freedom to focus

Medewerkers veilig in hun kracht, bedrijven beschermd

Voorwoord door:
Steven Bond, The Open University

Inclusief bijdragen van:
Shira Rubinoff, toonaangevend adviseur en auteur op het gebied van cybersecurity
Martin Veitch, IDG Connect

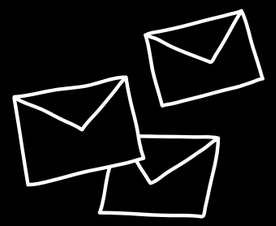
zivver

Inhoud

Onderzoeksaanpak
In maart 2022 hebben we interviews gehouden met:

- 6,031 werknemers uit verschillende functies en sectoren die e-mail gebruiken op het werk
- 855 IT-besluitvormers die verantwoordelijk zijn voor of invloed hebben op gegevensbeveiliging in organisaties met meer dan 250 werknemers

De enquêtes werden in de VS, het VK, Nederland, Frankrijk, Duitsland en België afgenomen door het gespecialiseerde marktonderzoeksbureau Insight Avenue.



freedom

Bijdrage van deskundige

Steven Bond
Information Rights Manager,
bij The Open University

E-mail. De eerste gedachte: hét communicatiegereedschap en-platform dat flexibel werken mogelijk maakt. Herkenbaar?
E-mail. Een zakelijke noodzaak. Het massacommunicatiegereedschap. Het middel om zonder onderbreking je punt te maken. De opvolging als er iets gemist is.

Je sluit een document bij en je klikt op verzenden. Makkelijk toch? Maar dan besef je je dat het verkeerde document is bijgesloten, of de verkeerde ontvanger is gekozen. Nu heb je een beveiligingslek en dat kan serieuze gevolgen hebben – financieel, juridisch én voor je zakelijke reputatie. Aangezien e-mail om de gebruiker draait, brengt het als platform significante beveiligingsrisico's mee. De meeste datalekken ontstaan door menselijke fouten met e-mail. Toch krijgt dit gebied meestal geen prioriteit van IT-leiders. Die leggen de focus meer op beveiliging tegen binnenkomende dreigingen.

Er zijn tegenwoordig heel veel tools om samenwerking te bevorderen. De meeste daarvan proberen oprecht behulpzaam te zijn, niet te hinderen. Toch ervaren we een overdaad aan communicatie. Die leidt tot verwarring, verloren tijd en lagere productiviteit. Terwijl wij de verschillende platforms proberen te leren kennen én moeten beslissen wat we voor welke taak gaan inzetten, worden we continu onderbroken. Bij implementatie van deze tools geeft niemand aan wat we voor welk scenario moeten gebruiken. E-mail is de vertrouwde 'alleskunner' waar mensen op terugvallen – het warme dekentje. Maar met die warmte komt ook onachtzaamheid, waardoor het risico op een verkeerde bijlage of ontvanger groter wordt.

Hoe verander je e-mail van een afleiding in het beloofde gereedschap?

In dit rapport onderzoeken we het effect van databeveiligingstraining op het individu, en vergelijken we wat leiders verwachten met wat er werkelijk gebeurt. We onderzoeken ook het veelvoud aan aangeboden tools en platforms voor gebruikers, en de impact die dit kan hebben op productiviteit en uitgaande databeveiliging. We herkennen tegelijkertijd de positieve synergie die ontstaat als zij goed geïntegreerd worden. Ter afsluiting onderzoekt dit rapport hoe de vooruitstrevende uitgaande beveiliging van de toekomst eruitziet.

Er zijn mechanismen die de gebruiker helpen om IT en e-mail te vertrouwen. Die nemen afstand van het 'menselijk probleem' door dat te ondervangen met een IT-oplossing. Hier is Zivver.

Nu de digitale transformatie steeds sneller verloopt en er meer op afstand wordt gewerkt, groeit de behoefte van werknemers om in realtime via digitale kanalen samen te werken met de dag. IT-leiders spelen hier een sleutelrol in. Zij dienen medewerkers de juiste hulpmiddelen en de vrijheid te geven om zich te kunnen focussen, zonder dat er sprake is van onnodige frictie.

Nu het aantal datalekken elk jaar toeneemt, moeten zij echter ook zorgen voor een robuuste beveiliging, en een omgeving creëren waarin snelle en voortdurende communicatie geen reputatieschade of dure boetes tot gevolg heeft. Hoe kunnen zij het juiste evenwicht vinden tussen vrijheid en beveiliging – en welke instrumenten of strategieën zijn van cruciaal belang voor hun succes?

Om dat uit te zoeken gaf Zivver – leider op het gebied van beveiligde communicatieoplossingen – opdracht tot een van de grootste onafhankelijke, wereldwijde enquêtes ooit over beveiligde digitale communicatie en productiviteit van werknemers. In de onderstaande artikelen lees je hoe IT-leiders, CISO's en DPO's een nieuw tijdperk van veilige en productieve samenwerking kunnen inluiden, inclusief een kort overzicht van onze belangrijkste bevindingen.

In maart 2022 heeft Zivver 6.031 werknemers uit verschillende functies en sectoren ondervraagd die e-mail gebruiken op het werk, en 855 IT-besluitvormers die verantwoordelijkheid dragen voor of invloed hebben op gegevensbeveiliging in organisaties met meer dan 250 werknemers.

De enquêtes werden in de VS, het VK, Nederland, Frankrijk, Duitsland en België afgenomen door het gespecialiseerde marktonderzoeksbureau **Insight Avenue**.

Overzicht

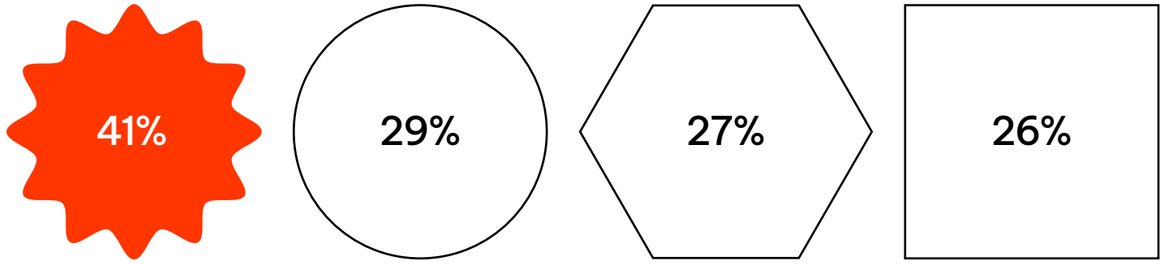
Focussen in een dynamische werkomgeving: De hindernissen op een rij

Een gedurfde nieuwe marketingcampagne pitchen. Een fantastische salespresentatie voor een potentiële nieuwe klant maken. Een slim nieuw systeem om de financiële efficiëntie te verhogen implementeren.

Om welk soort taak het ook gaat: werknemers boeken de beste resultaten wanneer ze het gevoel hebben zelf beslissingen te mogen en kunnen nemen en wanneer ze zich volledig op hun werk kunnen concentreren. Het mag dan ook geen verrassing zijn dat 98% van de werknemers uit ons recente onderzoek het eens was met de volgende stelling: *Het is belangrijk dat ik dit jaar de vrijheid heb om me te concentreren op mijn kerntaak op het werk.*

Toch is er in werkomgevingen van vandaag de dag sprake van allerlei soorten afleidingen en frictie, waardoor werknemers zich niet op hun belangrijkste werk kunnen concentreren.

De grootste belemmeringen voor focus onder werknemers op hun kerntaak



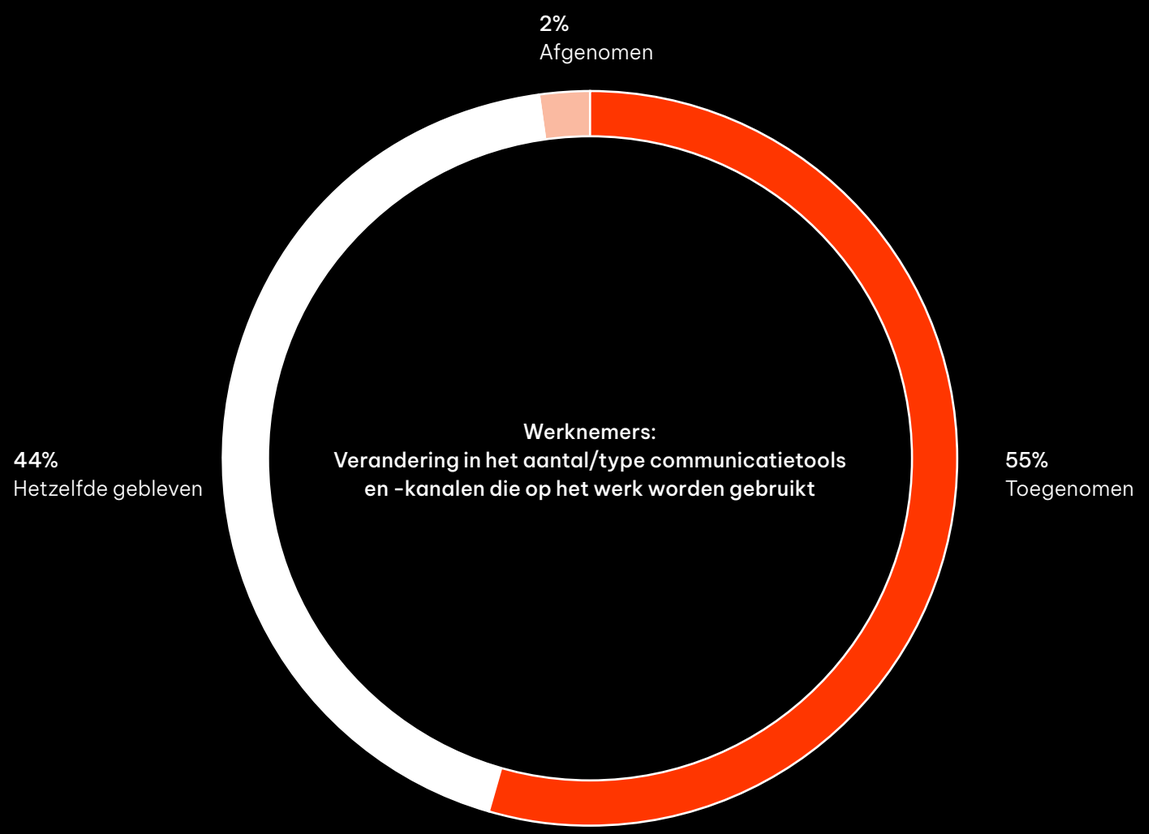
Te veel bureaucratie en procesoverbelasting

Zorgen over andere werk gerelateerde zaken

Tijdrovende beveiligingsprocessen en-protocollen

Te veel verschillende IT-systemen

Deze afleidingen zijn de afgelopen twee jaar verergerd door het werken op afstand: bij meer dan de helft van de werknemers (55%) is het aantal en het soort tools dat ze gebruiken om informatie voor werkdoeleinden te delen toegenomen.



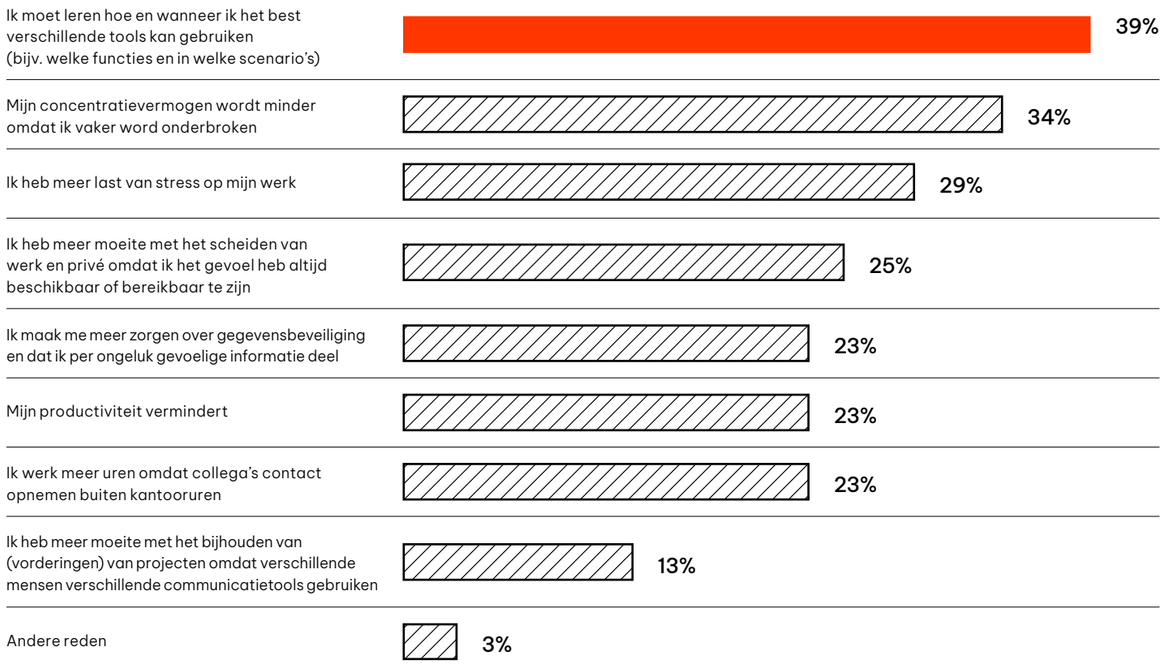
Momentopname per regio		
% werknemers dat zegt dat het aantal en het soort communicatiemiddelen dat ze gebruiken in de afgelopen twee jaar is toegenomen	VK: 57%	Duitsland: 50%
	VS: 63%	Frankrijk: 50%
	Nederland: 52%	België: 55%

Meer tools, meer problemen?

Het resultaat? Door minder efficiënte samenwerking en frictie op IT-gebied kunnen werknemers zich minder goed op hun werk concentreren, voelen ze zich meer gestrest en vormen ze een groter risico als het gaat om het veroorzaken van datalekken.

Dat wil niet zeggen dat het gebruik van een reeks samenwerkingstools een slechte zaak is; deze platforms zijn tijdens de pandemie immers van cruciaal belang geweest om de bedrijfscontinuïteit te waarborgen. Er is echter een duidelijk spanningsveld tussen het verlangen van werknemers naar de vrijheid om zich te concentreren en de manier waarop ze hun werk momenteel uitvoeren.

Werknemers: Impact van groeiende aantal (verschillende) samenwerkingstools



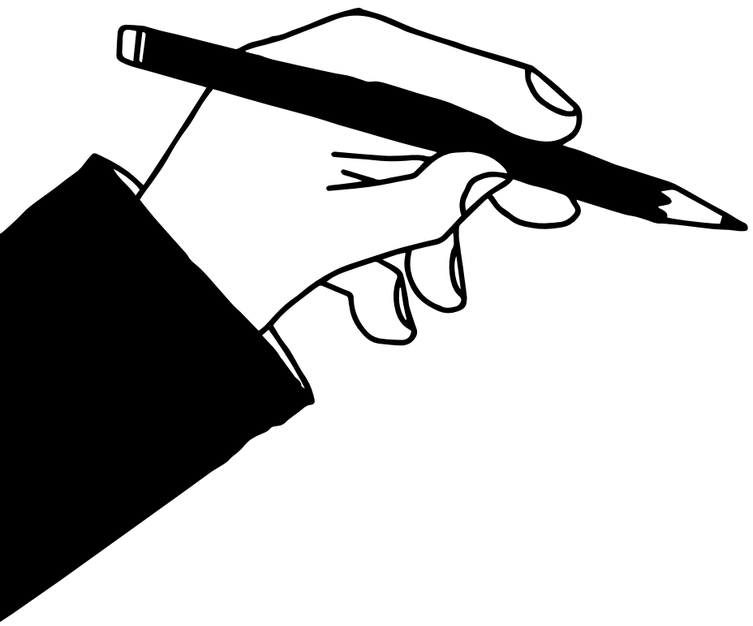
Momentopname per regio		
% van werknemers dat zegt dat een toenemend aantal tools hun vermogen om zich te concentreren en hun beste werk te leveren heeft verminderd, omdat ze vaker worden onderbroken	VK: 30%	Duitsland: 38%
	VS: 46%	Frankrijk: 28%
	Nederland: 31%	België: 29%

In het kort

Hoewel bijna alle werknemers de vrijheid willen hebben om zich te kunnen concentreren op hun kerntaak, vormen afleidingen zoals bureaucratie en tijdrovende beveiligingsprocessen een belemmering voor echte focus. Dit probleem wordt alleen maar groter naarmate werknemers meer communicatieplatforms gebruiken om hun werk te doen. Dit leidt vervolgens weer tot stress en een groter risico op het schenden van de gegevensbescherming.

Bijna alle werknemers willen de vrijheid hebben om zich te concentreren op hun kerntaak.

Effectieve communicatie: De tools en de risico's



Goed werk leveren is geen toevalstreffer. Om de best mogelijke voorwaarden voor het succes van werknemers te creëren, moeten IT-leiders tools, platforms en procedures implementeren die elke medewerker de vrijheid geven om zich te focussen, vrijuit te communiceren en zelfs af en toe een paar risico's te nemen (zonder dat de veiligheid van de gegevens hierbij daadwerkelijk in het geding komt).

De eerste stap om dat te bereiken, is door inzicht te verkrijgen in hoe werknemers tegenwoordig samenwerken, informatie delen en communiceren.

E-mail is het meest waardevolle kanaal, maar is niet volmaakt

Berichtendiensten en videoplatforms hebben de laatste jaren veel aandacht gekregen, maar e-mail blijkt nog steeds de meest gebruikte communicatiemethode onder werknemers.

E-mail wordt bovendien niet alleen het meest gebruikt, maar werknemers geloven ook daadwerkelijk dat het de meest waardevolle en veilige communicatiemethode is. Negen op de tien (88%) werknemers zeggen dat ze op e-mail vertrouwen om hun werk gedaan te krijgen, terwijl 81% gelooft dat e-mail de meest veilige manier is om gevoelige informatie te versturen.

> Over het algemeen zegt 88% van de werknemers dat ze op e-mail vertrouwen om hun werk gedaan te krijgen. Bijna alle IT-leiders (97%) zeggen dat hun organisatie afhankelijk is van e-mail als bedrijfstool.

Werknemers: Methoden voor communicatie waarop medewerkers het meest vertrouwen om hun werk te doen

- 75% E-mail
- 49% In persoon
- 43% Berichtendiensten
- 41% Videobellen/-conferenties
- 41% Telefoon

Momentopname per regio		
% werknemers dat zegt afhankelijk te zijn van e-mail om hun werk gedaan te krijgen	VK: 87%	Duitsland: 90%
	VS: 87%	Frankrijk: 86%
	Nederland: 94%	België: 86%

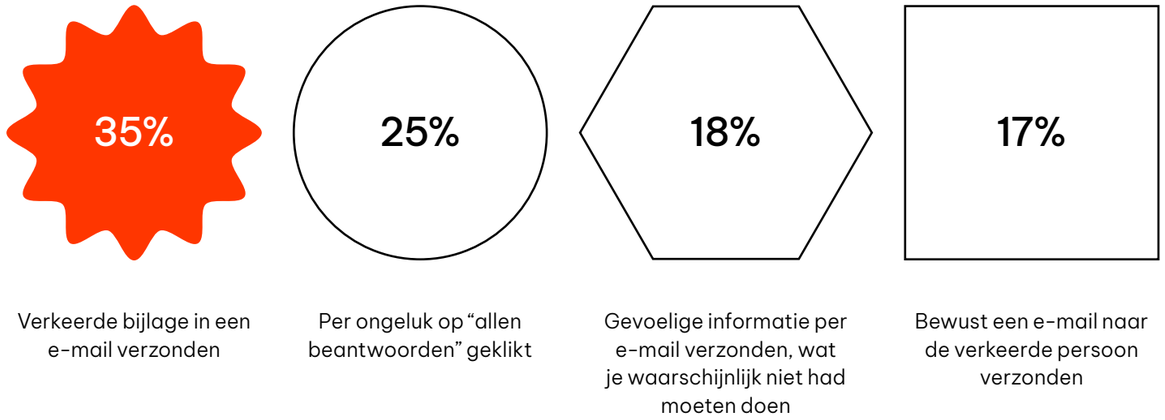
Dat iets vertrouwd is, betekent niet dat het veilig is

Maar hoewel werknemers e-mail prettig vinden werken en het vertrouwen, is het vanuit het oogpunt van bedrijfsveiligheid geen waterdichte tool. Er bestaat een reëel risico dat werknemers ervan uitgaan dat e-mail veilig is omdat het vertrouwd en nuttig aanvoelt, maar dat is niet per se het geval.

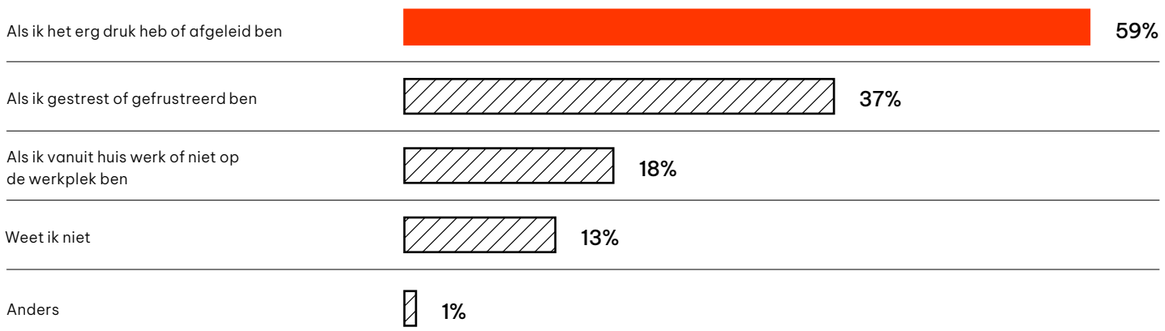
In totaal zegt 62% van de werknemers de afgelopen twee jaar 'fouten bij het e-mailen' te hebben gemaakt, variërend van het per ongeluk versturen van de verkeerde bijlage tot het bewust versturen van gevoelige informatie die ze waarschijnlijk niet hadden moeten versturen.

Zorgwekkend is dat werknemers deze fouten veel vaker maken als focussen bemoeilijkt wordt. Elders in onze interviews gaf 45% van de werknemers toe dat ze op het werk wel eens risicovolle beslissingen hebben genomen als gevolg van tijdgebrek.

E-mailfouten gemaakt door medewerkers in de afgelopen twee jaar



Situaties waarin werknemers de meeste kans hebben om e-mailfouten te maken

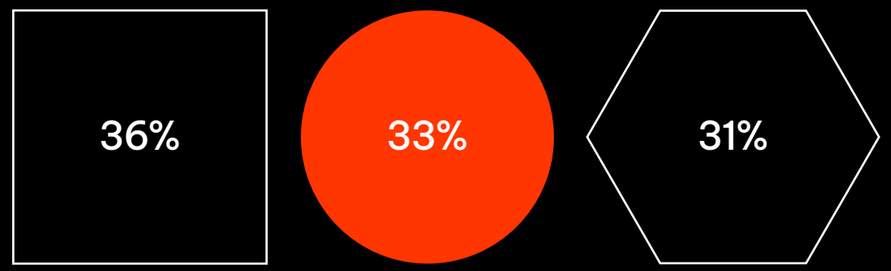


Toenemend risico, falende veiligheidsmaatregelen

De **kosten veroorzaakt door datalekken nemen wereldwijd toe**, wat betekent dat het de hoogste tijd is dat IT-leiders na gaan denken over hoe ze de toenemende beveiligingsrisico's willen aanpakken. Zorgwekkend is dat velen op gedragstraining lijken te vertrouwen om hun bedrijf te beschermen: driekwart van de IT-leiders (76%) denkt dat het organiseren van trainingen op het gebied van gegevensbeveiliging het aantal fouten bij het e-mailen zal beperken.

Maar de realiteit is dat deze trainingen ofwel tekortschieten, of überhaupt niet plaatsvinden. Een derde van de werknemers denkt dat ze geen training over gegevensbeveiliging hebben gekregen, en van de 67% die wél training heeft gehad, heeft slechts 36% de opgedane kennis ook daadwerkelijk in de praktijk gebracht. Voor de meeste organisaties is training in gegevensbeveiliging alleen niet genoeg om bedrijfsveiligheid te garanderen.

Werknemers: Training inzake gegevensbeveiliging in de afgelopen 12 maanden



Momentopname per regio		
% werknemers dat zegt een training in gegevensbeveiliging te hebben gevolgd, maar de opgedane kennis nog niet in hun kerntaak te hebben gebruikt	VK: 38%	Duitsland: 33%
	VS: 29%	Frankrijk: 29%
	Nederland: 32%	België: 27%

Werknemers hebben ook weinig vertrouwen in de huidige beveiligingsmethoden. De helft zegt dat "de huidige beveiligingsmethoden me afremmen en minder productief maken", terwijl 39% denkt dat "de paranoia van IT-teams over bedreigingen me belemmeren mijn werk te doen".

Dit alles leidt tot één duidelijk beeld: werknemers willen de vrijheid hebben om hun werk te doen, en e-mail wordt daarbij als een waardevolle tool beschouwd. Maar het gebruik van e-mail kent risico's, en de huidige maatregelen zijn niet afdoende om bedrijven daartegen te beschermen. Er is duidelijk een slimmere aanpak nodig. Of, zoals 79% van de werknemers stelt:

Het zou alle partijen ten goede komen als er een oplossing zou zijn die mensen beschermt tegen e-mailbeveiligings-fouten.

In het kort

E-mail is de favoriete tool van werknemers voor communicatie op het werk, maar velen geven toe fouten te maken als het gaat om de beveiliging. Alleen vertrouwen op trainingen op het gebied van gegevensbeveiliging is niet afdoende: zowel werknemers als IT-leiders zijn het erover eens dat het goed zou zijn als ze een slimme technologische oplossing zouden hebben die het juiste niveau van digitale beveiliging zou bieden om dit soort fouten te voorkomen.

Momentopname per regio		
% werknemers dat denkt dat het alle partijen ten goede zou komen als er een oplossing zou zijn die mensen beschermt tegen e-mailbeveiligingsfouten	VK: 84%	Duitsland: 78%
	VS: 85%	Frankrijk: 75%
	Nederland: 78%	België: 77%

king of comms

Martin Veitch
Freelance schrijver, analist en Contributing Editor bij IDG Connect

Communicatiekoning e-mail moet zijn beveiliging repareren om nog vijftig jaar te regeren

Om de bekende uitspraak van Mark Twain te parafraseren: de geruchten over de dood van e-mail zijn al vele jaren sterk overdreven. Slate magazine publiceerde een artikel over '**De dood van e-mail**' in 2007 én in 2011. De Britse krant The Independent stelde de suggestieve vraag: '**Aanschouwen we de dood van e-mail?**' Intussen gebruiken miljarden mensen het meer dan vijftig jaar oude systeem nog steeds. Maar als we e-mail nog eens vijftig jaar willen laten bloeien en groeien, dan moeten we de beveiliging fiksen.

Het is een feit, dit nieuwe onderzoek van Zivver maakt dat duidelijk: e-mail gaat voorlopig niet weg. E-mail blijft volgens mij vandaag de dag zeer relevant. We zien het als controleerbaar, formeel en relatief niet opdringerig... Een medium dat je kunt bewaren, doorzoeken en archiveren. E-mail was er al voor er cd's, punkmuziek of videorecorders waren, maar dat maakt het niet onverslaanbaar. De grootste uitdaging is beveiliging.

E-mail heeft, zoals ieder bedrijfsmiddel, bescherming nodig. Het is zorgwekkend dat het een zwakke plek blijft voor aanvalspogingen zoals malware, phishing, ransomware en wat al niet meer. Aanvallen via e-mail zijn traumatisch, kostbaar en zeer schadelijk voor je reputatie. Met aangescherpte wet- en regelgeving, zoals de AVG, en de bijkomende zwaardere sancties, zien we hoe fundamenteel veilig werken is voor het welzijn van een bedrijf.

Al geven we het misschien niet allemaal toe, iedereen heeft wel eens een verkeerde bijlage aan een mail toegevoegd, per ongeluk op 'allen beantwoorden' geklikt of (verschrikkelijk!) een e-mail verkeerd geadresseerd. Daarom hebben we verdediging nodig, zowel tegen ons eigen falen als tegen de aanvallen van anderen. In het beste geval hebben we goede processen, opleidingen en trainingen. Maar we moeten ook meer kunnen vertrouwen op automatisering en slimme systemen die afwijkend gedrag detecteren en onze acties controleren. Als ik een e-mail verstuur met een bijlage waarin financiële verwachtingen staan, en de ontvanger staat niet in mijn adresboek, dan moet er controle en validatie plaatsvinden.

Veel CIO's en CISO's rapporteren dat aanvallen de afgelopen twee jaar zijn toegenomen. Aanvallers proberen hun voordeel te doen met snel (her-) ontworpen processen en de kwetsbaarheid van endpoints thuis en netwerken.

Dit onderzoek laat zien dat veel bedrijven hun beveiligings-assessment te lang hebben uitgesteld. Een terugkeer naar de pre-pandemische wereld zit er voor de meeste kenniswerkers niet in. In feite moeten we beveiliging heropbouwen met het oog op een hybride werkwereld waarin de meesten van ons niet veilig achter bedrijfsfirewalls zitten, maar wel heel afhankelijk zijn van de communicatie-infrastructuur.

IT wordt al op allerlei manieren zwaar belast en niet iedere organisatie kan zich een hoogwaardig SecOps-team veroorloven. We hebben slimme, onopvallende tools nodig die, zonder ons te vertragen, bescherming bieden. Zo ontwikkelen we bij onze mensen het vertrouwen dat ze veilig kunnen werken.

Als ik met CIO's, CTO's en CISO's spreek (via de e-mail!) dan zie ik dat grote organisaties een cocktail van modellen gebruiken om informatie, inzichten en nieuws te delen. Wat ze allemaal benadrukken is een behoefte aan beveiliging en regelgeving. Een ervaren CIO zegt: "Als ik iets wil vastleggen, dan stuur ik een e-mail... Maar dan heb ik de zekerheid nodig dat die e-mail veilig is."

Een CTO voegt daaraan toe: "E-mail zegt 'dit is waarschijnlijk best belangrijk en ik wil hier mogelijk op terugkomen' [en] ik heb dat gevoel niet bij Teams of Zoom. Maar om e-mail relevant te houden, moet het niet gezien worden als overdrachtspunt van veiligheidsdreigingen."

Een CISO zegt: "Ik woonde recent een conferentie bij waar een IT-leider op het gebied van transformatie zei dat hij 'op missie was om e-mail eruit te schoppen' omdat er snellere media waren. Maar als ik weet dat e-mail veilig en controleerbaar is, dan kan ik daar op rekenen, terwijl ik dat niet kan op een Slack-kanaal, IM of DM. Daarom denk ik dat e-mail nog wel even blijft. Als je het adequaat beschermt en respect hebt voor de risico's, dan werkt het gewoon."

Dat geldt ook voor mij als schrijver. Als ik een snel citaat wil voor een verhaal, dan doe ik waarschijnlijk wat ik vandaag deed voor dit verhaal: dan stuur ik een e-mail aan een select aantal mensen. Zeven jaar geleden stuurde ik een e-mail om **een gesprek met Ray Tomlinson op te zetten**. Dat is de uitvinder van wat we nu zien als e-mail. Deze informele hiërarchie zit al decennia bij mij ingebakken. Ik denk dat de meesten van ons weten welk medium geschikt is, en e-mail is nog steeds correct voor veel dingen die we willen bereiken. Maar ons vertrouwen in e-mail verdwijnt als we de veiligheid in twijfel trekken.

Meningen over e-mail verschuiven zoals de meeste technologische veranderingen: meer als een evolutie dan een revolutie. We zien een verschuiving van één aanpak naar de andere, maar we kunnen ook lange periodes van co-existentie verwachten. E-mail voldoet nog steeds en zou, als wij er de ruwe kantjes maar af blijven vijlen, zo maar honderd jaar kunnen worden.

Het huidige risicolandschap van communicatie: Uitdagingen voor IT-leiders

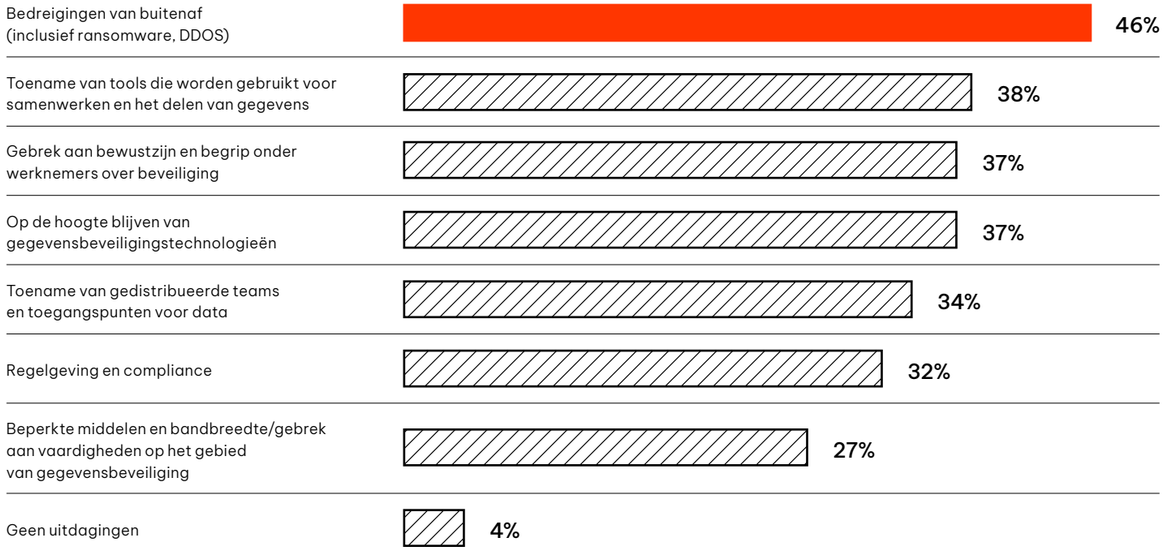
Het is enorm belangrijk dat werknemers de vrijheid krijgen om te focussen en weloverwogen risico's te nemen. IT-leiders weten echter maar al te goed dat die vrijheid niet ten koste mag gaan van beveiliging en governance.

Om een evenwicht te vinden tussen die vrijheid en de bijbehorende risico's, is het voor IT-leiders nuttig om het huidige risicolandschap van communicatie te begrijpen.

Wat zijn vandaag de belangrijkste uitdagingen op het gebied van gegevensbeveiliging?

Veiligheidsbedreigingen van buitenaf (46%) komen het meest voor, maar een wildgroei van gegevensuitwisselings- of samenwerkingstools is een ander groot probleem (38%), net als een gebrek aan inzicht in beveiliging (37%) en het op de hoogte blijven van de nieuwste gegevensbeveiligingstechnologieën (37%).

IT: De belangrijkste uitdagingen op het gebied van gegevensbeveiliging



Meer focus op uitgaande communicatie

IT-leiders besteden begrijpelijkerwijs veel aandacht aan de dreiging van malware en phishing. Maar 'datalekken door e-mailfouten van werknemers' is een bijna net zo grote zorg (43%), wat aangeeft dat IT-leiders net zozeer moeten nadenken over uitgaande beveiligingsfouten als over bedreigingen van buitenaf.

IT: Meest zorgwekkende beveiligingsdreigingen voor organisaties

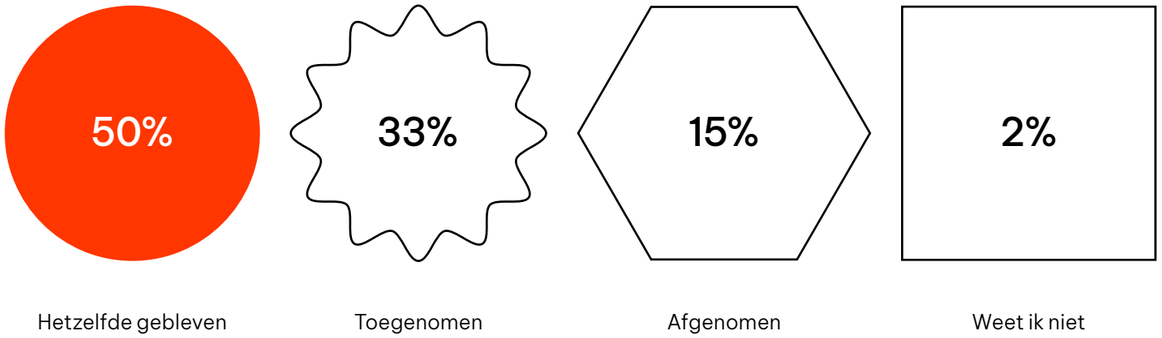
- 48% Malware
- 46% Phishing
- 43% Datalekken door e-mailfouten van werknemers
- 41% Ransomware
- 40% Kwetsbaarheden van werken in de cloud
- 31% APT (Advanced Persistent Threats)

Momentopname per regio		
% IT-leiders dat zegt dat datalekken door e-mailfouten van werknemers de grootste bedreiging voor de veiligheid is	VK: 50%	Duitsland: 37%
	VS: 45%	Frankrijk: 42%
	Nederland: 35%	België: 37%

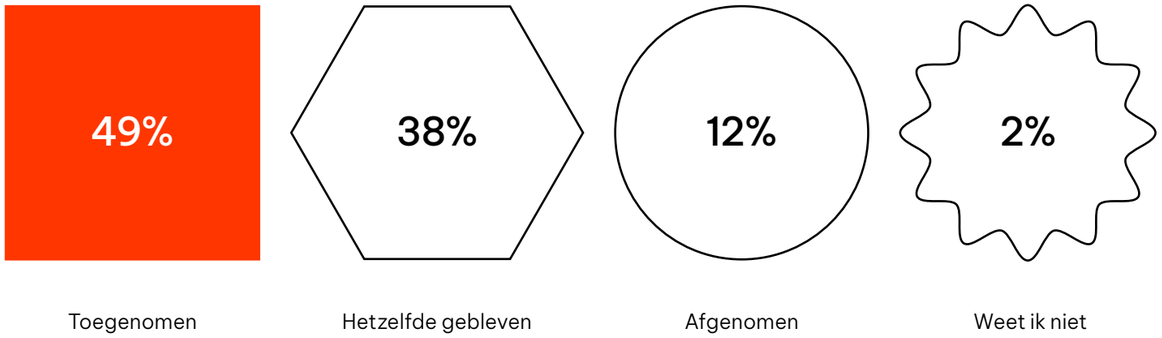
De toenemende risico's het hoofd bieden

De risico's nemen alleen maar toe. De helft van de IT-leiders (49%) zegt dat 'het aantal bedreigingen van buitenaf, zoals phishing of malware via links in e-mails' de afgelopen twee jaar is toegenomen, terwijl 33% denkt dat er meer incidenten zijn van 'datalekken doordat werknemers de verkeerde bijlage in e-mails versturen'.

Datalekken doordat werknemers de verkeerde bijlage in e-mails versturen



Bedreigingen van buitenaf, zoals phishing of malware via links in e-mails

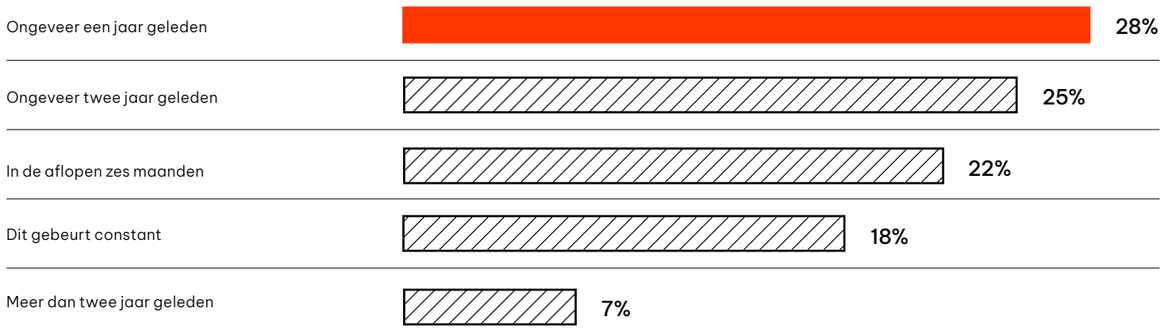


Proactief progressief proberen te blijven

Maar ondanks de constant veranderende aard van de risico's - en het groeiende probleem van e-mailfouten of -bedreigingen - hierzien veel IT-teams zich niet op regelmatige wijze de gegevensbeveiliging. Bij slechts 18% van de IT-leiders wordt de aanpak van risico's en e-mailbeveiliging voortdurend onder de loep genomen. Bijna een derde van de IT-teams (32%) heeft hun aanpak van risico's en e-mailbeveiliging twee jaar of langer geleden voor het laatst herzien. Gegeven hoeveel en hoe snel de manier van werken verandert, is een proactieve aanpak van essentieel belang.

Aangezien training in gegevensbeveiliging niet afdoende is, kan een strategie die is gebaseerd op de invoering van progressief risicobeheer met slimmere technologie het antwoord zijn. Het trainen van mensen zal altijd belangrijk blijven, maar technologie kan een grotere rol spelen bij het voorkomen van datalekken. Hierdoor worden werknemers in het hele bedrijf bovendien in staat gesteld om veilig en zonder onderbrekingen te werken.

IT: Laatste keer dat de organisatie het risicobeheer en e-mailbeveiliging onder de loep nam



Momentopname per regio		
% van de IT-leiders dat zegt dat ze hun aanpak van risico- en e-mailbeveiliging twee jaar of langer geleden hebben herzien	VK: 29%	Duitsland: 32%
	VS: 23%	Frankrijk: 50%
	Nederland: 38%	België: 18%

In het kort

IT-leiders worden met tal van evoluerende beveiligingsrisico's geconfronteerd, maar bedreigingen van buitenaf zijn niet het enige probleem. Gegevensverlies door e-mailfouten van werknemers is bijna een net zo groot probleem als malware en phishing. De meeste IT-leiders herzien hun beveiliging echter niet op periodieke wijze, waardoor ze risico's lopen in het snel veranderende bedreigingslandschap.

Verlies van data door e-mail is een grote zorg.

Shira Rubinoff
Cybersecurity Executive,
Adviseur & Auteu

focus

Technologie beïnvloedt en bestuurt onze wereld steeds meer. We leven in een tijd waarin taken worden gestroomlijnd door technologische vooruitgang. Maar de enorme hoeveelheid apps, opties en platforms waarmee we werken vormt ook een belasting. Als het gaat om de productiviteit van bedrijven, kunnen workflows vastlopen of worden vertraagd, verliezen medewerkers hun concentratie en kan de beveiliging van gegevens - met name de uitgaande digitale beveiliging van een organisatie - in gevaar komen. Hoe werken de meeste mensen? Hoe willen ze werken? Wat is het beste voor een organisatie; zowel wat betreft productiviteit als, misschien nog belangrijker, uitgaande beveiliging?

Het recente onderzoek van Zivver heeft een interessant thema aan het licht gebracht. Het lijkt erop dat meer vrijheid voor medewerkers om zich te concentreren, samen met de hulpmiddelen en technologieën om ze daarbij te helpen, zorgt voor grotere uitgaande digitale veiligheid en bescherming voor het bedrijf. Hoe kan dat? En wat betekent het allemaal?

In de voortdurend veranderende wereld van technologie, innovatie en steeds complexere communicatiemethoden, neemt de tijd die we gefocust aan elke actie besteden af, zowel in kwantiteit als in kwaliteit. Als mens hebben we maar een beperkte aandachtsspanne. Het werk stelt hoge eisen aan ons. We worstelen om ons meer technologieën eigen te maken. Gelijktijdig worden we geacht productiever te zijn. COVID-19 ligt bijna achter ons. In het post-pandemische tijdperk moet er wel iets wijken. In veel gevallen is dat de beveiliging. Dit kan een organisatie onnoemelijk veel schade berokkenen, vooral als het gaat om uitgaande digitale beveiliging.

Waarom de nadruk op e-mail?

Het Zivver-onderzoek toont aan dat meer dan 85% van alle ondervraagde medewerkers, in elk van de marktgebieden, afhankelijk is van e-mail om het werk gedaan te krijgen. 97% van de ondervraagde IT-beveiligingsprofessionals zegt dat e-mail één van de belangrijkste zakelijke tools is binnen hun organisatie. Allemaal geloven ze dat het ook de veiligste manier is om gevoelige informatie te delen. Maar in werkelijkheid zijn fouten van medewerkers de oorzaak van 80 tot 90%van alle datalekken. Omdat e-mail zo'n cruciale rol speelt in de bedrijfsvoering nemen hackaanvallen via e-mail toe. Daaronder vallen malware en phishing; waarmee twee derde van de ondervraagde IT-leiders in de afgelopen twee jaar te maken heeft gehad. Om nog maar te zwijgen van gegevens die verloren zijn gegaan, of zijn beschadigd, door fouten van medewerkers. Kortom: e-mail is een goede plek om te beginnen als het gaat om betere beveiliging.

In het onderzoek werd vastgesteld dat zowel externe cyberdreigingen als interne fouten en ongelukken van medewerkers toenemen. Zivver heeft aangetoond dat een groot deel van deze escalatie kan worden toegeschreven aan een gebrek aan concentratie bij medewerkers. Dat is op zijn beurt het gevolg van inefficiënte technologie. We zien onder meer een overvloed aan (en verwarring rond) allerlei platforms die nodig zijn om het werk uit te voeren. Ook zijn er te veel verschillende communicatiemethoden. E-mail is in alle opiniepeilingen een constante. Organisaties kunnen zich hierop concentreren als een gebied waar beveiligingstechnologie voor beschikbaar is waarmee mensen meer gedaan krijgen. Een betere beoordeling van security awareness training is ook aan de orde. Wat werkt wel en wat niet? Ook is aandacht voor upgrades en ondersteuning nodig. Zo kunnen organisaties op relatief korte termijn succes realiseren.

Op dit moment geeft slechts 18% van de IT-leiders aan dat ze regelmatig hun aanpak voor risico- en e-mailbeveiliging evalueren. Bijna een derde geeft toe dat hun laatste evaluatie minstens twee jaar geleden plaatsvond; in sommige gevallen is het zelfs veel langer geleden. Gezien het snelle tempo van de technologische en sociale veranderingen die onze wereld doormaakt, is een pro-actievere aanpak op zijn plaats.

En hoe staan medewerkers er van dag tot dag voor? Uit de enquête blijken de verwachtingen waaraan medewerkers worden blootgesteld niet alleen onpraktisch, maar ook onrealistisch en oneerlijk. Je kunt niet verwachten dat overbelaste mensen steeds weer trainingssessies bijwonen en nog meer nieuwe protocollen gaan naleven. Om de workflows en productieprocessen voor alle medewerkers te stroomlijnen, en tegelijkertijd de (met name uitgaande) beveiliging van de organisatiegegevens te verbeteren, zijn nieuwe technische hulpmiddelen nodig.

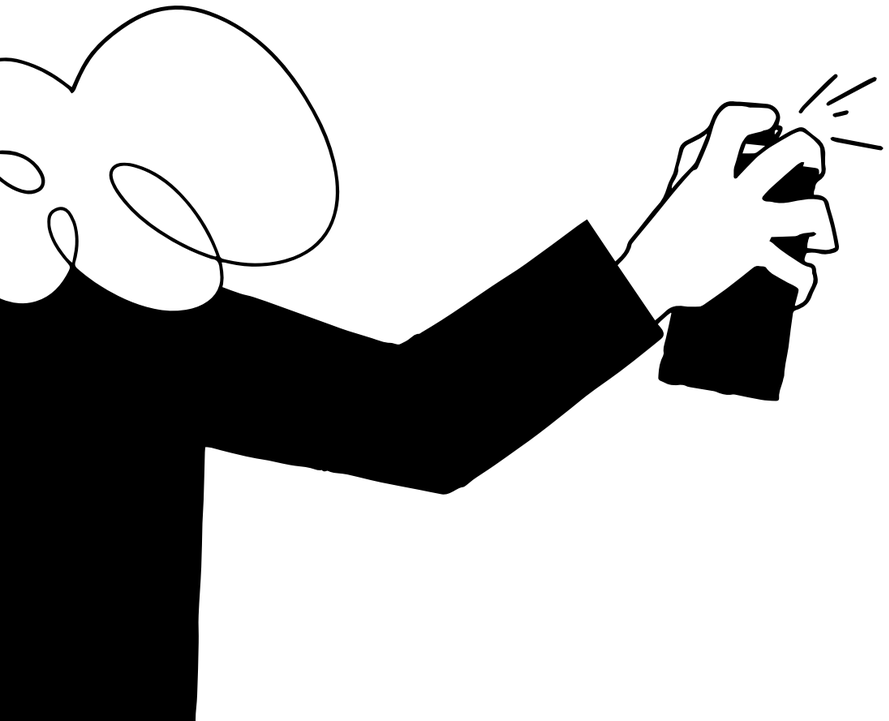
Medewerkers zijn te ondersteunen via een gebalanceerde en proactieve aanpak van risicobeheer, aangevuld met alomvattende, innovatieve en slimme technologie. Zo zullen bedrijven in staat zijn processen en communicatie samen te brengen. Dat geeft medewerkers de ruimte om beter te presteren, in minder tijd en met meer focus. Dit zal op zijn beurt de druk verlichten, waardoor menselijke fouten afnemen en bedrijven beschermd worden tegen eventuele interne veiligheidsrisico's.

Beter gefocuste medewerkers leiden tot een veiliger en productiever bedrijf. Is dat niet wat zowel medewerkers als leidinggevenden echt willen?

Progressief risicobeheer dankzij slimme technologie

Werknemers willen de vrijheid hebben om zich op hun werk te focussen. IT-leiders moeten ervoor zorgen dat de gegevensbeveiliging in orde is. Het goede nieuws is dat deze twee standpunten elkaar niet per se uitsluiten.

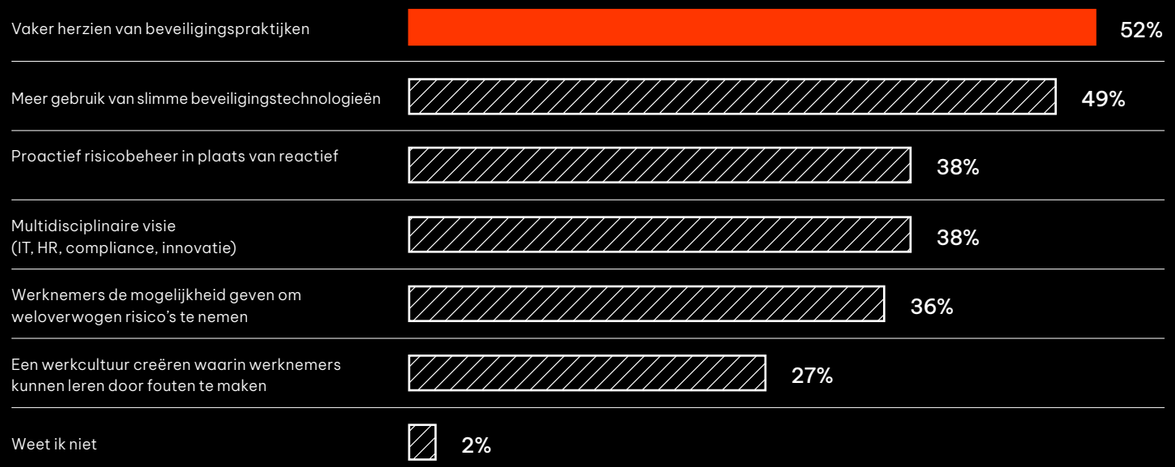
Met de juiste technologie en een meer vooruitstrevende aanpak van risicobeheer kunnen IT-leiders mensen de vrijheid geven om zich te concentreren op wat echt belangrijk is, terwijl de veiligheid van het bedrijf en de gegevens wordt gewaarborgd. Gelukkig zijn de meeste IT-leiders al bezig deze stap te zetten.



"Progressief risicobeheer" is in feite een combinatie van op gedrag gebaseerde strategieën en slimmere technologie. Iets meer dan de helft (52%) van de IT-leiders zegt dat dit betekent dat beveiligingspraktijken vaker moeten worden geëvalueerd (52%), terwijl 49% stelt dat het betekent dat er meer gebruik moet worden gemaakt van slimme beveiligingstechnologieën.

> Bijna alle IT-leiders (91%) denken dat ze progressiever te werk kunnen gaan als het gaat om risicobeheer.

IT: Hoe modern risicomanagement eruitziet



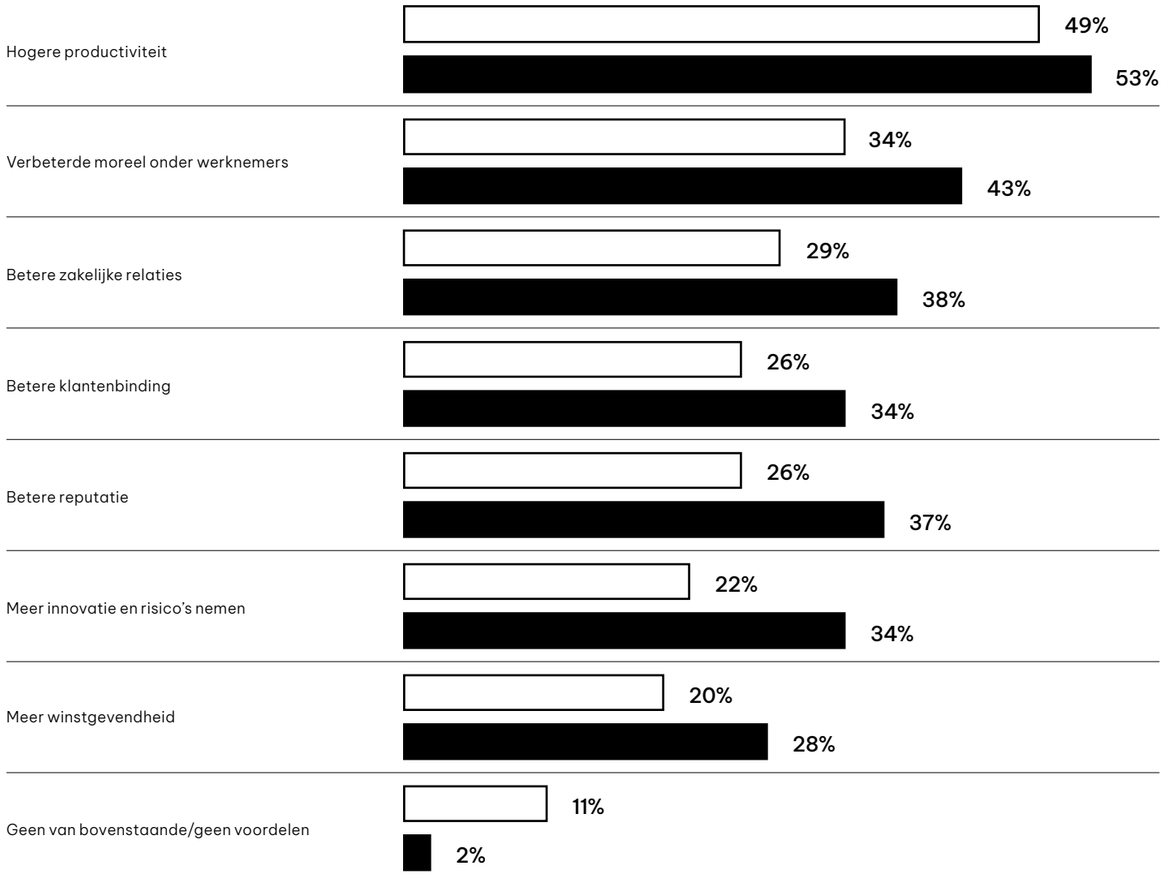
Progressief risicobeheer dankzij technologie

In plaats van e-mailbeveiligingsrisico's als een gedragsprobleem te beschouwen, denken vier op de vijf (79%) IT-leiders nu dat slimmere e-mailbeveiliging fouten kan beperken, en 87% zegt dat het gunstig zou zijn als bedrijven een oplossing zouden hebben die mensen beschermt tegen e-mailbeveiligingsfouten.

Oftewel: IT-leiders begrijpen nu dat werknemers tools en technologieën nodig hebben die hen in staat stellen in vrijheid te werken. Meer beperkende maatregelen of processen zijn niet de oplossing. Zo is 73% van de IT-teams van plan om in de komende twee jaar meer te investeren in de beveiliging van uitgaande e-mail.

Zoals we eerder in dit rapport hebben gezien, beschouwen werknemers e-mail als hun belangrijkste tool om te communiceren en samen te werken, ook in een tijdperk waarin het gebruik van berichten-apps en videoconferentie software aan de orde van de dag is. Dit zou dus voor veel bedrijven een positieve stap zijn. En zoals de laatste grafiek van ons onderzoek laat zien, denken zowel werknemers als IT-medewerkers dat ze er profijt van zouden hebben als ze zich bij het gebruik van e-mail geen zorgen hoefden te maken over problemen met gegevensbeveiliging.

Werknemers - IT: Voordelen als een organisatie investeert in technologie die ervoor zorgt dat men zich nooit zorgen hoeft te maken over gegevensbeveiliging bij het gebruik van e-mail, zodat er ruimte is voor aandacht voor andere dingen



In het kort

Nu duidelijk wordt dat alleen training in gegevensbeveiliging bedrijven niet kan beschermen, onderzoeken veel IT-leiders strategieën voor progressief risicobeheer. Slimme technologie wordt steeds meer gezien als de oplossing, in plaats van werknemers te belasten met meer beveiligingsprotocollen en beleidsmaatregelen.

IT-leiders onderzoeken strategieën voor progressief risicobeheer.

Werknemers
IT

De veilige toekomst van digitale communicatie

In een wereld die zo snel evolueert, moeten werknemers in staat worden gesteld om zonder onnodige IT-fricties te werken, wat betekent dat logge beveiligingsprotocollen moeten worden afgeschaft. In een werkomgeving vol afleidingen is het echter niet realistisch om puur op training in gegevensbeveiliging te vertrouwen om het bedrijf veilig te houden.

De slimme technologie van vandaag en een proactieve aanpak van risicobeheer kunnen het antwoord bieden en een nieuw tijdperk van veilige digitale communicatie inluiden. Zo blijft het bedrijf veilig, productief en soepel, en krijgen werknemers wat ze het allerliefst willen: de vrijheid om zich te concentreren op het werk dat er echt toe doet.

...de vrijheid om zich te concentreren op het werk dat er echt toe doet.

zivver

Voor meer informatie over hoe Zivver jouw organisatie kan helpen om de volgende generatie veilige digitale communicatie te ontdekken, ga naar zivver.com/nl