijsheid heeft ons geleerd dat het erom gaat je eigen IT-systemen, netwerk en kwetsbaarheden te kennen. Je kunt niet iets verdedigen wat je niet kent. IT-systemen worden bediend door mensen, dus je moet de mensen kennen en hun bewustzijn van veilige IT.

Over bewustzijntrainin gesproken, hoe zie jij de ontwikkeling van een nalevingsvereiste naar een duurzame maatregel waarmee je mensen tot een verdedigingslinie kunt vormen?

In het huidige tijdperk van digitalisering kan IT niet alleen functioneel zijn - het moet ook veilig en conform zijn. Maar niet alles wat goed is voor naleving is goed voor beveiliging. Bewustzijn is een goed voorbeeld. Je implementeert een bewustwordingsprogramma via een online training, vinkt je nalevingsvereisten af en de toezichthouder is tevreden. Maar dat betekent niet dat je in de tussentijd persé veiliger bent geworden.

> We worden aangevallen door mensen die AI gebruiken en daarom hebben we mensen nodig die AI gebruiken om ons te verdedigen. Deze mensen moeten worden opgeleid en beschikken over de juiste kennis en inzicht.

Dit is waar de bekwaamheid van medewerkers om de hoek komt kijken. We hebben al vroeg geleerd dat je een aansprekende, leuke benadering van bewustzijn moet hanteren en hier niet te veel druk op moet uitoefenen. Je moet ook het juiste moment kiezen om mensen te trainen. Het ideale moment is wanneer je net een phishing campagne of een echte phishing e-mail heb ontvangen waarbij je al dan niet in de fout bent gegaan. De volgende uitdaging is om de aandacht van mensen vast te houden en de Phishing Report Button van SoSafe is daarvoor een uiterst nuttige tool. Als medewerkers niet zeker weten of ze een echte phishing e-mail hebben ontvangen, kunnen ze deze knop gebruiken om hen te vertellen of het een phishing aanval is en hoe ze deze kunnen herkennen. Op die manier is het leereffect enorm. Plus, er is het plezier en de motivatie die voortkomen uit het feit dat mensen zelfstandig leren en de Phishing Report Button als een soort assistent kunnen gebruiken. Gebruikers kunnen gelijk toepassen wat ze hebben geleerd, wat een directe beloning is.

IT-teams staan op verschillende manieren onder druk waar het gaat om zowel verdediging als bewustwordingstraining op het gebied van beveiliging. Wat denk je dat mogelijke maatregelen zouden kunnen zijn om de last van IT-teams wat te verlichten?

We moeten ons afvragen waar de echte problemen liggen – het uitvoeren van crisisoefeningen op elk niveau, tot aan het topmanagement en de raad van bestuur. We doen dat bij Allianz al jaren regelmatig. Verschillende psychologische factoren spelen hierbij een rol, te beginnen met het feit dat mensen niet graag laten zien dat ze iets niet kunnen. Ten tweede moeten de voordelen van de geïnvesteerde tijd vanaf het begin duidelijk en snel zichtbaar zijn. Bewustzijnstraining kost immers geld en middelen.

Een van de kernuitdagingen ligt in het tastbaar en voelbaar maken van de urgentie van cyberbeveiliging voor het topmanagement in alle bedrijfseenheden. Als het gaat om bedrijfsdoelen, moet IT zowel functioneel als veilig zijn. Tenzij er iets ernstigs gebeurt, is het moeilijk te zeggen of de genomen maatregelen je veiliger hebben gemaakt dan voorheen. Het bewijzen van de effectiviteit en het wegnemen van wantrouwen is heel moeilijk omdat je niet kunt aantonen of je veiligheid verbetert – met aanvalsimulaties maak je inzichtelijk dat je sneller, efficiënter en effectiever wordt in je verdediging.

Denk je dat er KPI's zijn die overtuigender zouden kunnen zijn voor het topmanagement?

Bij Allianz hebben we acht gezondheidsindicatoren voor cyberbeveiliging die we beoordelen met een kleurensysteem van rood, oranje, geel, lichtgroen en groen, zodat we het succes van onze maatregelen zichtbaar kunnen evalueren. Net als bloeddruk, hartslag en cholesterolniveaus moeten onze acht gezondheidsindicatoren binnen een bepaald bereik vallen.

Twee van deze indicatoren hebben zich bijzonder effectief bewezen. Eén daarvan is onze zero- tolerance ten opzicht van schadelijke elementen, wat betrekking heeft op technische aspecten. Dit leidde ertoe dat we al onze verouderde, onvoldoende beschermde applicaties opspoorden. We begonnen ook met automatiseren, analyseerden alle verouderde databases en besturingssystemen, identificeerden schadelijke componenten en vernieuwden systematisch ons hele IT-systeem. De zero-tolerance component werd om veiligheidsredenen geïmplementeerd, maar gaat veel verder dan dat. De tweede effectieve indicator is onze Awareness Score, waarmee we wereldwijde phishing campagnes meten. We registreren klikpercentages en hoeveel mensen een schadelijke e-mail melden.

In een eerder interview zei je dat hiërarchische structuren in bedrijven de cyberbeveiliging kunnen belemmeren. Wat bedoel je daarmee?

Externe aanvallen die worden uitgevoerd met tools kunnen alleen worden voorkomen door experts met tools die hier tegenop gewassen zijn. Beveiligingsexperts moeten beslissen wat er moet gebeuren. Het uitvoerend niveau moet alles in de gaten houden en op het juiste moment middelen en initiatieven bieden. Toch gebeurt dit 'ter plekke', dus er is ook autonomie nodig. Het management legt de basis, voorziet in de middelen voor effectieve cyberverdediging en brengt beveiligingsexperts samen met interne en externe partners.

> Beveiligingsexperts moeten beslissen wat er moet gebeuren. Het uitvoerend niveau moet alles in de gaten houden en op het juiste moment middelen en initiatieven bieden.

4 Digitale onenigheid en misleiding: De twee gezichten van hacktivisme en cybercriminaliteit in een gefragmenteerde wereld

Het ingewikkelde dreigingslandschap strekt zich uit voorbij individuen die streven naar financieel of persoonlijk gewin. Escalerende politieke en sociale spanningen voeden de opkomst van een andere significante stroming in het digitale speelveld: **hacktivisten**. Gedreven door de wens om onenigheid te uiten of steun te betuigen aan zaken als gewapende conflicten of sociale onrechtvaardigheden, maken deze individuen **gebruik van kwetsbaarheden en beveiligingslekken om hun standpunten kenbaar te maken** - een situatie die met de maand intenser wordt.

Volgens het meest recente rapport van Motorola, is hacktivisme in het derde kwartaal van 2023 met 27% toegenomen.[1] Een opvallend voorbeeld van deze trend is het pro-Russische hacktivistische initiatief **DDoSia**, dat bekend staat om aanvallen op westerse entiteiten. De groep zag een dramatische toename in deelnemers in 2023, met een stijging van het aantal leden met 2.400% en 45.000 abonnees op hun belangrijkste kanaal, Telegram.[2]

De lopende conflicten, zoals tussen Rusland en Oekraïne, laten zien hoe moderne confrontaties zich hebben ontwikkeld tot **hybride oorlogen, die zowel fysiek als digitaal worden uitgevochten**. Binnen dit kader gebruiken zowel hacktivisten als door de overheid gesponsorde entiteiten **cyberaanvallen** als een **essentieel onderdeel van hun uitgebreide toolkit voor moderne oorlogsvoering**. Een sprekend voorbeeld hiervan is de aanval door de Oekraïense groep Cyber.Anarchy.Squad tegen Infotel JSC, een cruciale Russische telecomprovider die essentieel is voor het functioneren van belangrijke Russische banken en financiële instellingen.[3] Deze aanval had een aanzienlijke impact, verstoorde veel Russische banksystemen en zorgde ervoor dat ze gedurende enkele uren geen online betalingen konden verwerken.

Het recente conflict tussen Israël en Gaza is een ander voorbeeld van de escalatie en verdere implicaties van deze dreiging. Kort nadat het conflict begon, voerde Anonymous Sudan hun eerste cyberaanval uit, gericht op de waarschuwingssystemen van Israël.[4] Daarbij beweerden ze waarschuwingsapplicaties uit te schakelen die burgers op de hoogte stellen van inkomende raketten. Bijna tegelijkertijd richtte KillNet zich op het verstoren van verschillende

1 **Motorola Solutions (2023).** New Report Outlines Q3 2023 Cyber Threats to Public Safety.

2 **Bleeping Computer (2023).** Pro-Russia DDoSia hacktivist project sees 2,400% membership increase.

3 **Bleeping Computer (2023).** Ukrainian hackers take down service provider for Russian banks.

4 **Security Week (2023).** Hackers Join In on Israel-Hamas War With Disruptive Cyberattacks.

Israëlische overheidswebsites. Als vergelding voor deze en verschillende andere aanvallen, steunde de hacktivistische groep Indian Cyber Force uit India Israël en haalde de websites van Hamas, Palestine National Bank, Palestine Web Mail Government Services en Palestine Telecommunications Company offline.[5]

Maar hacktivisme gaat verder dan oorlogsvoering en politieke spanningen en omvat verschillende sociale kwesties. Zo lanceerde Anonymous Sudan vorig jaar een cyberaanval op Scandinavian Airlines als reactie op het openbaar verbranden van de Heilige Koran door een extreemrechtse nationalistische groep buiten de Turkse ambassade in Stockholm.[6] De aanval veroorzaakte aanzienlijke problemen in het online systeem van de luchtvaartmaatschappij, waarbij passagiersgegevens, waaronder contactinformatie, details van eerdere en toekomstige vluchten en gedeeltelijke creditcardnummers openbaar werden gemaakt.

Later in 2023 beweerde de hackergroep VulzSec gevoelige Franse politiegegevens te hebben gecompromitteerd en gelekt als vergelding voor politiegeweld.[7] Dit resulteerde in de onthulling van 7.092 gegevensrecords van politieafdelingen en de profielen van 30 politieagenten. Dit incident benadrukt een bredere trend: een significante toename van 28% in cyberaanvallen tegen wetshandhaving, waarbij hacktivisme een van de belangrijkste bijdragende factoren is.[8]

Het is echter belangrijk je te realiseren dat hacktivisten niet uit zijn op financieel gewin. Ze gaan over tot cybercriminaliteit om onderwerpen waarin ze geloven te steunen. Aan de andere kant maken sommige cybercriminelen gebruik van sociale instabiliteit voor hun eigen doeleinden. Zoals te zien is in de tactieken van het conflict tussen Rusland en Oekraïne, waar nu frauduleuze liefdadigheidssites worden opgezet om in te spelen op het altruïsme van individuen die willen helpen in de crisis in Gaza.[9] En dat is nog niet alles. Door de overheid gesponsorde cybercriminelen voegen zich ook in de mix, zoals te zien is in de 'WildCard'-hackercampagne, gericht op Israëlische instellingen met geavanceerde malware zoals 'SysJoker.'[10] Dit maakt het steeds moeilijker voor organisaties om te identificeren van wie een aanval afkomstig is. Bovendien creëert het een zeer complex dreigingslandschap waarin verschillende spelers actief zijn, elk met hun eigen motieven.

↗ **28%**

toename in cyberaanvallen tegen wetshandhaving, waarbij **hacktivisme** een van de belangrijkste bijdragende factoren is.

Bron: Motorola Solutions[8]

Naarmate de wereldwijde spanningen blijven escaleren en het einde hiervan nog niet in zicht is, lijkt een toename van hacktivistische aanvallen in 2024 vrijwel zeker. In deze context dragen zowel hacktivisten als cybercriminelen bij aan de instabiliteit van de cyberwereld. Ze opereren in een soort antagonistische synergie, waarbij ze elk profiteren van de kwetsbaarheden die door de acties van de ander worden onthuld. Deze wisselwerking creëert een dynamische en voortdurend evoluerende omgeving van cyberdreigingen, die de complexiteit en onvoorspelbaarheid van het digitale landschap weerspiegelt.

5 **CSO (2023).** Israel-Hamas conflict extends to cyberspace.

6 **Security (2023).** Scandinavian Airlines getroffen door datalek na cyberaanval op site en app.

7 **The Cyber Express (2023).** Cyber Attack on French National Police: VulzSec Hacking Group Claims to Leak Sensitive Data.

8 **Motorola Solutions (2023).** New Report Outlines Q3 2023 Cyber Threats to Public Safety.

9 **InfoSecurity Magazine (2023).** Cyber-Criminals Exploit Gaza Crisis With Fake Charity.

10 **Cyberscoop (2023).** Shadowy hacking group targeting Israel shows outsized capabilities.

CHECKLIST

Beveiliging best-practices

Bouw een redundante netwerkinfrastructuur: Het hebben van meerdere datapaden kan helpen bij het handhaven van beschikbaarheid, zelfs bij een DDoS-aanval. Dit omvat het kunnen beschikken over extra servers, alternatieve datacenters of cloudservices. Als één pad wordt gecompromitteerd of overbelast, kan het verkeer worden omgeleid naar een ander pad, waardoor de continuïteit van de service behouden blijft.

Regelmatige stresstesten: Voer stresstests uit op je infrastructuur om te begrijpen hoe deze zich gedraagt onder hoge belasting. Het gebruik van 'Red Team'-oefeningen om realistische aanvalsscenario's te simuleren, kan heel waardevol zijn bij deze tests.

Implementeer snelheidsbeperking, scrubbing-services en overdimensionering van bandbreedte: Deze strategieën stellen je in staat om de hoeveelheid verkeer te controleren die een server over een bepaalde periode accepteert, kwaadaardig verkeer te filteren en een hogere bandbreedtecapaciteit te behouden om plotselinge pieken in het verkeer aan te kunnen.

Regelmatige gegevensback-up en externe opslag: Maak regelmatig back-ups van kritieke gegevens en sla deze op externe locaties of op een cloudplatform op om het risico van verlies te verminderen, mocht de primaire locatie worden gecompromitteerd. Het is raadzaam om het gebruik van onveranderlijke back-ups over te nemen en de 3-2-1-back-upregel te volgen. Hierbij worden drie totale kopieën van gegevens onderhouden - twee lokale kopieën op verschillende apparaten voor eenvoudige toegang en herstel en één kopie die extern is opgeslagen voor extra beveiliging.

Netwerksegmentatie: Segmenteer je netwerk om de verspreiding van malware te beperken. Als één segment wordt gecompromitteerd, heeft dit niet noodzakelijkerwijs invloed op het gehele netwerk. Het gebruik van microsegmentatie wordt aanbevolen voor verbeterde granulariteit en bescherming van gevoelige gegevens binnen segmenten.

CHECKLIST

Beveiliging best-practices

Beperkingen van gebruikersprivileges: Implementeer richtlijnen van minste privilege-toegang, waarbij gebruikers alleen de benodigde machtigingen voor hun functierollen krijgen toegekend. Deze aanpak, een essentieel onderdeel van de Zero-Trust-netwerkarchitectuur, minimaliseert het risico van interne bedreigingen effectief . Zorg ervoor dat deze machtigingen regelmatig worden herzien en bijgewerkt.

Web Application Firewall (WAF): Implementeer een WAF om het verkeer van en naar een webtoepassing te monitoren. Dit helpt ongeautoriseerde wijzigingen aan de website te voorkomen. Een WAF kan worden geïntegreerd met andere beveiligingstools en het wordt aanbevolen om een geünificeerd threat management-systeem te creëren. Overweeg bovendien het gebruik van geavanceerde WAF's die machine learning bevatten, aangezien je daarmee beschikt over de mogelijkheid van dynamische aanpassing aan opkomende en steeds veranderende cyberdreigingen.

Sterke authenticatiemaatregelen: Handhaaf robuuste wachtwoordbeleidsregels en implementeer multifactorauthenticatie (MFA) voor een extra beveiligingslaag, vooral voor toegang tot gevoelige systemen en de backend van de website. Gebruik waar mogelijk technologieën voor wachtwoordloze authenticatie en biometrische verificatie om de beveiliging verder te verbeteren.

Bewaking- en waarschuwingssystemen: Gebruik bewakingstools om het netwerkverkeer, de systeemprestaties en toegangslogboeken in de gaten te houden. Gebruik ook Security Information and Event Management (SIEM)-systemen en Security Orchestration, Automation, and Response (SOAR)-systemen voor uitgebreide monitoring, analyse en geautomatiseerde reacties. Stel waarschuwingen in voor ongebruikelijke activiteiten of wijzigingen, waardoor het beveiligingsteam snel kan reageren op mogelijke beveiligingsincidenten.

5 Desinformatie-as-a-service: Een uiterst krachtig middel in het arsenaal van hackers

In de jaren sinds het Cambridge Analytica-schandaal hebben desinformatiecampagnes een belangrijke rol gespeeld bij het verergeren van sociale polarisatie. Deze tactiek, waarbij **opzettelijk valse informatie** wordt verspreid, wordt steeds vaker gebruikt door verschillende spelers[1] om de publieke opinie te manipuleren, reputaties te beschadigen en invloed uit te oefenen op bedrijfs- en politieke landschappen.[2] In Nederland presenteerde het kabinet eind 2022 een nieuwe Rijksbrede strategie tegen desinformatie.[3] Daarmee wil men het publieke debat versterken en de invloed van desinformatie verminderen.

2023 markeerde een keerpunt in desinformatiecampagnes: met de **opkomst van generatieve AI** groeien de zorgen over een wereld waar manipulatieve inhoud zo goedkoop en gemakkelijk op grote schaal kan worden geproduceerd, dat het **bijna onmogelijk wordt om onderscheid te maken tussen authentieke en kunstmatige verhalen**.

Een belangrijk voorbeeld dat de impact van desinformatiecampagnes aantoont, zijn de Amerikaanse presidentsverkiezingen. Tijdens de verkiezingen van 2016 was er sprake van wijdverspreide desinformatie op sociale media, aangewakkerd door extreemrechtse activisten, buitenlandse inmenging en nepnieuwssites. In 2020 werd de verkiezing overspoeld met complottheorieën en ongefundeerde claims van kiezersfraude, die miljoenen mensen bereikten en een antidemocratische beweging stimuleerden. Met het oog op de verkiezingen van 2024 zijn er toenemende zorgen over hoe de nieuwste ontwikkelingen in AI mogelijk kunnen worden gebruikt om **meer geavanceerde vormen van misinformatie**, deepfakes en gerichte propagandacampagnes te creëren.[4]

In feite werd dit **potentiële gevaar voor de democratie** al zichtbaar bij de Slowaakse verkiezingen, waar een door AI geproduceerde deepfake-audio werd gebruikt om desinformatie via sociale media te verspreiden.[5] De audio, die duizenden gebruikers bereikte, bevatte Monika Tódová, een bekende journaliste, en Michal Šimečka, de leider van de Progressieve Slowaakse partij, die spraken over verkiezingsfraude. Ondanks onmiddellijke ontkenningen van de authenticiteit van het gesprek door de betrokkenen en de bevestiging van de onwaarheid ervan door verschillende fact-checking-organisaties, was de verspreiding van de video significant vanwege het tijdstip. Het werd vrijgegeven tijdens een periode van 48 uur van stilte voor de verkiezing, waardoor het moeilijk was voor mediabedrijven en politici om het publiekelijk te weerleggen.

1 **Nu.nl (2024).** Experts zien door AI gegenereerde desinformatie als grootste risico van 2024.

2 **The New York Times (2021).** Disinformation for Hire, a Shadow Industry, Is Quietly Booming.

3 **Digitale Overheid (2023).** Nieuwe Rijksbrede strategie tegen desinformatie.

4 **Unite (2023).** Kunnen de Amerikaanse verkiezingen van 2024 gebruikmaken van generatieve AI?

In deze context vertegenwoordigt **desinformatie-as-a-service (DaaS)** een opmerkelijke verschuiving in de schaal en verfijning van misinformatie-inspanningen. Dit **nieuwe model van informatie-oorlogvoering** stelt individuen en organisaties in staat om nepnieuws en desinformatiecampagnes met ongekende eenvoud te kopen en te verspreiden. Gestimuleerd door de snelle vooruitgang van generatieve AI en een netwerk van professionele trollen, bots en geavanceerde online manipulatietools, biedt DaaS de mogelijkheid om desinformatiecampagnes uit te voeren, op dezelfde manier als RaaS dat heeft gedaan met ransomware aanvallen - een revolutie die cybercriminelen en hacktivisten ongetwijfeld zullen uitbuiten.[6]

Dit betekent dat **2024 een toename zal zien van zowel politiek als financieel gemotiveerde desinformatiecampagnes** die waarschijnlijk een breed scala van sectoren zullen targeten, waaronder de gezondheidszorg, de financiële sector, technologie, onderwijs en media. Aan de ene kant zullen hacktivisten en door de overheid gesponsorde cybercriminelen doorgaan met het destabiliseren van regeringen en politieke organisaties met desinformatie om de publieke opinie te beïnvloeden en meer steun te krijgen voor hun doelen. Een voorbeeld hiervan deed zich voor in 2023 met de verspreiding van een deepfake-beeld van Atlético Madrid-supporters die een Palestijnse vlag tonen, een misleidend verhaal dat online aanzienlijke tractie kreeg.[7] Sommige van deze aanvallen zullen brede economische implicaties hebben, tot aan **invloed op de aandelenmarkt**. Dit gebeurde al in mei 2023, toen een nepbeeld van een explosie in de buurt van het Pentagon wijdverspreid werd gedeeld op sociale media en werd verspreid door verschillende media, waaronder het Russische staatsnieuwsagentschap RT. Dit leidde tot een korte beursdaling toen de angst zich verspreidde.[8]

Aan de andere kant zullen financieel gemotiveerde cybercriminelen proberen organisaties en bedrijven op verschillende manieren te destabiliseren. Met behulp van DaaS **kunnen zij tegen heel lage kosten desinformatie gebruiken in geavanceerde phishing en social engineering aanvallen**, waarbij ze profiteren van het verspreiden van verontrustend nieuws over een organisatie om de emoties van angst en urgentie van individuen uit te buiten. Maar daar stopt het niet. Desinformatiecampagnes door verschillende spelers die extern breed worden gedeeld, kunnen **ook de reputatie van een bedrijf schaden**. Dit was duidelijk in het geval van Wayfair, waar samenzweringstheoretici gelinkt aan QAnon de chaos van de pandemie benutten om de reputatie van de winkelketen te schaden.[9] Met behulp van platforms zoals Twitter, Instagram en Reddit verspreidden ze valse beweringen dat Wayfair betrokken was bij kinderhandel. Ondanks de inspanningen van het bedrijf om deze beschuldigingen te weerleggen, bleven de leugens online voortbestaan, wat de aanzienlijke reputatierisico's aantoont waarmee bedrijven worden geconfronteerd als gevolg van dergelijke desinformatie.

Ook CEO's zijn belangrijke doelwitten voor deepfakes omdat het handhaven van een openbaar profiel deel uitmaakt van hun werk. Aangezien ze regelmatig spreken tijdens kwartaalrapporten, aandeelhoudersvergaderingen en televisie-interviews, is het voor cybercriminelen niet moeilijk om audio- en videoclips van hen te verkrijgen. En bij de trend van kunstmatige intelligentie hebben we al gezien wat ze met dit materiaal kunnen doen.

Met de escalatie van desinformatiecampagnes die de het mondiale informatielandschap bedreigen, worden organisaties zich steeds meer bewust van de risico's die deze met zich meebrengen, waaronder aanzienlijke financiële verliezen en langetermijnschade wat betreft reputatie. Naarmate deze tactieken geavanceerder en alomtegenwoordiger worden, zullen organisaties daarom robuuste tegenmaatregelen moeten ontwikkelen om hun integriteit te beschermen en het vertrouwen van het publiek te behouden.

5 **Wired (2023).** Slovakia's Election Deepfakes Show AI Is a Danger to Democracy.

6 **Hackernoon (2022).** Disinformation-as-a-Service: Content Marketing's Evil Twin.

7 **Reuters (2023).** Fact Check: Image of Atletico Madrid fans holding giant Palestinian flag is fake.

8 **NOS (2023).** Nepfoto van explosie bij Pentagon veroorzaakt korte beursdip.

9 **The Globe and Mail (2023).** Disinformation campaigns, including those using AI deepfakes, are creating risks for corporations.

CHECKLIST

Beveiliging best-practices

Beoordeel potentiële dreigingen: Het is belangrijk dat organisaties regelmatig hun vatbaarheid voor desinformatiecampagnes evalueren. Dit omvat een goed doordachte benadering van dreigingsmodellering die niet alleen de waarschijnlijkheid van gerichte aanvallen beoordeelt, maar ook de mogelijke impact van dergelijke campagnes meeneemt. Bovendien kunnen het gebruik van tools voor sentimentanalyse en trendmonitoring helpen bij het analyseren van de publieke opinie en trends. Hierdoor kunnen organisaties effectief anticiperen en strategieën ontwikkelen tegen mogelijke desinformatiedreigingen.

Informeer en train medewerkers: Rust medewerkers uit met kennis van tactieken voor desinformatiecampagnes en de mogelijke impact op de organisatie. Leer hen hoe ze informatie kunnen controleren, geloofwaardige bronnen kunnen identificeren en kritisch kunnen nadenken over de juistheid en betrouwbaarheid van de inhoud die ze tegenkomen. Het ontwikkelen van een cultuur van kritisch denken en verificatie maakt een organisatie sterker en minder vatbaar voor de effecten van misleidende informatie.

Verbeter interne communicatie: Versterk interne communicatiekanalen om valse informatie snel aan te pakken en te verminderen. Het gebruik van communicatietools zoals Sofie Rapid Awareness, de integratie van SoSafe met MS Teams, stelt je in staat om je medewerkers snel op de hoogte te stellen wanneer je een desinformatiecampagne over je bedrijf identificeert.

Creëer een crisisteam voor communicatie: Richt een rapid response team op dat gespecialiseerd is in crisiscommunicatie en in staat is om snel tegen desinformatie op te treden met feitelijke informatie.

CHECKLIST

Beveiliging best-practices

Bevorder waakzaamheid en het melden van onregelmatigheden: Bedrijven moeten een omgeving creëren waarin medewerkers waakzaam en bereid zijn alle ongebruikelijke dingen die ze online tegenkomen, zoals misleidend nieuws, deepfake-afbeeldingen of bewerkte video- of audiobestanden, te melden. Medewerkers moeten zich veilig voelen om deze incidenten te melden zonder vrees te worden veroordeeld. Het is cruciaal om hiervoor een gebruiksvriendelijk, anoniem rapportagesysteem te implementeren dat medewerkers veilig en zonder angst voor represailles kunnen gebruiken om gevallen van desinformatie te melden.

Automatiseer het monitoren van sociale media: Houd sociale media in de gaten waar het gaat om DaaS-operaties. Controleer op vervalst nieuws, gemanipuleerde afbeeldingen en nep-audioclips. Een gezamenlijke inspanning met de PR- en marketingteams is essentieel om dit te bereiken. Er zijn ook op AI gebaseerde tools voor het monitoren van sociale media die potentiële desinformatie in realtime kunnen detecteren en signaleren, wat directe actie mogelijk maakt.

Werk samen aan dreigingsinformatie: Werk samen met externe cybersecurity-netwerken, waaronder samenwerkingsverbanden met sectorgenoten, overheidsinstanties en wereldwijde cybersecurity-allianties, voor gedeelde inzichten in trends en best-practices op het gebied van desinformatie.

6 2024: Een jaar van beveiligingsuitdagingen voor de publieke sector en kritieke infrastructuren

Hoewel hacktivisme een bekende dreiging is voor instellingen in de publieke sector, is dit slechts één aspect van de vele uitdagingen waarmee ze te maken hebben. De publieke sector moet ook omgaan met dreigingen van **door overheden gesponsorde cybercriminelen en onafhankelijke** hackers, die streven naar gegevensvernietiging, verstoring, financieel gewin en spionage – elk met ernstige gevolgen. In feite meldt het IBM-rapport 'Kosten van gegevensinbreuk 2023' dat **de gemiddelde kosten van een cyberaanval in de publieke sector zijn gestegen naar een alarmerende $ 2,6 miljoen**.[1]

De digitalisering van gevoelige informatie in entiteiten van de publieke sector, samen met de kritieke diensten die ze leveren, maakt de publieke sector **aantrekkelijk voor cybercriminelen die op zoek zijn naar gevoelige gegevens en verstoring van diensten**. Alleen al in 2022 steeg het aantal door overheden gesteunde **cyberaanvallen die specifiek gericht waren op kritieke infrastructuur wereldwijd van 20% naar 40%**.[2] Deze toename is grotendeels te wijten aan door de overheid gesponsorde aanvallen als gevolg van het conflict tussen Rusland en Oekraïne. Met het conflict in Oekraïne nog steeds actief en andere conflicten zoals de Gaza-Israël oorlog, verwachten we dat deze trend zich zal voortzetten in 2024 en de dreigingsomgeving verder zal compliceren.

> **Cyber is een geopolitiek instrument van macht en een nieuwe aanvalsvector die overheden gebruiken om hun eigen doelen na te streven.**

Dr. Katrin Suder
Strategie-expert (digitale technologieën, bedrijfsleven en politiek)

De omvang van waardevolle informatie die organisaties in deze sector bezitten, is een goudmijn voor velen en de onderwijssector is zich daar goed van bewust. In Nederland kwam men na een aantal voorvallen zoals de hack van het ROC Mondriaan in Den Haag tot de conclusie dat het aantal cyberaanvallen op scholen toeneemt, maar de regulering ontbreekt.[3]

Vorig jaar bedroeg de **kostprijs van een succesvolle gegevensinbreuk in de onderwijssector $ 3,65 miljoen**.[4] In 2023 zagen we hoe de hackergroep Vice Society gevoelige informatie lekte van de Pates Grammar School in Engeland, waaronder paspoortscans

1 **IBM (2023).** Cost of a Data Breach 2023.
2 **Microsoft (2022).** Digital Defense Report 2022.
3 **Techzine (2022).** Aantal cyberaanvallen op scholen neemt toe, regulering ontbreekt.
4 **IBM (2023).** Cost of a Data Breach 2023.

van kinderen, salarisschalen van het personeel en contractgegevens.[5] Verscheidene andere aanvallen volgden in heel Europa, waarbij hackers verschillende interne netwerken en de IT-infrastructuur van Franse[6] en Duitse[7] universiteiten platlegden. Ze lanceerden zelfs een DDoS-aanval op het online examenplatform van een Griekse middelbare school, waardoor de normale werking van examens werd verstoord.[8]

Overheden over de hele wereld staan ook onder enorme druk door de groeiende dreiging van cyberaanvallen. Een opvallend incident deed zich voor in juli 2023, toen het eCitizen-portaal van Kenia, een kritische digitale toegangspoort, werd lamgelegd door een cyberaanval.[9] Deze verstoring maakte meer dan 5.000 overheidsservices online ontoegankelijk, met gevolgen voor essentiële functies zoals paspoortaanvragen, bezoekersvisa, rijbewijzen, ID-kaarten en gezondheidsdossiers. Bovendien had de aanval een bredere impact, waarbij mobiel bankieren en transportdiensten werden verstoord, wat aantoonde hoe onderling verbonden en kwetsbaar moderne systemen zijn.

Dit incident benadrukt een harde realiteit: in het complexe geopolitieke landschap van vandaag de dag **zijn overheden op alle niveaus** - lokaal, nationaal en federaal - **kwetsbaar voor cyberdreigingen**. Dergelijke aanvallen kunnen **verstrekkende gevolgen hebben, waarbij niet alleen gevoelige gegevens, maar ook de openbare veiligheid in gevaar komt**. De potentiële impact beperkt zich niet tot serviceonderbrekingen; het strekt zich uit tot het risico van compromitteren van vitale infrastructuur, wat economische ontwrichting kan veroorzaken en zelfs levens

5 **BBC (2023).** Schools hit by cyber attack and documents leaked.

6 **The Record (2023).** Aix-Marseille, France's largest university, hit by cyberattack.

7 **The Record (2023).** Cyberattack on German university takes 'entire IT infrastructure' offline.

8 **The Record (2023).** Cyberattack disrupts Greek national high school exams.

9 **BBC (2023).** Kenya cyber-attack: Why is eCitizen down?

in gevaar kan brengen. Bovendien omvat de nasleep van deze aanvallen vaak een kostbaar en tijdrovend herstelproces dat de publieke middelen en het vertrouwen belast. Deze verhoogde kwetsbaarheid is met name zichtbaar in de gezondheidszorgsector, waar gegevensintegriteit en -beschikbaarheid van vitaal belang zijn. Het ENISA Threat Landscape: Health Sector-rapport onthult dat **bijna de helft van de ransomware-aanvallen op openbare gezondheidsorganisaties leidt tot gegevensinbreuken of lekken**.[10]

Uit de Dreigingsmonitor die het Nederlandse expertisecentrum Z-CERT in maart vorig jaar overhandigde aan de toenmalige minister van gezondheid, Ernst Kuipers, blijkt dat het aantal ransomware incidenten in de Nederlandse zorgsector niet toeneemt, maar de impact wel groter is.[11] Oorzaak daarvan is de succesvolle aanval op Colosseum Dental.[12] Daardoor hadden in één klap 120 tandartspraktijken tijdelijk geen toegang meer tot hun patiëntendossiers. De onderneming zag zich uiteindelijk genoodzaakt het losgeld te betalen.

Deze **aanvallen op gezondheidsorganisaties zijn het afgelopen jaar in heel Europa toegenomen**.[13] Begin vorig jaar was de website van het Nederlandse Universitair Medisch Centrum Groningen (UMCG) onbereikbaar door een cyberaanval.[14] Het ging om een DDoS-aanval van de pro-Russische hackersgroep Killnet. De website met de medische dossiers van UMCG-patiënten was volgens het ziekenhuis niet aangetast.

In december 2023 werd het Duitse ziekenhuisnetwerk Katholische Hospitalvereinigung Ostwestfalen (KHO) getroffen door ransomware, waardoor verstoringen ontstonden in drie ziekenhuizen.[15] Eerder in het jaar werd een ziekenhuis in Brussel getroffen door een cyberaanval die hen dwong ambulances om te leiden naar andere ziekenhuizen.[16] In dit geval waren de IT-operaties van het ziekenhuis de dag na de aanval volledig operationeel dankzij het noodplan dat het ziekenhuis had opgesteld vóór de aanval. Dit toont **het belang aan van preventie en snelle respons bij dergelijke scenario's**.

Helaas is **snel herstel na cyberaanvallen** niet gebruikelijk, maar eerder **een uitdaging** voor overheidsorganisaties, voornamelijk **vanwege ontoereikende budgetten, verouderde technologie en onderbezette teams**. Overheidsorganisaties hebben vaak niet de middelen om voldoende preventieve beveiligingsmaatregelen te implementeren. Volgens de bevindingen van het ENISA-rapport heeft bijvoorbeeld slechts 27% van de gezondheidsorganisaties een specifiek ransomware verdedigingsprogramma en heeft 40% geen bewustwordingsprogramma voor beveiliging voor niet-IT-personeel.[17] **Het is essentieel om preventieve maatregelen te implementeren**, zoals beveiligingsaudits en een Zero-Trust Architecture. Ook het ontwikkelen van **een beveiligingscultuur met behulp van gepersonaliseerde bewustwordingstraining** draagt bij aan een verbeterde beveiliging. Dit is cruciaal, niet alleen voor de bescherming van deze organisaties, maar ook voor de veiligheid van iedereen omdat deze organisaties dienend zijn en toebehoren aan het publiek.

10 **ENISA (2023).** ENISA Threat Landscape: Health Sector.

11 **Skipr (2023).** Z-CERT verwacht binnen een jaar succesvolle ransomware aanval in de zorg.

12 **RTL Nieuws (2022).** Tandartsketen betaalt 2 miljoen euro losgeld aan criminelen na cyberaanval.

13 **RTL Nieuws (2023).** Is onze zorg tegen een cyberaanval opgewassen?

14 **NOS (2023).** Pro-Russische hackersgroep Killnet zit achter cyberaanval UMCG.

15 **Techzine (2023).** Systemen spoedeisende hulp offline na ransomware aanval.

16 **VRT (2023).** Spoedafdeling Brusselse ziekenhuis Sint-Pieter heropend na cyberaanval.

17 **ENISA (2023).** ENISA Threat Landscape: Health Sector.

CHECKLIST

Beveiliging best-practices

- **Analyseer en kwantificeer risico's:** Maak risicoanalyses en risicobeheer een integraal onderdeel van de bedrijfsvoering. Dit moet bovendien regelmatig worden gedaan, vooral bij de implementatie van nieuwe technologieën of bij het plannen van bedrijfsprocessen. Evaluaties van cyberrisico's zijn cruciaal om een nulmeting voor risico's vast te stellen, naleving te waarborgen en de integriteit van gegevens te waarborgen.

- **Zorg voor leiderschap bij digitale transformatie:** Leiders in de publieke sector zouden moeten overwegen een afdelingshoofd aan te stellen die het belang van digitale transformatie begrijpt, zoals een Chief Information Security Officer (CISO). Deze rol is essentieel voor het aansturen van digitale beveiligingsstrategieën.

- **Implementeer een Zero-Trust Architecture (ZTA):** Deze aanpak betekent geen impliciet vertrouwen verlenen en elk verzoek rigoureus verifiëren alsof het afkomstig was van een open netwerk. Het adopteren van een Zero-Trust Architecture is vooral belangrijk in het licht van het toenemende aantal complexe cyberaanvallen op de publieke sector.

- **Leer van incidenten en plan vooruit:** Gebruik de kennis die is opgedaan uit eerdere incidenten om het algehele beveiligingsmanagementproces te verbeteren. Ontwikkel een incidentresponsplan en actualiseer dit regelmatig. Dit plan moet de te nemen stappen uiteenzetten in geval van een cyberaanval, zodat er snel en effectief kan worden gereageerd om schade te minimaliseren.

- **Voer regelmatig beveiligingsaudits uit:** Voer frequente en uitgebreide beveiligingsaudits uit om kwetsbaarheden binnen het systeem te identificeren en aan te pakken. Deze proactieve benadering helpt potentiële kwetsbaarheden bloot te leggen voordat cybercriminelen ze kunnen misbruiken.

- **Implementeer gepersonaliseerde trainingsprogramma's:** Bied regelmatige trainingen aan die zijn afgestemd op de specifieke behoeften van de organisatie en de functies van haar personeelsleden. Bijvoorbeeld specifieke trainingsmodules voor de gezondheidszorgsector die ingaan op de meest toegepaste social engineering technieken voor deze sector. Ook phishing simulaties zijn effectiever wanneer ze zijn afgestemd op de sector.

INTERVIEW

John Noble

Niet-uitvoerend bestuurder en voorzitter van het Cyber Security Committee van NHS Digital in Engeland

John Noble was Directeur Incident Management bij het National Cyber Security Centre (NCSC) in het Verenigd Koninkrijk van 2016 tot 2018. Hij gaf hier leiding aan reacties op bijna 800 significante cyberincidenten die bij hebben gedragen aan het doel om het VK de veiligste plek te maken voor online zakendoen. Op dit moment is hij niet-uitvoerend bestuurder bij NHS Digital (National Health Service), waar hij voorzitter is van het Information Assurance and Cyber Security Committee.

> Door informatie te delen tussen overheden en samenwerking te bevorderen tussen het bedrijfsleven en de overheid, kunnen we opkomende dreigingen beter begrijpen.

Wat is het Nationaal Cyber Security Centrum (NCSC) en wat is het hoofddoel van deze organisatie?

De beslissing om het NCSC op te richten kwam voort uit een politiek oordeel van toenmalig premier Gordon Brown. Gezien de verschuiving naar een digitale samenleving gebouwd op het inherent onveilige internet, zag de regering de noodzaak van het oprichten van een instantie die advies en hulp kon bieden.

Waarom besloot je om het NCSC onderdeel te maken van de inlichtingendienst GCHQ?

De beslissing om het NCSC onderdeel te maken van de Government Communications Headquarters (GCHQ) inlichtingendienst was strategisch. De expertise van GCHQ op het gebied van netwerkverdediging en de reeds opgebouwde cyberbeveiligingscapaciteiten maakten het tot de ideale gastheer voor het NCSC.

Wat is de rol van het NCSC?

Toen we begonnen, moesten we uitzoeken hoe de overheid het beste kon helpen en hoe het NCSC kon bijdragen aan het realiseren van het doel om het VK de veiligste plek te maken om online zaken te doen. We realiseerden ons dat we dit moesten doen door de ervaring van de overheid te delen en invulling te geven aan een partnerschap tussen de overheid en het bedrijfsleven.

Waarom is samenwerking tussen de publieke en private sector belangrijk bij inspanningen op het gebied van cyberbeveiliging?

Zowel de overheid als het bedrijfsleven hebben unieke competenties op het gebied van cyberbeveiliging. Daarom onderzoekt het NCSC hoe de overheid middelen kan bieden voor samenwerking tussen beide. Dit leidde tot de oprichting van twee initiatieven: de Cyber Information Sharing Partnership (CISP), waarmee bedrijven anoniem informatie over cyberdreigingen in realtime kunnen uitwisselen. De Cyber 100 is een initiatief waarbij experts uit het bedrijfsleven worden ingeschakeld om hun kennis te delen met het NCSC.

Er is scepsis bij organisaties om hun kwetsbaarheden te delen met publieke entiteiten omdat ze vrezen dat deze informatie tegen hen zal worden gebruikt. Hoe kunnen we de boodschap overbrengen dat de overheid organisaties wil ondersteunen en niet wil schaden?

Hier zijn vertrouwen en openheid cruciaal. Als een inlichtingendienst een kwetsbaarheid in een stuk software ontdekt en deze niet openbaar maakt, kunnen cybercriminelen er misbruik van maken. Instanties zoals het NCSC moeten vertrouwen opbouwen bij bedrijven door te laten zien dat deze kwetsbaarheden gedeeld kunnen worden zonder nadelige gevolgen. Dit kan resulteren in zeer winstgevende en belangrijke relaties met bedrijven.

> **Er is sprake van een andere denkwijze bij de overheid waarbij de bescherming van onze digitale economie - en digitale bedrijven - topprioriteit is geworden.**

Ik denk ook dat er sprake is van een andere denkwijze bij de overheid waarbij de bescherming van onze digitale economie - en digitale bedrijven - topprioriteit is geworden. Mensen moeten begrijpen dat het beschermen van onze digitale economie betekent dat informatie wordt gedeeld met de overheid.

Wat zijn enkele belangrijke thema's die je hebt waargenomen in het dreigingslandschap gedurende de afgelopen decennia?

Het dreigingslandschap, met name cybercriminaliteit, is aanzienlijk veranderd gedurende de afgelopen decennia. Een opvallend aspect is de explosieve groei van ransomware, die het dreigingslandschap heeft getransformeerd in een geavanceerd en gespecialiseerd ecosysteem. Groepen cybercriminelen zoals Conti vertonen nu bedrijfsachtige structuren en hiërarchieën met duidelijke afdelingen en functietitels. Autoriteiten kunnen sommige van deze organisaties stoppen, maar ze leren, hervormen en passen zich aan.

Er is een toenemende trend waar te nemen waarbij cybercriminelen systemen infiltreren en niets doen. Hoe kunnen we dit verklaren?

Wanneer een kwetsbaarheid wordt blootgelegd, infiltreren kwaadwillende actoren en plaatsen ze een implantaat bij veel verschillende bedrijven. Ze doen dit gewoon zodat ze later kunnen terugkeren. Dit is het geval bij kritieke infrastructuren, waar het belangrijk is om kwetsbaarheden snel te patchen.

Het aanpakken van kwetsbaarheden kan vooral uitdagend zijn in de publieke sector omdat organisaties 24 uur per dag opereren. Kun je inzichten delen over de aanpak van de NHS om dit probleem aan te pakken?

De NHS heeft belangrijke lessen geleerd van incidenten zoals WannaCry, die een bekende kwetsbaarheid exploiteerde die veel ziekenhuisorganisaties niet hadden aangepakt. Dit incident had niet alleen financiële gevolgen, maar beïnvloedde ook de patiëntenzorg. Als reactie op kwetsbaarheden in gezondheidssystemen zijn twee belangrijke strategieën geïmplementeerd. De eerste is om duidelijk kritieke kwetsbaarheden te identificeren die actief worden misbruikt en te eisen dat deze dringend worden gepatcht. De tweede is het stellen van duidelijke verplichte standaarden waaraan organisaties zich moeten houden.

Wat voor impact heeft de centralisatie van gezondheidszorgsystemen, zoals te zien is bij de NHS in het VK, gehad op het aanpakken van uitdagingen en kwetsbaarheden op het gebied van cyberbeveiliging?

De centralisatie van gezondheidssystemen heeft zowel positieve als negatieve implicaties voor het aanpakken van uitdagingen op het gebied van cyberbeveiliging. Aan de positieve kant biedt een meer gecentraliseerd systeem duidelijkere standaarden en verwachtingen, waardoor communicatie en handhaving van cyberbeveiligingsmaatregelen in het hele netwerk eenvoudiger worden. Deze gecentraliseerde aanpak verbeterde ook de patiëntenzorg en zorgde voor snellere reacties op kwetsbaarheden. Het introduceert echter ook uitdagingen. Een gecentraliseerd systeem betekent dat een inbreuk op een deel van het systeem invloed kan hebben op andere delen, wat betekent dat een storing in één systeem een grotere impact kan hebben op het hele systeem.

Welke rol speelt geopolitiek in het vormgeven van dreigingen op het gebied van cyberbeveiliging en hoe beïnvloedt het de interactie tussen overheden en particuliere entiteiten?

Bij het analyseren van een dreiging moeten we naar twee dingen kijken: de intentie van een speler en hun capaciteit. Gebeurtenissen zoals de invasie van Oekraïne hebben geleid tot de intentie van overheden om aanvallen te gebruiken om hun oorlogsinspanningen te laten slagen. Wat betreft de capaciteit zien we dat landelijke overheden vaardigheden ontwikkelen die uiteindelijk tegen ons worden gebruikt.

Hoe zit het met hacktivisme?

Het Russische conflict heeft geleid tot een toename van hacktivisme aan beide zijden. We hebben gezien dat een cyberleger van Oekraïne aanvallen heeft uitgevoerd op Russische bedrijven, in bijvoorbeeld de mediasector. Maar we hebben ook groepen gezien zoals KillNet, die sterk zijn gericht op de Russische zaak, DDoS-aanvallen uitvoeren en heel expliciet zijn dat ze landen willen aanvallen die Oekraïne steunen.

> Het Russische conflict heeft geleid tot een toename van hacktivisme aan beide zijden.

Is er een grijs gebied van interactie tussen de commerciële kant van cybercriminaliteit en politiek gemotiveerde cybercriminaliteit?

Normaal gesproken besluit een overheid om geen cybermiddelen te gebruiken vanwege de mogelijke gevolgen, zoals de gênante situaties die het zou veroorzaken. Echter, in een context zoals de oorlog in Oekraïne, maakt het overheden niet echt uit wat anderen denken of wat de gevolgen van hun acties zijn.

We zijn overgegaan van een situatie waarin we zeer effectieve acties hadden tegen hackergroepen naar een positie waarin er nu samenwerking is tussen deze groepen en de overheid. Er is nu zelfs een discussie gaande bij leidende Russische politici over het legitimeren van aanvallen. Het zou vreselijk zijn als we in een situatie terechtkomen waarin een land criminaliteit tegen anderen legitimeert. Ik hoop echt dat het niet zover gaat komen.

Welke andere strategieën gebruiken overheden in deze samenwerking?

Ontkenning is belangrijk voor landen omdat het hen in staat stelt hun acties te verbergen. We zien dat deze overheden veel van de tools gebruiken die door criminele groepen worden ingezet om hen in staat te stellen hun verantwoordelijkheid voor deze aanvallen te ontkennen. Als bijvoorbeeld een commercieel verkrijgbare implant wordt ontdekt in een deel van de kritieke nationale infrastructuur, is het heel lastig om te achterhalen of een overheid erachter zit of niet. Daardoor is het heel gemakkelijk voor de overheid om het te ontkennen. De beschikbaarheid van deze tools stelt een overheid in staat om gebruik te maken van de criminele talentenpool.

Je hebt andere landen genoemd toen we het hadden over Rusland. Wie zijn andere belangrijke spelers in het cyberdreigingslandschap?

Als we kijken naar enkele heel belangrijke strategische kwesties, moeten we praten over de groeiende invloed van China, de spanningen in de Zuid-Chinese Zee en de houding ten opzichte van Taiwan en andere buurlanden zoals de Filipijnen. De cybercapaciteit van China heeft een aanzienlijke groei doorgemaakt, gekenmerkt door toenemende verfijning en het gebruik van nieuwe zero-day-aanvallen. Ze hebben hun inlichtingenorganisaties hervormd om conflicten te vermijden en ze zijn veel professioneler geworden. De Chinezen hebben ook hun interessegebieden verbreed. Ze hebben altijd een langetermijnvisie waarbij ze in de loop van de tijd vaardigheden opbouwen.

Europa en het VK daarentegen hebben een consistente kijk op cyber en we hebben erkend dat we meer strategisch moeten zijn in plaats van reageren op de meest recente gebeurtenissen.

Welke stappen kunnen worden ondernomen om cyberdreigingen, met name die van geavanceerde aanhoudende dreigingen (APT), te verminderen?

Door informatie op internationaal niveau te delen tussen overheden en samenwerking tussen de private sector en de overheid te bevorderen, kunnen we een alomvattend begrip van opkomende bedreigingen creëren. Door indicatoren van compromissen (IOC's) te delen en een vertrouwensrelatie tussen beide sectoren op te bouwen, kunnen we commerciële gevoeligheden overwinnen. We kunnen een gezamenlijk front vormen om opkomende bedreigingen efficiënt te detecteren en erop te reageren.

Luister hier →

Vond je dit interview interessant?

Je kunt de **volledige versie** beluisteren in onze Human Firewall podcast. Luister naar het gesprek tussen onze CEO Dr. Niklas Hellemann en John Noble over hun aanvullende inzichten inzake het belang van internationale samenwerking op het gebied van cyberbeveiliging.

7 Cyberaanvallen worden realistischer en gevaarlijker door pretexting en multichannel tactieken

Geavanceerde methoden voor sociale manipulatie, zoals **pretexting**, worden steeds vaker door cybercriminelen gebruikt om slachtoffers te exploiteren en te manipuleren voor financieel gewin of diefstal van gevoelige gegevens. Hierbij doen hackers zich voor als iemand die het slachtoffer vertrouwt en gebruiken ze een verzonnen verhaal om hen op te lichten - Volgens een rapport uit 2023 van Verizon **maken pretexting-aanvallen meer dan 50% uit van alle incidenten van sociale manipulatie**.[1] Dat laat zien dat aanvallers veel gebruik blijven maken van bedrog en manipulatie, waarbij ze altijd inspelen op menselijke emoties.

In de meest geavanceerde vorm van pretexting **onderzoeken cybercriminelen het slachtoffer via meerdere kanalen**, zoals sociale media, blogs of websites, om inzicht te krijgen in heel specifieke gegevens over het slachtoffer. Informatie die ze later kunnen gebruiken in om hun verzonnen verhaal geloofwaardiger te maken en hun slagingspercentage te verhogen.[2] Dit kan informatie zijn over de werkplek van slachtoffers, hun sociale leven, huisdieren, partners of andere persoonlijke details die criminelen helpen zeer overtuigende en op maat gemaakte verhalen te creëren die betrouwbaar overkomen op het slachtoffer.

De kanalen die cybercriminelen inzetten om deze gegevens te vinden, zijn echter niet alleen bronnen van informatie, maar ook aanvalsvectoren. Volgens onze Human Risk Review 2023 domineert e-mail phishing nog steeds en wordt maar liefst 61% van de organisaties hiermee aangevallen.[3] De cyberdreigingsomgeving breidt zich echter uit, waarbij 34% van de aanvallen nu gebruikmaakt van sociale media. Neem de vele kleine bedrijven die voornamelijk leunen op hun sociale media kanalen om klanten aan te trekken. Bij deze doelgroep is het niet moeilijk voor hackers om accounts over te nemen en bedrijven lam te leggen. Dit overkwam een klein bedrijf dat granola verkocht via Instagram.[4] Aanvallers namen contact op met de eigenaar via Instagram en deden zich voor als een ander bedrijf uit het netwerk van het slachtoffer. Ze vroegen haar op een link te klikken om voor het bedrijf te stemmen in een wedstrijd. Vervolgens namen ze haar Instagram-account over en eisten $10.000 'losgeld', wat ze betaalde om weer controle te krijgen over haar bedrijf. Maar dit

1 **Verizon (2023).** Data Breach Investigation Report.

2 **The Wall Street Journal (2021).** What Hackers Can Learn About You From Your Social-Media Profile.

3 **SoSafe (2023).** Human Risk Review.

4 **CNBC (2023).** Phishing scams targeting small business on social media including Meta are a 'gold mine' for criminals.

is slechts één voorbeeld. Cybercriminelen kunnen sociale media gebruiken om organisaties op veel verschillende manieren aan te vallen. Bijvoorbeeld door accounts van medewerkers over te nemen om met hun collega's te praten en gevoelige informatie op te vragen. Of door medewerkers schadelijke bijlagen te laten downloaden die zijn vermomd als legitieme zakelijke documenten. De gevolgen van ransomware voor kleine ondernemers is enorm.[5]

Messaging-apps zoals WhatsApp en Microsoft Teams zijn ook favoriete kanalen van hackers, zowel in ons privéleven als professioneel. Onlangs waarschuwde de politie in Kolkata, India, voor een reeks WhatsApp-aanvallen waarbij hackers de aanleiding van Wereld Yoga Dag gebruikten om berichten te versturen waarin ze yogaklassen aanboden en mensen vroegen op een link te klikken en vervolgens een zescijferige OTP-code te delen.[6] Dit gaf de aanvallers onbedoeld toegang tot het WhatsApp-account van het slachtoffer. Nadat ze het account hadden overgenomen, stuurden ze berichten naar de contacten van het slachtoffer, waarin ze een gevoel van urgentie creëerden en om geld vroegen.

Bij een andere aanval met de professionele app Microsoft Teams stuurden aanvallers berichten naar hun slachtoffers waarin ze zich voordeden als medewerker van het HR-team en beweerden dat hun vakantieplanning was gewijzigd.[7] De aanvaller drong er bij de slachtoffers op aan een bestand met de vakantieplanning te downloaden, wat in plaats daarvan een malware genaamd DarkGate laadde.

Maar cybercriminelen gaan nog veel verder. Ze veranderen en verbeteren voortdurend hun tactieken om hun aanvallen overtuigender te maken. En ze orkestreren nu ook **zeer geavanceerde aanvallen waarbij ze contact opnemen met hun slachtoffer via meerdere kanalen**, zoals sms, e-mail of telefoongesprekken. Neem het voorbeeld waarbij een vrouw werd opgelicht met een combinatie van sms- en voice-phishing.[8] De aanvallers stuurden haar een sms met de vraag of ze een overschrijving van $ 7.500 had geautoriseerd. Kort daarna maakte ze misbruik van de bij het slachtoffer ontstane angst door haar te bellen en zich voor te doen als fraudeonderzoeker. Ze vroegen haar om haar referenties te wijzigen om te voorkomen dat een oplichter er met haar geld vandoor zou gaan. Op die manier slaagde de aanvallers erin $ 15.000 te stelen van beide bankrekeningen van het slachtoffer.

Deze aanvallen met meerdere kanalen worden nog overtuigender en effectiever wanneer gebruik wordt gemaakt van AI technologie. Een schrijnend voorbeeld hiervan deed zich voor bij een medewerker van Retool.[9] Eerst stuurden de aanvallers een sms naar het slachtoffer waarin ze zich voordeden als het IT-team dat bezig was met het oplossen van een probleem met de loonadministratie. De medewerker voerde vervolgens hun referenties in op een nep-landingspagina. Omdat de medewerker MFA had ingeschakeld, moesten de cybercriminelen het slachtoffer bellen met een door AI gegenereerde gekloonde stem van een IT-teamlid en vroegen om de OTP-token om deze te omzeilen. Van daaruit slaagden de aanvallers erin de accounts van 27 klanten over te nemen en duizenden dollars aan crypto currency te stelen.

Nu cybercriminelen telkens een tandje bijzetten met zeer geavanceerde en professionele tactieken, **moeten wij extra voorzichtig zijn en ervoor zorgen dat veilig gedrag in ons DNA is ingebed**.

5 **RTL Nieuws (2021).** Ransomware raakt kleine ondernemers keihard: 'Ik zie bedrijven kapot gaan'.

6 **The Times of India (2023).** Police warns netizens about WhatsApp hacking, here's how fraudsters hack accounts.

7 **Decipher (2023).** Threat actors deliver DarkGate malware via Skype, Teams Chats.

8 **The Guardian (2023).** Gone in seconds: rising text message scams are draining US bank accounts.

9 **The Hackers News (2023).** Retool Falls Victim to SMS-Based Phishing Attack Affecting 27 Cloud Clients.

CHECKLIST

Beveiliging best-practices

- **Geef training over het verifiëren van afzenders en bellers:** Het is belangrijk om je werknemers te trainen om de identiteit van afzenders en bellers zelfstandig te verifiëren. Zelfs als een inkomende oproep legitiem lijkt, is het veiliger om de persoon rechtstreeks te benaderen via een apart vertrouwd kanaal als het gaat om gevoelige verzoeken of als het verdacht lijkt.

- **Controleer externe partijen:** Wees waakzaam bij externe partijen die contact hebben met je systemen. Wanneer ze toegang tot gevoelige informatie nodig hebben, bevestig dan dat ze voldoen aan de cyberbeveiligingsnormen van je organisatie.

- **Stimuleer snelle en onbezorgde rapportage:** Stimuleer een cultuur waarin werknemers onmiddellijk elke phishing poging of ongebruikelijke activiteit melden zonder angst voor repercussies. Snel en onbezwaard rapporteren, stelt beveiligingsteams in staat direct te handelen en voorkomt mogelijk dat een aanval verergert.

- **Houd beveiligingsbeleid actueel:** Herzie je beveiligingsbeleid voortdurend en integreer opkomende social engineering tactieken zoals pretexting. Met een up-to-date beleid blijft je verdediging sterk en effectief.

- **Verbeter incident response plannen:** Werk regelmatig je incident response (IR) strategieën bij om de impact van succesvolle pretexting aanvallen of andere methoden te verminderen. Stel duidelijke procedures vast voor het detecteren, beheren en beperken van aanvallen om de bedrijfscontinuïteit en beveiliging te waarborgen. Zorg er ook voor dat je de IR-plannen continu verbetert en periodiek tafeloefeningen uitvoert om de IR-vaardigheden te trainen.

- **Blijf medewerkers continu trainen:** Bied doorlopende training aan over de nieuwste bedreigingen op het gebied van cyberbeveiliging, inclusief pretexting en multichannel aanvallen. Maak opgedane kennis praktisch toepasbar met simulaties die je personeel trainen in situaties uit het echte leven. Het opleiden van werknemers in het herkennen en omgaan met verdachte activiteiten is essentieel om een waakzame werknemerspopulatie te ontwikkelen die in staat is frauduleuze plannen te identificeren en af te wenden.

8 Stijgende burn-outcijfers dagen cyberbeveiligingsteams uit als nooit tevoren

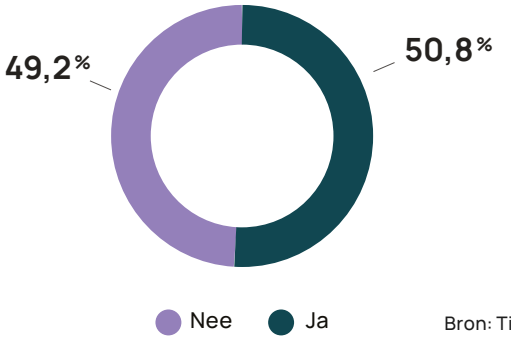
We hebben het vorig jaar al gehad over het probleem van burn-out bij beveiligingsteams. De recente wereldwijde spanningen en de voortdurende professionalisering van cybercriminaliteit, nog extra aangewakkerd door op AI gebaseerde tools, maken aanvallen niet alleen nog complexer en moeilijker te detecteren, maar leggen ook ongekende druk op beveiligingsprofessionals. In deze voortdurende golf van uitdagingen worden de veerkracht en het aanpassingsvermogen van onze teams getest als nooit tevoren.

Ook onderzoek- en adviesbureau Gartner waarschuwt dat stress de personeelsbezetting in de beveiligingssector verder onderdruk zetten.[1] Bijna de helft van de managers op het gebied van cyberbeveiliging verandert tegen 2025 van baan en 25% van functie door meerdere werkgerelateerde stressfactoren, meldt de marktonderzoeker.

Een belangrijke factor die de druk nog verder vergroot, is het tekort aan geschoolde arbeidskrachten in de branche. Volgens het laatste rapport van ISC2 zijn er wereldwijd 3,9 miljoen onvervulde posities op het gebied van cyberbeveiliging, een verhoging van 12,6% in 2023 in vergelijking met 2022.[2] Met de grootste stijgingen in Azië-Pacific (vooral Japan en India) en Noord-Amerika. Europa blijft ook niet achter met een groei van 9,7% in het tekort aan cyberbeveiligingspersoneel ten opzichte van vorig jaar. Maar dat is nog niet alles. Volgens een studie van ISACA heeft 59% van de organisaties een tekort aan cyberbeveiligingspersoneel, wat de werkdruk voor bestaande teams dramatisch **verhoogt en beveiligingsfunctionarissen vaak tot aan de rand van burn-out of zelfs ontslag drijft**.[3]

Een enquête onder meer dan duizend leden van beveiligingsteams in de VS en Europa bevestigt dit: **66% van de respondenten heeft last van aanzienlijke werkdruk**, 51% heeft medicatie voorgeschreven gekregen voor geestelijke gezondheid en 19% gebruikt meer dan drie alcoholische dranken per dag om met de situatie om te kunnen gaan.[4] Maar het gaat veel verder dan een last voor het individu. Het kan er ook voor zorgen dat **teams belangrijke details over het hoofd zien, waardoor hun vermogen om effectief te reageren op bedreigingen wordt aangetast** en het risico op beveiligingsinbreuken in hun organisaties aanzienlijk wordt verhoogd.

Heeft een arts ooit medicatie voorgeschreven voor je geestelijke gezondheid?



Bron: Tines[4]

1 **Dutch IT Channel (2023).** Gartner: Stress kan personeelsbezetting in security sector onder druk zetten.

2 **ISC2 (2023).** How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce.

3 **ISACA (2023).** New ISACA Research: 59 Percent of Cybersecurity Teams are Understaffed.

4 **Tines (2022).** State of Mental Health in Cybersecurity.

Dit risico wordt verder versterkt door het feit dat cybercriminelen voortdurend hun technieken evolueren en steeds geavanceerder worden in hun aanvallen, zoals we al hebben gezien in de vorige secties.

Het geval van AccessPress is een goede illustratie van de enorme uitdagingen waarmee beveiligingsteams worden geconfronteerd.[5] Als aanbieder van WordPress-plugins was AccessPress het doelwit van een geavanceerde cyberaanval. Hackers compromitteerden 40 thema's en 53 plugins die werden gebruikt op meer dan 360.000 actieve websites. Dit maakt ook de potentiële reikwijdte van aanvallen op de softwaretoeleveringsketen duidelijk. De verstrekkende compromittering, die de aanvallers toegang gaf tot een groot aantal websites, illustreert de ernst en complexiteit van dreigingen in het hedendaagse cybersecurity landschap. Het toont niet alleen de technische uitdagingen, maar ook de menselijke aspecten van cybersecurity, met name de druk op beveiligingsteams.

Naast het beschermen van andere afdelingen binnen de organisatie en het snel reageren op aanvallen, behoren beveiligingsteams volgens onze Human Risk Review 2023 zelf tot de afdelingen die het meeste risico lopen om slachtoffer te worden van cyberaanvallen.[6] Een van de redenen hiervoor is dat cybercriminelen zich bewust zijn van het feit dat stress beveiligingspersoneel kwetsbaarder kan maken. Zij gebruiken teamburn-out strategisch als een ingang voor hun aanvallen. Door organisaties te onderzoeken, identificeren ze bedrijven waarvan de teams tekenen vertonen van overwerktheid of stress, waardoor ze primaire doelwitten worden.

In deze dynamische en uitdagende omgeving **is het essentieel dat organisaties investeren in hun beveiligingsteams** om het welzijn van hun medewerkers te bevorderen. Het is belangrijk om passende budgetten toe te wijzen en loopbaanplannen voor behoud te ontwikkelen om burn-out te verlichten, talent te behouden en voldoende middelen te hebben om de juiste beveiligingsmaatregelen te kunnen implementeren. Alleen wanneer deze stappen worden gezet, zullen teams effectief kunnen werken om cyberaanvallen tegen te gaan en de beveiliging te verhogen.

> **De grootste uitdaging in de cybersecuritysector op dit moment is burn-out: er is sprake van te veel data, te veel gevallen en niet genoeg tijd.**

Stéphane Duguin
CEO van het CyberPeace Institute

5 **WP Handleiding.** AccessPress thema's en plugins kwetsbaar door backdoor.

6 **SoSafe (2023).** Human Risk Review.

CHECKLIST

Beveiliging best-practices

- **Geef een hoge prioriteit aan mentale gezondheid en werk-privébalans:** Ontwikkel programma's ter ondersteuning van de mentale gezondheid en het welzijn van leden van het beveiligingsteam. Flexibele werktijden, toegang tot counselingdiensten en regelmatige pauzes kunnen allemaal bijdragen aan het voorkomen van burn-out.
- **Implementeer effectieve dreigingsdetectietools:** Gebruik geavanceerde tools, zoals op AI gebaseerde dreigingsdetectietools, phishing meldknoppen en andere tools zoals de e-mail assistent PhishFeedback van SoSafe. Hiermee verminder je de tijd en moeite die nodig is om dreigingen te identificeren.
- **Automatiseer e-mailanalyse:** Implementeer automatiseringstools specifiek voor teams van het Security Operations Center (SOC) om gemelde e-mails te analyseren. Door het proces van het evalueren van potentiële bedreigingen vanuit e-mails op die manier te stroomlijnen, kunnen SOC-teamleden zich concentreren op meer essentiële en complexe beveiligingskwesties.
- **Automatiseer routinetaken:** Gebruik automatisering voor terugkerende en routinetaken, dan kunnen beveiligingsprofessionals zich concentreren op de meer complexe en strategische aspecten van cybersecurity.
- **Stimuleer training en bijscholing:** Bied doorlopende training en bijscholingsprogramma's aan om de vaardigheden van teams te verbeteren die ze nodig hebben om het hoofd te bieden aan de nieuwste cyberdreigingen en technologieën. Faciliteer daarnaast onderlinge samenwerking en zorg ook voor beveiligingsspecialisten in andere technische teams.
- **Investeer in het behoud van werknemers:** Ontwikkel loopbaanplannen en ontwikkelingsprogramma's om talent te behouden en het verloop te verminderen.
- **Houd regelmatige feedbacksessies en beoordelingsgesprekken:** Voer regelmatig één-op-één gesprekken om feedback te geven en te ontvangen zodat je de behoeften van medewerkers begrijpt en hierop kunt inspelen.

Gedurende 2024 kun je meer inbreuken verwachten waar de **menselijke factor** bij betrokken is

Alle trends van dit jaar hebben één ding duidelijk gemaakt: onze cybersecurity maatregelen zullen onvolledig blijven totdat we ons richten op mensen, net zoals hackers dat doen. Zij weten dat hun grootste kans op succes ligt in het bespelen van menselijke emoties en daarom staat social engineering centraal in hun praktijken, zoals we herhaaldelijk hebben gezien in dit rapport.

Het Data Breach Investigations Report van Verizon schatte dat bij maar liefst 74% van de inbreuken in 2023 een menselijk element betrokken was.[1] Zelfs op technologie gerichte brancheorganisaties erkennen nu de rol van mensen bij het exploiteren van technologie. Dit is slechts het begin van wat komen gaat. **In 2024 zal het percentage van inbreuken met een menselijk element nog verder toenemen**, als we het Predictions 2024-rapport van Forrester mogen geloven.[2] Met de professionalisering van cybercriminaliteit en de opkomst van AI kunnen cybercriminelen nu echt overtuigende en complexe social engineering aanvallen creëren. Dit maakt het moeilijker om het verschil te zien tussen echte en kwaadwillende berichten. En met meer digitale communicatiemogelijkheden verspreiden deze bedreigingen zich ook nog eens sneller dan ooit.

De Allianz Risk Barometer 2024 schat ook in dat cyberincidenten het grootste wereldwijde zakelijke risico zullen zijn in 2024.[3] Het is daarom geen optie meer voor beveiligingsleiders om het menselijke element in hun beveiligingsstrategieën te negeren. Het goede nieuws is dat er een krachtige tegenmaatregel is voor dit risico: **cybersecurity bewustzijn en -training**. Door cybersecurity naar de mensen te brengen en veilig gedrag vanzelfsprekend te maken, kunnen we het gevaar van cyberdreigingen verminderen. Onthoud, het zijn niet alleen systemen, maar mensen die doelwit zijn en die de gevolgen van cyberaanvallen dragen. Het zijn tegelijkertijd ook **mensen die de kracht hebben om deze aanvallen te stoppen**.

Het ontwikkelen van een veiligheidscultuur is niet alleen de verantwoordelijkheid van het bedrijf, maar ook een persoonlijke. Samen kunnen we de dreiging van geavanceerde cybercriminaliteit terugdringen en onze toekomst beschermen.

1 **Verizon (2023).** Data Breach Investigations Report.

2 **Forrester (2024).** Predictions 2024: Exploration Generates Progress.

3 **Allianz (2024).** Allianz Risk Barometer 2024.

Versterk je veiligheidscultuur met gemak

Met zijn awareness platform stelt SoSafe organisaties in staat om hun veiligheidscultuur te versterken en menselijke risico's te minimaliseren. Het platform levert boeiende leerervaringen en slimme aanval simulaties waarmee medewerkers actieve beschermers worden tegen online dreigingen. Alles gebaseerd op gedragswetenschap om leertrajecten leuk en effectief te maken. Uitgebreide analyses meten de impact van de gedragsverandering en vertellen organisaties precies waar de kwetsbaarheden zitten, zodat zij proactief kunnen inspelen op cyberdreigingen. Het SoSafe platform is makkelijk te gebruiken en op te schalen en stimuleert moeiteloos veilige gewoontes bij elke medewerker.

TEACH — Interessant microleren

Een op gedragswetenschap gebaseerd trainingsplatform waar medewerkers mee weglopen. Versterk je weerbaarheid tegen cyberdreigingen en voldoe aan complianceverplichtingen met behulp van dynamische en impactvolle leerervaringen via verschillende kanalen en ontwikkel eenvoudig blijvend veilig gedrag.

- Verhaalgedreven, gegamificeerde trainingscontent die is ontwikkeld om te boeien en te blijven hangen
- Zorgvuldig samengestelde contentbibliotheek met handleidingen, schaalbaar voor elke groei
- Aanpasbaar met beperkte inspanning en contentmanagement die bij elke organisatie past

TRANSFER — Slimme aanval simulaties

Gebruikersgerichte phishing simulaties die veilige gewoontes bevorderen. Train je medewerkers in hoe zij cyberaanvallen kunnen herkennen met regelmatige geautomatiseerde spear phishing simulaties die leiden tot blijvende security awareness in hun dagelijkse werk. Zo verminder je op een effectieve manier risico én cruciale tijd die nodig is om een dreiging te ontdekken.

- Gepersonaliseerde en realistische cyberaanval simulaties
- Context-gebaseerde trainingshandleidingen om veilig medewerkergedrag te stimuleren
- Eenvoudig melden van dreigingen met één druk op de Phishing Report Button

ACT — Monitoren van strategische risico's

Bescherm je organisatie tegen kostbare incidenten door gebruik te maken van onze uitgebreide human risk assessment oplossing. Ontvang een compleet overzicht van je menselijke beveiliging zodat je potentiële kwetsbaarheden voor kunt blijven. Monitor en interpreteer de impact van je awareness programma, analyseer gedrag en neem datagedreven besluiten.

- Contextuele inzichten, inclusief technische en gedrags-KPI's
- Branch benchmarks en praktische richtlijnen
- Gebouwd volgens ISO/IEC-27001 eisen op basis van een privacy-by-design aanpak

CONNECT — Sofie Rapid Awareness

Cybercriminelen ontwikkelen zich sneller dan ooit, maar dat kun jij ook. Met Sofie Rapid Awareness leg je direct contact met je medewerkers in MS Teams. Voor snelle, korte e-learning sessies om nieuwe bedreigingen aan te pakken, je team te informeren via directe waarschuwingen en hen te transformeren tot je sterkste verdediging.

- Leg direct contact met je medewerkers in MS Teams
- Bespaar tijd en communiceer met gemak
- Verstuur korte beveiligingswaarschuwingen die medewerkers eenvoudig kunnen verwerken
- Meet het resultaat en zie hoeveel mensen de waarschuwing hebben gezien

Human Firewall Conference

HuFiCon is een Europees cybersecurity evenement dat is ontworpen om security professionals te helpen hun teams te transformeren in cybersecurity helden. Doe mee met expert talks, hands-on workshops en draag bij aan een gemeenschap die zich inzet om mensen centraal te stellen in cybersecurity.

Ben jij klaar om de toekomst van cybersecurity te leiden?

Registreer nu voor HuFiCon24

Waar? Halle Tor 2, Keulen

Wanneer? 14-15 november 2024

Contact

Voor aanvullende vragen over dit rapport kun je contact opnemen met:

Laura Hartmann
Hoofd Corporate Communicatie
press@sosafe-awareness.com

SoSafe GmbH
Lichtstrasse 25a
50825 Keulen, Duitsland

info@sosafe.de
www.sosafe-awareness.com/nl
+49 221 65083800