Baobab
Risk Solutions

Data Breach Report

Het MKB als doelwit: niet te klein om interessant te zijn

Inleiding

Als verzekeraar van digitale risico's beoordelen we bij Baobab continu beide dimensies van het risico: de technische kwetsbaarheid vóór de aanval en de financiële schade die erop volgt. Onze data-analyse onthult: er is een scheur in het beveiligingslandschap. Terwijl grote bedrijven hun digitale deuren steeds vaker vergrendelen, staan ze in het midden- en kleinbedrijf vaak nog wijd open. Maar onze gegevens tonen ook hoop: de meeste aanvallen zijn niet hoogcomplex, maar opportunistisch. Dit betekent: bedrijven zijn niet hulpeloos aan het risico overgeleverd. Met de juiste maatregelen kan het gevaar drastisch worden verminderd. Onze bevindingen zijn gebaseerd op de continue analyse van Deep Scans en op de inflow van offertetrajecten. Hoewel deze dataset geen aanspraak maakt op volledige statistische representativiteit voor de gehele markt, laten de onderzochte gevallen en de langetermijnobservatie duidelijke, betrouwbare trends zien.

Inhoud

Dataset

>10.000 aanvalsoppervlakte-scans geanalyseerd

57.660 gelekte datasets uit > 5.000 bronnen geanalyseerd

>100 echte schadegevallen geanalyseerd

>100 externe ransomware cases onderzocht

Samenvatting

88,7% van de gelekte gegevens herhaalt zich

Hackers hoeven het wiel niet opnieuw uit te vinden. De meerderheid van de in het dark web gevonden inloggegevens komt uit massale, historische aggregaties. Wie eenmaal in het netwerk van info-stealers belandt, blijft daar jarenlang als doelwit gemarkeerd, omdat gegevens systematisch opnieuw worden verpakt en geautomatiseerd tegen netwerken worden ingezet.

Wachtwoorden zijn niet voldoende als bescherming

De complexiteit van een wachtwoord is van secundair belang als het in platte tekst in databases te koop staat. Onze analyse toont aan: zonder multi-factor authenticatie (MFA) blijft de initiële toegang triviaal. Aanvallers breken niet in, ze loggen zich eenvoudig in met geldige, goedkoop verworven inloggegevens.

75% van alle bedreigingen zijn geconcentreerd

De externe aanvalsfocus ligt voornamelijk op de rand van het netwerk (VPN's/firewalls) en communicatiehulpmiddelen (e-mail). Deze twee categorieën maken ongeveer driekwart van de totale bedreigingssituatie uit en dekken bijna alle zero-day signalen. Daarom ligt de prioriteit bij het beveiligen van internet-exposed systemen, aangezien aanvallen hier bijzonder vaak voorkomen.

Hoeveelheid data weegt zwaarder dan omzet

De misvatting "We zijn te klein om een doelwit te zijn" is levensgevaarlijk. Hackers meten aantrekkelijkheid niet aan de omzet, maar aan de hoeveelheid persoonlijke gegevens (PII). Zelfs bij bedrijven met minder dan 5 miljoen € omzet beheert 31% meer dan 10.000 datasets - een perfect doelwit voor aanvallen.

In plaats van in te breken, gewoon een wachtwoord kopen

Het is een veelvoorkomende misvatting dat cybercriminelen complexe code moeten ontwikkelen om firewalls te omzeilen. De realiteit is veel banaler en economischer: waarom een complexe inbraak als je de sleutel voor een paar euro op het dark web kunt kopen? Gecompromitteerde identiteiten zijn tegenwoordig het goedkoopste en meest effectieve wapen in het arsenaal van aanvallers.

Het archief van de verschrikking

Onze analyse toont aan dat hackers zelden complexe versleutelingen hoeven te omzeilen. De meerderheid van de in het dark web gevonden inloggegevens is in platte tekst beschikbaar - ze zijn onmiddellijk leesbaar en inzetbaar.

91% van de geanalyseerde datalekken bevat wachtwoorden in platte tekst. Dit maakt de initiële toegang voor aanvallers triviaal en extreem kosteneffectief.

Deze eenvoudige beschikbaarheid van wachtwoorden maakt cybercriminaliteit niet alleen eenvoudig, maar ook uiterst lucratief. Een voorbeeld uit een door ons geanalyseerd Telegram-kanaal illustreert het businessmodel: via een eenvoudig abonnement krijgen kopers daar wekelijks toegang tot minstens 5.000 datasets.

Voorbeeld van een Darknet-aanbieding

Bron: Darknet-Telegram-kanaal

Aanbieding

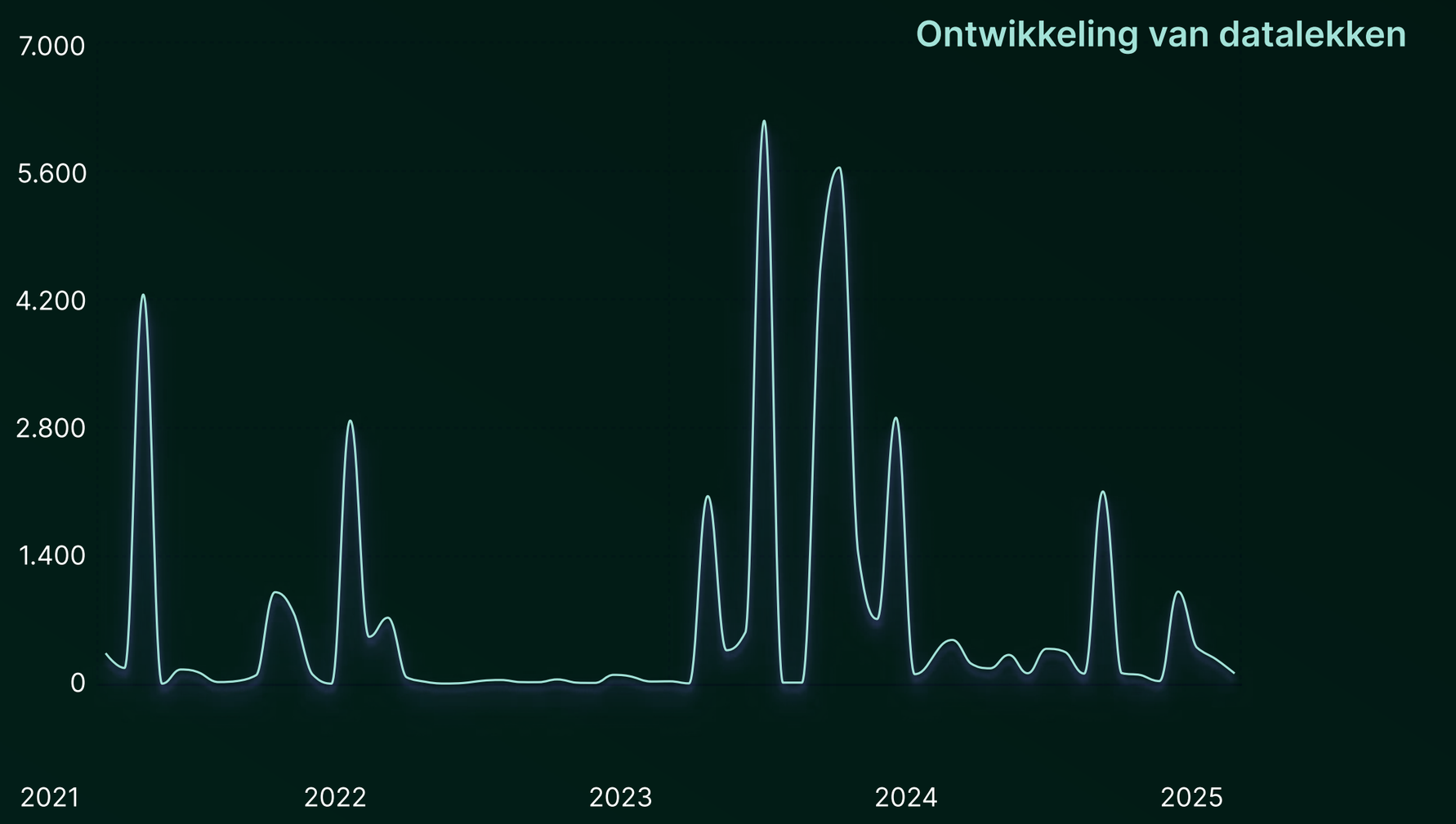
- Toegang tot het exclusieve kanaal
- Dagelijks 5.000 - 15.000 gestolen gegevens
- Maandabonnement inclusief overdracht van 45.000 logs

Prijzen

- Een week: 75$
- Twee weken: 150$
- Een maand: 250$
- Drie maanden: 600$

Mega-inbreuken op Info-Stealers

Terwijl in het verleden individuele diefstallen bij bedrijven zoals Adobe of LinkedIn de krantenkoppen domineerden, zien we momenteel een verschuiving naar Info-Stealer-logs.



Wat zijn Info-Stealers?

Dit zijn malware die zich ongemerkt op apparaten nestelt en daar inloggegevens direct uit de browser, uit wachtwoordmanagers of uit actieve sessies (sessie-cookies) extraheert. Deze logs zijn bijzonder gevaarlijk, omdat ze vaak actuele wachtwoorden bevatten en eenmaal gelekte gegevens blijven in omloop. Onze gegevens tonen een duplicatiepercentage van ongeveer 88,7% - dat betekent dat dezelfde gestolen gegevens steeds weer in verschillende dataverzamelingen opduiken.

Chandan Raj Nivanda
Cybersecurityonderzoeker

"We zien een duidelijke verschuiving in de aanvalstrategie: van enkele, massale server-hacks naar schaalvergroting door duizenden kleine info-stealer."

De omvang van de beveiligings-kwetsbaarheid

Veel bedrijven geloven dat een datalek slechts één of twee afzonderlijke accounts betreft. Onze analyse onthult echter een veel systemischer risico: voor het gemiddelde bedrijf is de bedreiging geen kleine vergissing, maar een massaal probleem dat een groot aantal gecompromitteerde wachtwoorden omvat.

Meerdere lekken	Onze analyse identificeerde gemiddeld 18 wachtwoorden per bedrijf.
Hoog gevaar	In sommige bedrijven is het risico bijzonder hoog: bij 23 bedrijven zijn tussen de 100 en 400 individuele wachtwoorden op het dark web gevonden.
Blijvend risico	Als een domein herhaaldelijk in deze datasets voorkomt, is dit vaak een teken dat beveiligingslekken jarenlang onopgelost zijn gebleven. Gestolen gegevens stapelen zich zo continu op.

Wachtwoord-paradox

Ondanks voortdurende waarschuwingen van systeemleveranciers over onveilige wachtwoorden, domineren nog steeds schokkend voorspelbare patronen. Onze analyse toont aan dat de grote meerderheid van de gecompromitteerde inloggegevens nog steeds op eenvoudige cijferreeksen is gebaseerd - waarbij 123 het meest gebruikte startpunt is.

Typische patronen

Ook voornamen zoals Hannah en Michael of termen zoals Backend, deurbel en Star Wars komen vaak voor.

De meest voorkomende wachtwoorden

Rang 1	12345678
Rang 2	123456

Geanalyseerde patronen

Korte woorden · Filmtitels · Steden · Namen · Nummers

Het risico

Of het nu eenvoudige cijferreeksen zoals 123456 zijn of triviale termen zoals Starwars – het gebruik van zwakke wachtwoorden blijft een groot risico. Hoewel dergelijke wachtwoorden steeds vaker in een privécontext worden gebruikt, zoals voor het doen van online boodschappen.

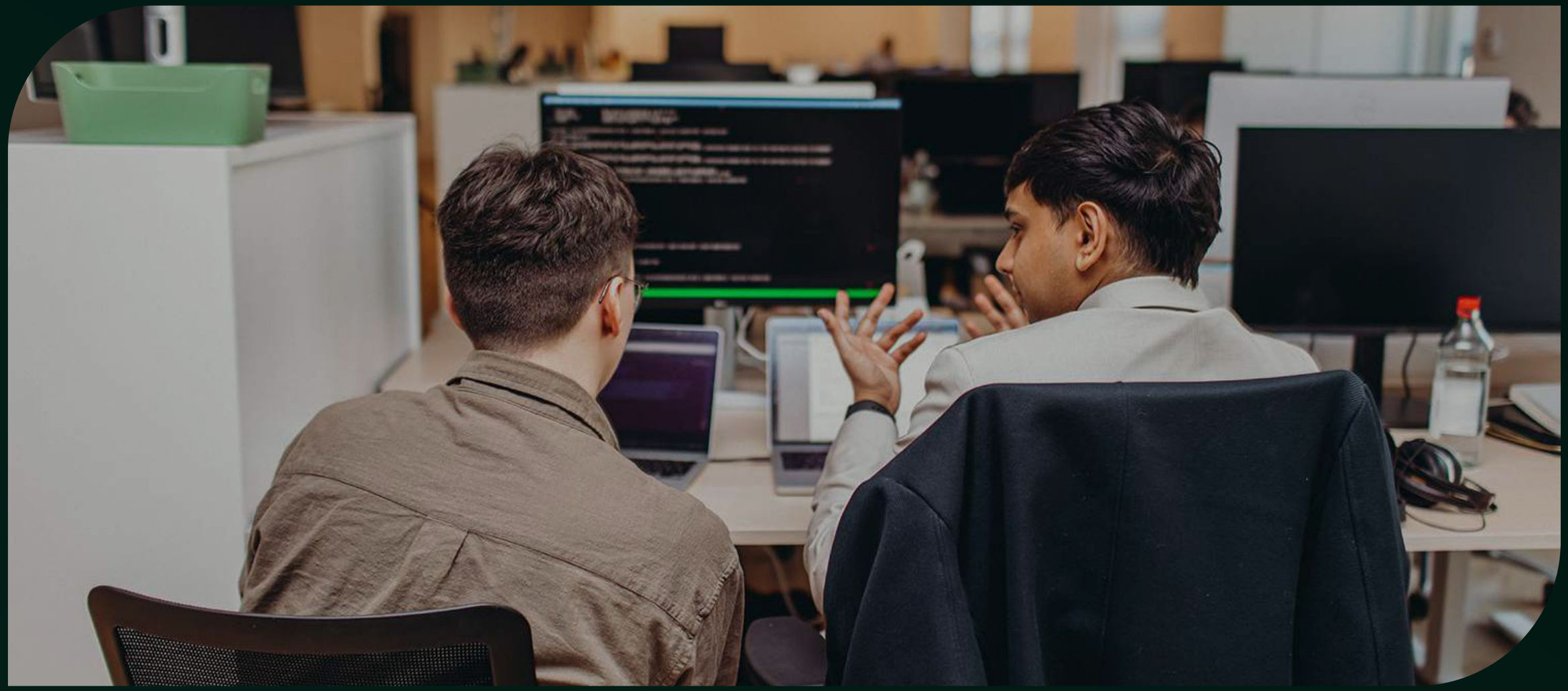
Maar het gevaar gaat dieper: onze analyse toont aan dat zelfs complexe, willekeurig gegenereerde tekenreeksen massaal in datalekken verschijnen.

Andrew Saula
Head of Cybersecurity

"Criminele groeperingen doen tegenwoordig niet meer de moeite om wachtwoorden te kraken; ze voegen gecompromitteerde inloggegevens rechtstreeks in geautomatiseerde tools in (Credential Stuffing). Zonder extra factoren zoals Multi-Factor Authenticatie (MFA) blijft de initiële toegang tot de bedrijfsarchitectuur triviaal, ongeacht de complexiteit van het wachtwoord."

Het aanvalsoppervlak

Terwijl gecompromitteerde wachtwoorden de primaire toegang tot systemen omzeilen, gedragen softwarekwetsbaarheden zich als onzichtbare scheuren in de fundamenten van de IT-architectuur. Om deze risico's te identificeren, doorlicht onze Deep-Scan-technologie de IT-infrastructuur van onze klanten en controleert deze bij elke scan op 10.355 kwetsbaarheden (CVE's).



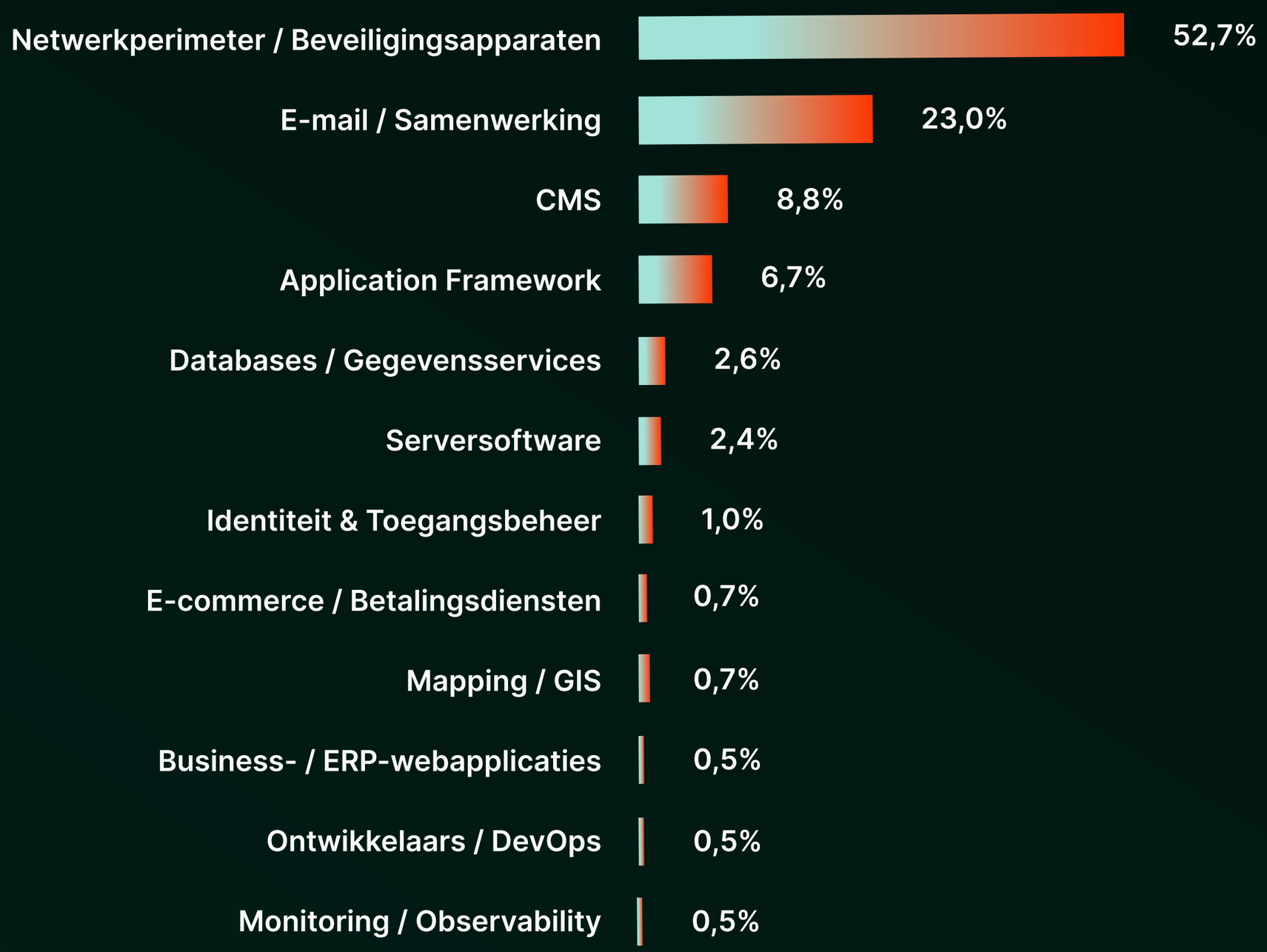
De onderschatte hiaten

Bij cyberbedreigingen is het gevaar niet gelijkmatig verdeeld, maar geconcentreerd. De externe aanvalsfocus in het MKB ligt bijna uitsluitend op de Network Edge (netwerkperiferie) en e-mail. Deze twee categorieën maken driekwart van het totale dreigingslandschap uit en dekken bijna alle actieve of zero-day signalen. CMS en applicatie-frameworks blijven relevant, maar staan duidelijk achter deze eerste risicolaag.

Voor bedrijven is de prioriteit bij verdediging dan ook duidelijk: beveilig eerst de naar het internet blootgestelde lagen. Hier zijn aanvallen het hardnekkigst en zijn de potentiële schade het grootst.

75% van alle kritische bedreigingsactiviteiten concentreert zich op twee gebieden: de Network Edge (VPN's/ firewalls) en samenwerkingshulpmiddelen (e-mail).

Meest voorkomende aanvaldoelen per technologie



Kleine bedrijven, grote kansen

Onze gegevens tonen een duidelijke correlatie tussen de grootte van bedrijven en patchdiscipline. Terwijl grote bedrijven meestal over gespecialiseerde teams voor IT-beveiliging beschikken, blijven kleinere organisaties hier vaak achter:

12,7%

Kritieke kwetsbaarheden komen voor bij bedrijven met minder dan 1 miljoen € omzet.

6,23%

Kritieke kwetsbaarheden komen voor bij bedrijven met meer dan 100 miljoen € omzet.

Verouderde software

Hoe kleiner het bedrijf, hoe ouder de software vaak is. Verouderde VPN-gateways of ongepatchte Exchange-servers zijn als open ramen op de begane grond – een uitnodiging voor ransomwaregroepen.

Terwijl het systeemonderhoud in grote bedrijven door aangewezen IT-afdelingen wordt beheerd, wordt het in MKB's vaak slechts reactief of naast de hoofdtaak uitgevoerd vanwege een gebrek aan personeel. Juist dit gebrek aan vaste middelen verklaart waarom de kritieke kwetsbaarheden bij bedrijven met een omzet van 100 miljoen € bijna gehalveerd zijn.

Klein in omzet, groot in risico

Een gevaarlijke misvatting houdt hardnekkig stand in het management van kleinere bedrijven: "We zijn te klein om een doelwit te zijn." Deze misvatting is gebaseerd op de aanname dat aanvallers hun doelwitten handmatig selecteren. De huidige realiteit wordt echter gedomineerd door massale automatisering. Dadergroepen scannen het hele internet in een fractie van een seconde op open kwetsbaarheden en onbeschermde interfaces. Een geautomatiseerde bot-scan zoekt simpelweg naar de weg van de minste weerstand. Wie een kwetsbaarheid vertoont, wordt een doelwit.

Onze analyse toont aan: de aantrekkelijkheid voor hackers wordt niet gemeten aan de omzet, maar aan de gegevens.

De verborgen schat

We hebben bedrijven met minder dan 5 miljoen € jaarlijkse omzet geanalyseerd. Het resultaat weerlegt de mythe van onbelangrijkheid:

31% van alle kleine bedrijven beheert meer dan 10.000 PII-gegevens.

De prijs van PII

Een enkele gestolen dataset kost gemiddeld ongeveer 134€. Verliest een bedrijf 10.000 datasets, dan ligt de theoretische totale schade al snel op 1,34 miljoen €. Voor een bedrijf met minder dan 5 miljoen € jaaromzet is dat desastreus.

11% van alle kleine bedrijven beheert tussen de 100.000 en 500.000 datasets.

Voor een aanvaller is zo'n bedrijf een goudmijn. Een dataset is op de zwarte markt geld waard - de omzet is de hacker om het even. Zelfs als de hacker de gegevens niet doorverkoopt, zijn ze extreem waardevol.
Bij moderne ransomware-aanvallen zoals Double Extortion worden de systemen niet alleen versleuteld, maar worden de gegevens ook onopgemerkt gekopieerd en geëxfiltreerd.

De hacker dreigt het bedrijf dan: "Als je geen losgeld betaalt, publiceer ik de gegevens van je klanten." De angst voor GDPR-boetes, rechtszaken van klanten en reputatieverlies dwingt het bedrijf vaak tot betaling. De eigen gegevens worden zo de perfecte gijzelaar.

Het ontbrekende schild

Ondanks dit risico ontbreekt vaak de belangrijkste bescherming: de multi-factor-authenticatie (MFA). Onze gegevens tonen aan: pas vanaf 50 miljoen € omzet behoort MFA tot de standaard in de IT-beveiliging.

Statistiek: Bedrijven zonder MFA

53%
<5 miljoen € omzet

46%
<50 miljoen € omzet

28%
>50 miljoen € omzet

Gevaarlijke kloof

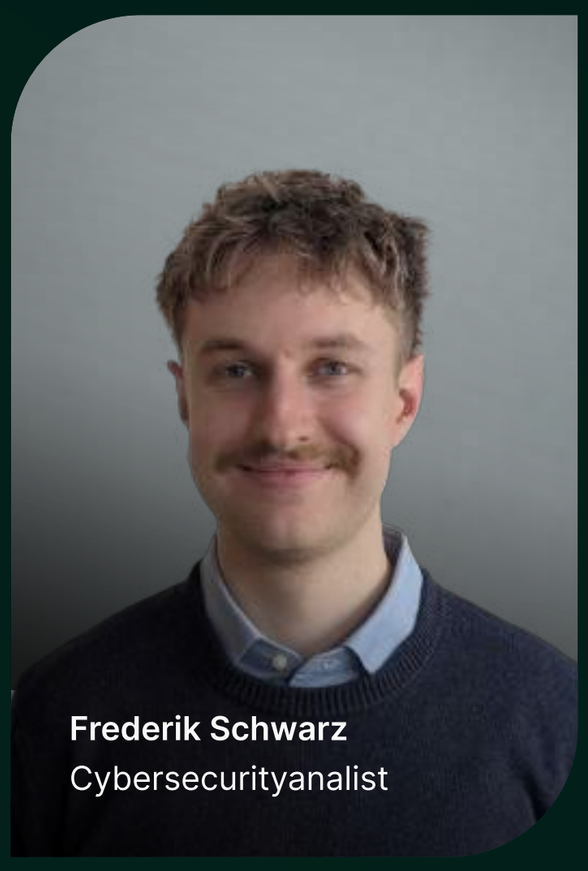
Fatih Kenar
Cybersecurityanalist

"Kleine bedrijven hebben net zo belangrijke gegevens als grote ondernemingen, maar ze laten belangrijke veiligheidsnormen achterwege. Multi-Factor Authenticatie (MFA) kan deze kloof eenvoudig dichten. Het zorgt ervoor dat een inlog alleen succesvol is als naast het wachtwoord een tweede, persoonlijk bewijs zoals een code op de bedrijfstelefoon wordt geleverd. Zelfs als hackers een gestolen wachtwoord hebben, falen ze bij deze cruciale hindernis."

MFA als NIS2-eis

Met de invoering van de Cyberbeveiligingswet heeft twee-factorauthenticatie een wettelijke status verkregen. Waar MFA passend is, moet MFA worden toegepast. MFA is niet langer een eenvoudig veiligheidsverzuim, maar een potentieel aansprakelijkheidsrisico dat kan leiden tot aanzienlijke boetes en juridische consequenties.

1 Juli 2026 markeert de inwerkingtreding van de Cyberbeveiligingswet (NIS2) voor betrokken Nederlandse organisaties.

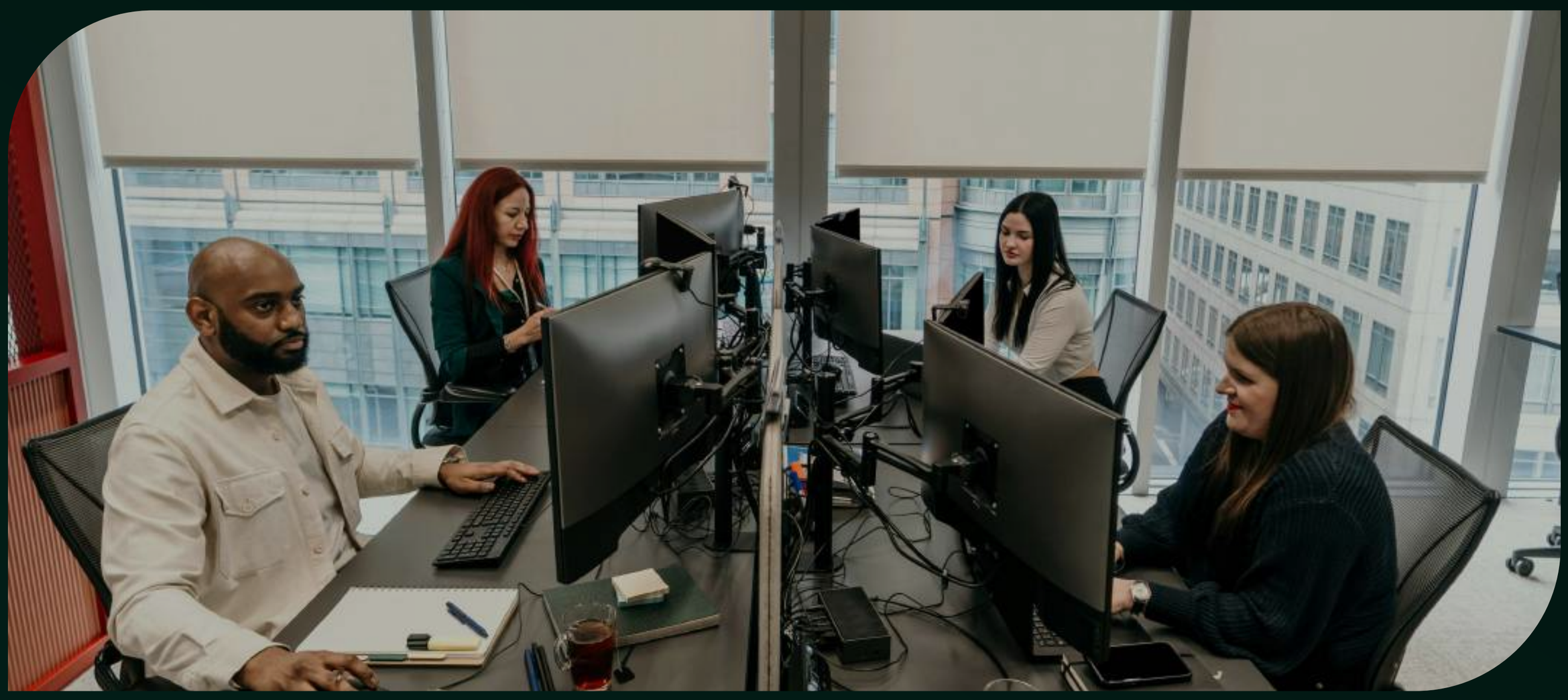


Frederik Schwarz
Cybersecurityanalist

„De NIS2-richtlijn is een belangrijke stap voor de Europese cyber security en creëert een actieve verplichting voor bedrijven. De echte uitdaging ligt echter in de uitvoering: de wettelijke druk is hoog, terwijl interne middelen vaak schaars zijn. Het is daarom niet langer de vraag of de veiligheid wordt verbeterd, maar hoe snel deze kloof kan worden gedicht."

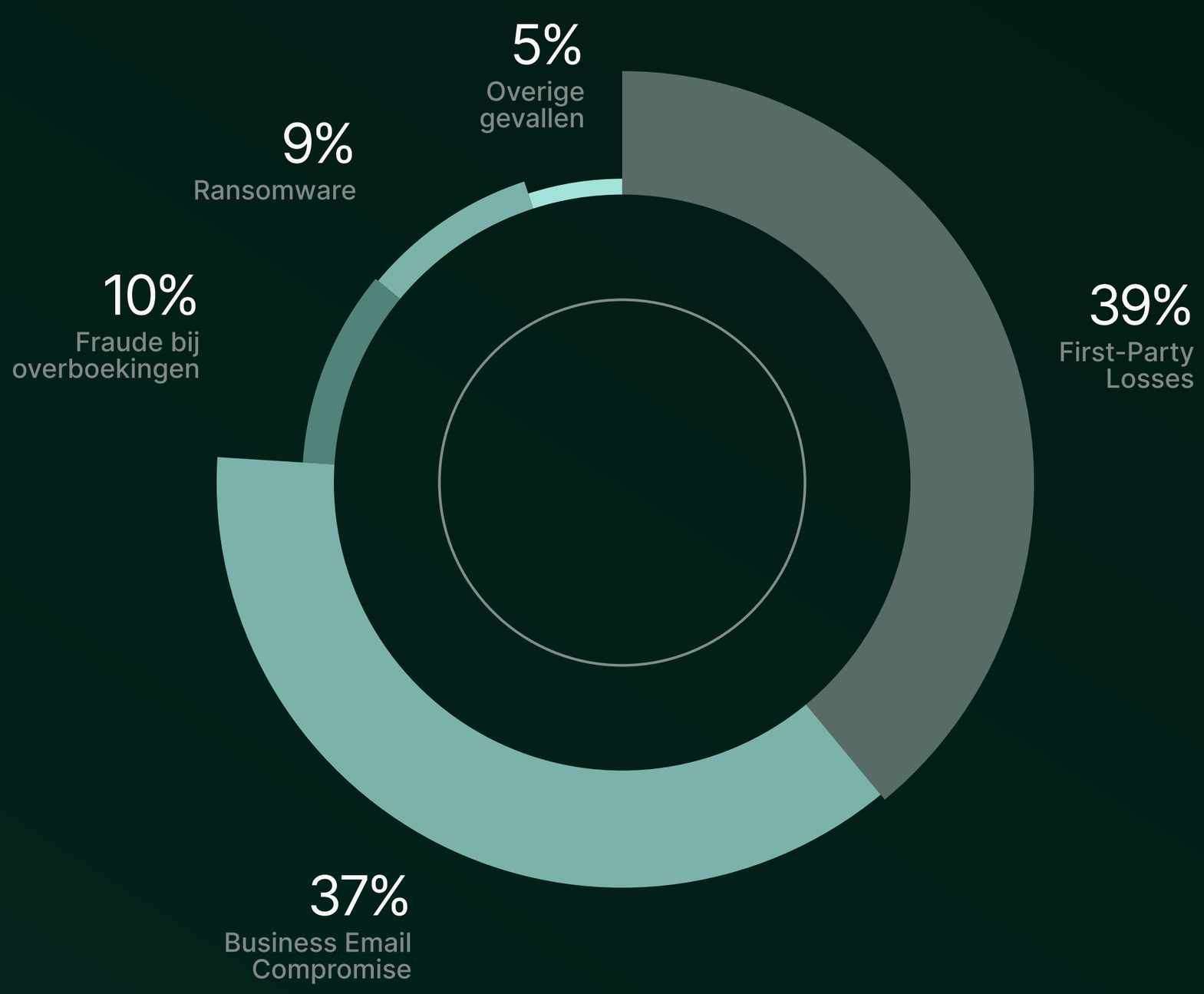
De kunst van schadebeperking

Als preventie faalt, komt crisismanagement in actie. Onze schadegegevens bieden een nuchtere kijk op de realiteit tijdens en na de aanval.



Oorzaken van financiële schade

Technische hacks zijn maar zelden de oorzaak van financiële schade. In de meeste gevallen speelt de mens een cruciale rol. De meest voorkomende redenen voor financiële schade zijn:



Bewustzijns-trainingen

Bron: ENISA Bedreigingslandschap 2025

Aangezien First-Party Losses (zoals phishing) met 39 % het grootste risico vormt, is een brede bewustwording van het personeel belangrijk.

Maar de realiteit is anders: Onze gegevens tonen aan dat 46 % van de grote bedrijven (met meer dan 100 miljoen € omzet) geen phishing-simulaties uitvoeren. Het feit dat bijna de helft van deze bedrijven dergelijke normen verwaarloost, onthult een kwetsbaarheid.

Vooral omdat al in 2025 80 %* van de social engineering-aanvallen door kunstmatige intelligentie werden uitgevoerd. Zonder regelmatige training zijn dergelijke phishing-e-mails nauwelijks meer van echte berichten te onderscheiden.

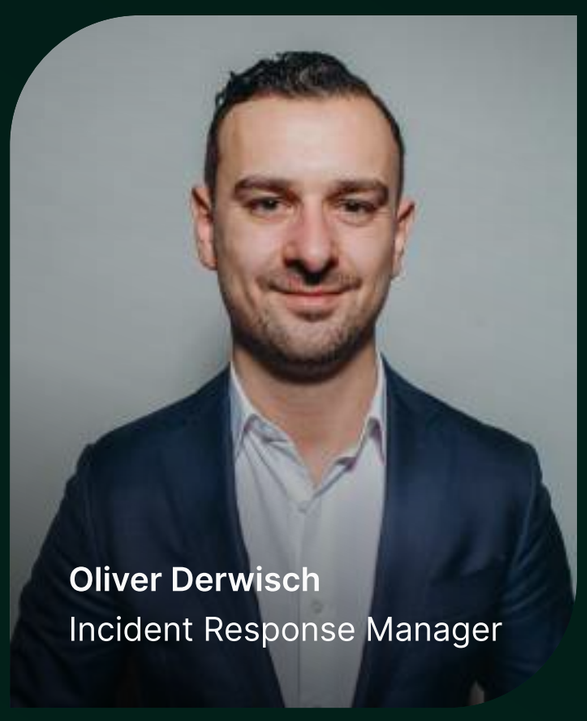
De prijs van afpersing

Ransomware blijft een dure bedreiging. Onze analyse van 245 echte ransomware-gevallen toont aan: De eerste eisen (initiële eisen) liggen soms zelfs bij 2,59 miljoen $. Terwijl de waarde van de meerderheid van de afpersingen zich tussen de 100.000 $ en 500.000 $ bevond, overschrijden bijna 30 % van de eisen de miljoen dollar-grens.

Onderhandelen loont

Tegenover de paniekreactie van veel betrokkenen is de eerste eis vrijwel nooit de eindprijs. Professionele ondersteuning helpt om de financiële schade te beperken.

51% daling van de afpersingseis wanneer wordt onderhandeld met behulp van een incidentrespons-expert.



Oliver Derwisch
Incident Response Manager

"Losgeldbetalingen zijn zelden de juiste oplossing. Ware veerkracht ontstaat door voorbereiding en een gestructureerd incident response management – waarbij de schade wordt beperkt, herstel mogelijk wordt gemaakt en een betaling in de meeste gevallen overbodig wordt."

Onderhandelings voorbeeld

Bron: Ransomware.live

260.000 $ als u vandaag betaalt.

We kunnen vandaag 155.000 $ betalen.

220.000 $ vandaag. Hier is onze BTC-portemonnee. Laat het ons weten wanneer u klaar bent om te betalen.

Betaal niet zomaar

Ondanks deze onderhandelingsresultaten is het raadzaam om geen geld aan afpersers te betalen. Want in de overgrote meerderheid van de gevallen bleven aanvallers zonder succes. Waarom? Omdat de backups werkten en incidentresponse-experts ingrepen.

Ongeveer 77 % van de getroffen bedrijven betaalde geen losgeld.

De back-up-illusie

Maar een werkende backup is geen vanzelfsprekendheid. Onze gegevens onthullen een lichtzinnigheid bij bedrijven:

21 % van de grote bedrijven (meer dan 100 miljoen € omzet) test hun volledige herstel niet regelmatig.

Zonder regelmatige validatie van de herstelprocessen bieden backups in geval van nood geen operationele zekerheid, maar een onberekenbaar restrisico.

Veerkracht in plaats van paniek

IT-beveiliging is geen eenmalig project, maar een continu proces. Het goede nieuws: het hoeft geen digitale vesting te zijn. Voor MKB's is de implementatie van geselecteerde beschermingsmechanismen de cruciale hefboom. Drie concrete praktijken zijn voldoende om de veerkracht te vergroten.

1. Digitale identiteiten beveiligen met MFA

Een strikte multi-factor-authenticatie (MFA) moet door de gehele IT-infrastructuur worden geïmplementeerd – voor alle interne medewerkers, externe dienstverleners en alle toegangspunten (VPN, cloud-diensten, e-mailtenants). MFA is het beste mechanisme ter bescherming bij gecompromitteerde inloggegevens en gestolen wachtwoorden.

2. Aanvallers eenvoudig blokkeren

AI-gestuurde phishing maakt misleidingen steeds realistischer. Voor echte veerkracht zijn technische beschermingsmechanismen nodig in plaats van alleen bewustwording. Phishing-simulaties bevorderen weliswaar het bewustzijn, maar cruciaal is het gebruik van Managed Detection and Response (MDR). In combinatie met Zero Trust en 24/7 monitoring worden bedreigingen in realtime gedetecteerd en geneutraliseerd – zelfs als schadelijke links worden aangeklikt.

3. Operationele veerkracht waarborgen met geverifieerde back-ups

Een ongeteste back-up is geen beveiligingsmaatregel, maar slechts een vage hoop. Veel grote bedrijven maken de fout zich te verlaten op geautomatiseerde opslagprocedures. Minstens één keer per jaar moet een volledige disaster recovery-test (hersteltest) worden uitgevoerd. Een geverifieerde, offline beschikbare databeveiliging blijft het sterkste en enige betrouwbare instrument tegen double-extortion-ransomware.

We sluiten de kloof

Baobab Risk Solutions is een van de toonaangevende Europese aanbieders van cyberverzekeringen. Als gespecialiseerde Managing General Agent (MGA) begrijpt Baobab digitale risico's door diepgaande, datagestuurde analyses en biedt proactieve bescherming als een essentieel onderdeel van de verzekering.

Het bedrijf werkt samen met uitstekend beoordeelde Lloyd’s-syndicaten, evenals Zurich en Liberty Specialty Markets, die fungeren als kapitaalverschaffers. Gevestigde venture capital-partners – zoals Viola FinTech of eCapital – zorgen voor langdurige financiële stabiliteit.

Sinds 2022 biedt Baobab de cyberverzekering Cyber Safe op de markt aan. De Crime-verzekering en de IT-aansprakelijkheidsverzekering oneIT-protect maken het productportfolio compleet.

Baobab Risk Solutions is actief in de Benelux met hoofdkantoor in Duitsland.

Baobab Risk Solutions
Cyber-, verzekerings- en underwriting-experts

BRS werkt samen met gevestigde capaciteitgevers

Baobab
Risk Solutions

baobab.io