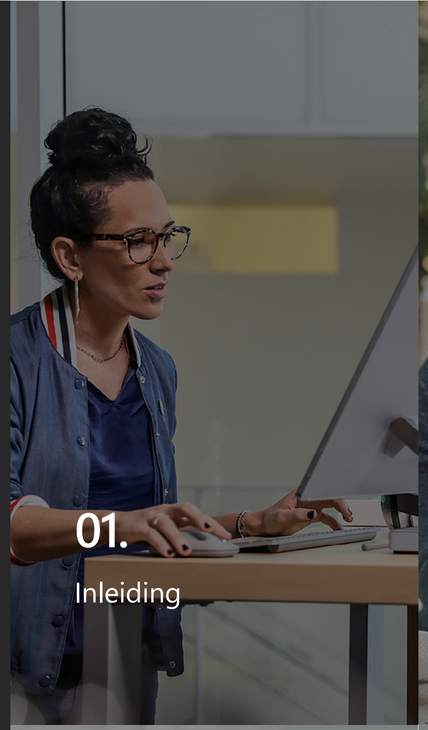
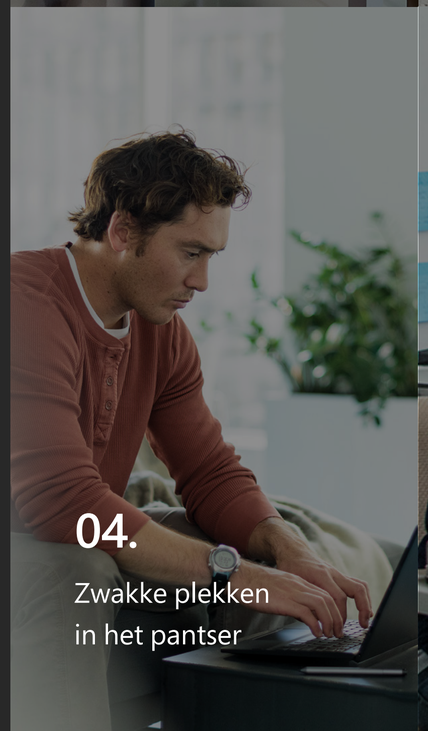
Microsoft

De staat van de beveiliging van het midden- en kleinbedrijf

Inhoudsopgave

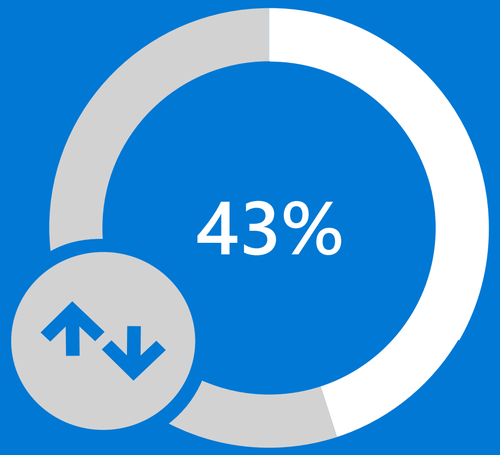




01. Inleiding

Als je in het mkb werkt, heb je waarschijnlijk meerdere petten op. Cyberbeveiliging wordt daarbij steeds belangrijker.

Voorbij zijn de dagen dat cybercriminaliteit uitsluitend een probleem voor grote bedrijven was. Tegenwoordig lopen alle bedrijven risico, ongeacht hun omvang of de bedrijfstak. Bedrijven begrijpen tegenwoordig dat het implementeren van een programma voor cyberbeveiliging een essentieel onderdeel van de bedrijfsvoering uitmaakt, net als het aannemen van personeel of het vergroten van de omzet.



Aangezien 43% van alle cyberaanvallen op het mkb is gericht,[1] is het niet verwonderlijk dat veel bedrijven cyberbeveiliging als prioriteit hebben aangemerkt.

Ook met een krap budget is sterke beveiliging mogelijk

De meerderheid van de bedrijven in het mkb is begonnen met het nemen van maatregelen om hun bedrijf en gebruikers te beschermen, zoals het actueel houden van software en het afdwingen van sterke wachtwoorden. Meer dan de helft zet antiphishing- en antivirussoftware in om zich tegen bedreigingen van buitenaf te beschermen, en een vergelijkbaar aantal heeft een proces voor het monitoren van waarschuwingen en bedreigingen ingesteld. Maar het is lastig om erachter te komen of je de juiste balans tussen bescherming en risico's hebt gevonden. Sommige bedrijven vragen zich af of ze groot genoeg zijn om door hackers te worden opgemerkt en of ze zich zorgen moeten maken over diefstal door medewerkers of het per ongeluk lekken van gevoelige informatie.

Klinkt dit als een beschrijving van jouw bedrijf? Lees dan verder. Er zijn bewezen oplossingen en deskundigheid beschikbaar om bedrijven van elke grootte en met elk budget te helpen met het beschermen van hun middelen. Sommige belangrijke maatregelen zijn zelfs gratis, zoals het bieden van trainingen voor je medewerkers. Je staat er dus niet alleen voor.

Aanpak en methodes van het onderzoek

Het rapport 'De staat van de beveiliging' belicht de unieke uitdagingen waar bedrijven in het mkb op het gebied van veiligheid mee worden geconfronteerd. We onderzochten ondernemingen uit vier landen (VS, Verenigd Koninkrijk, Duitsland en Brazilië), interviewden 12 bedrijven in het mkb en bestudeerden de bestaande literatuur om een allesomvattend inzicht in de houdingen en benaderingen voor beveiliging te krijgen. We doken in de stappen die bedrijven zetten om hun middelen te beschermen, hun ervaring met beveiligingsincidenten en hun meningen over de verschillende risicofactoren en oplossingen.

Onze analyse bracht lessen en kansen aan het licht die bedrijven in het mkb kunnen gebruiken om hun bedrijfsvoering veilig te maken.

Hoofdconclusies

Het onderzoek is samengevat in vijf hoofdconclusies:

01 Bedrijven begrijpen dat cybercriminaliteit een probleem is, maar onderschatten de ernst van de dreiging

02 Bedrijven in het mkb lopen evenveel kans om aangevallen te worden als grote ondernemingen

03 Medewerkers kunnen de beste bescherming voor een bedrijf zijn, maar ook de grootste bedreiging

04 Bedrijven zijn begonnen met het nemen van maatregelen om zichzelf te beschermen door middel van een reeks oplossingen en practices

05 In het Verenigd Koninkrijk, de VS, Duitsland en Brazilië variëren de maatregelen aan de hand van de unieke omstandigheden in elk land

De filosofie die Microsoft aan al zijn klanten, waaronder bedrijven in het mkb, aanbeveelt, is om op een beveiligingsincident te zijn voorbereid. Uit de data blijkt onomstotelijk: het is niet de vraag of je wordt aangevallen, maar wanneer. Door middel van een uitgebreide strategie ter bescherming van je meest waardevolle middelen, detectie van kwaadwillenden en reactie op aanvallen kun je voorkomen dat hackers je bedrijfsvoering verstoren. Op de volgende pagina's geven we je antwoorden op de meest prangende vragen en concrete aanbevelingen die de kans verkleinen dat je wordt aangevallen en waarmee je snel kunt herstellen als het ergste zich voordoet.

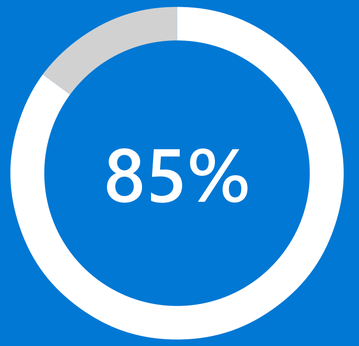
02.

Cyberbeveiliging serieus nemen

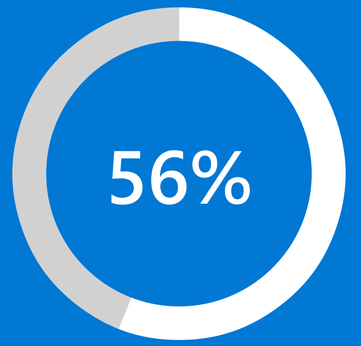
De kranten staan tegenwoordig vol met verhalen over cyberaanvallen, en de meesten van ons zijn niet langer verbaasd als we horen dat een groot, gerespecteerd bedrijf is gehackt. In alle lagen van de samenleving zijn mensen ervan doordrongen dat hun middelen, waaronder data, netwerken, apparaten, geld, reputatie en tijd, risico lopen.

De overgrote meerderheid van de bedrijven (85%) noemt cybercriminaliteit als zorg en meer dan de helft (56%) vindt het de belangrijkste prioriteit.[2] Bedrijven zetten deze mening ook om in maatregelen. De meeste bedrijven zijn begonnen om zowel tijd als geld te investeren in het beschermen van hun bedrijf tegen hackers en andere kwaadwillenden.

Het mkb neemt cyberbeveiliging serieus



van de bedrijven in het mkb maakt zich zorgen om cyberbeveiliging



van de bedrijven in het mkb zegt dat cyberbeveiliging de hoogste prioriteit heeft

Bedrijven onderschatten hun risico

Het goede nieuws is dat bedrijven zijn begonnen met het nemen van maatregelen om zichzelf te beschermen en dat ze erkennen dat cyberaanvallen een probleem zijn. Maar als je verder kijkt, wordt duidelijk dat veel bedrijven hun eigen risico's hebben onderschat. 74% van de bedrijven gelooft niet dat de kans dat ze worden aangevallen groot is en denkt dat grote ondernemingen twee keer zoveel risico lopen.[2]

Deze mening is begrijpelijk. De meeste nieuwsberichten gaan over grote, bekende bedrijven. Je begrijpt waarschijnlijk dat er een kans is dat kleinere bedrijven ook het doelwit kunnen zijn, maar je hebt mogelijk niet genoeg tijd of kennis om het risico echt te beoordelen. Helaas kan het onderschatten van de dreiging leiden tot ontoereikende beveiliging. Hackers houden de hele markt voortdurend in de gaten om kwetsbaarheden te vinden en richten zich juist vaak op kleinere bedrijven omdat ze weten dat deze bedrijven te weinig in cyberbeveiliging hebben geïnvesteerd.

> **Ik ben een kleine vis in een grote vijver. Ik ben voor hackers helemaal niet interessant.[2]**
>
> **SMB ITDM**
> Omnibus-enquête

Idee

2 X

De meeste bedrijven in het mkb geloven dat grote ondernemingen twee keer zoveel kans hebben om te worden aangevallen dan het mkb[2]

74%

74% van de bedrijven in het mkb gelooft niet dat de kans om te worden aangevallen groot is[2]

Werkelijkheid

43%

43% van de cyberaanvallen is gericht op het mkb[1]

41%

41% van de bedrijven in het mkb is al eens aangevallen[2]

En overschatten hoe goed ze zijn voorbereid

In je dagelijkse werk concurreren veel prioriteiten om je beperkte tijd en middelen. Het is niet verwonderlijk dat je niet genoeg tijd besteedt om inzicht te krijgen in je beveiligingsrisico en dat je de effectiviteit overschat van de beveiligingsmaatregelen die je hebt ingesteld. 90% van de bedrijven zegt de juiste bescherming te hebben om een aanval te voorkomen, en bedrijven met meer dan 50 medewerkers hebben hier nog meer vertrouwen in.[2] Het is bemoedigend dat bedrijven in beveiliging investeren, maar in werkelijkheid lopen ze meer risico dan ze denken. Bijna de helft (41%) is al eens aangevallen.[2]

Of je nu bent aangevallen of niet, dit is het juiste moment om je beveiligingsprocessen en -oplossingen te evalueren en verbeterpunten te bepalen voor bescherming van je middelen en reactie op aanvallen. Je kunt niet meer beschermingsmaatregelen implementeren dan je budget en middelen toestaan, maar je moet ook begrijpen dat elke maatregel telt en het verschil kan maken bij het weerstaan van een aanval. Op de volgende pagina's lees je veel van de oplossingen en processen die je kunt gebruiken om je belangrijkste middelen te beschermen.

"Je moet waakzaam zijn. Als het er verdacht uitziet, moet je ervan uitgaan dat het dat ook is."

Luister naar twee kleine ondernemers die bespreken hoe ze een proactieve instelling behouden om gemakzucht te voorkomen.

Aanbevelingen

- Leun niet achterover: ontwikkel een bewustzijn van de fundamentele beveiligingsconcepten en -bedreigingen. Maak je beveiliging vanaf het begin in orde, zodat je verstoringen kunt voorkomen en je energie in je bedrijf kunt steken.
- Stel prioriteiten: je kunt misschien niet in een keer een volledig beveiligingsplan implementeren, dus bedenk wat voor je bedrijf het belangrijkst is. Waar kun je het beste prioriteit aan geven: dagelijkse activiteiten, website, persoonsgegevens, intellectueel eigendom?

03.

Een veilige investering

Bedrijven tonen hun inzet voor cyberbeveiliging door tijd en geld te investeren in oplossingen en werkwijzen die kunnen helpen bij de bescherming en het detecteren van en reageren op cybercriminelen. Ze nemen verschillende maatregelen, waarvan sommige helemaal gratis zijn, om hun bedrijf te beschermen.

Wat oplossingen die geld kosten betreft: bedrijven reserveren ongeveer 15% van hun IT-budget aan cyberbeveiliging,[2] en de komende 12 maanden is 21% van plan om het budget voor bescherming van het bedrijf te verhogen.[2] Bedrijven begrijpen dat deze investering de moeite waard is, omdat drie van de vier bedrijven weet dat het meer kost om van een aanval te herstellen dan om deze te voorkomen.[2]

21% **van de bedrijven in het mkb is van plan om het budget voor cyberbeveiliging te verhogen[2]**

Bedrijven geven externe bedreigingen prioriteit

Bij cyberaanvallen denken de meesten van ons aan virussen, malware en andere externe bedreigingen. Dit komt tot uiting in de manier waarop de meeste bedrijven in het mkb in beveiliging investeren. De top vier van oplossingen waaraan bedrijven hun geld besteden, bestaat uit: eindpuntantivirussoftware, antiphishingsoftware, back-ups in de cloud en e-mailencryptie.[2] Deze oplossingen zijn gericht tegen de kwaadwillende, externe hacker. We zien de prioriteit voor bedreigingen van buitenaf ook terug in de praktijken die bedrijven erop na houden.

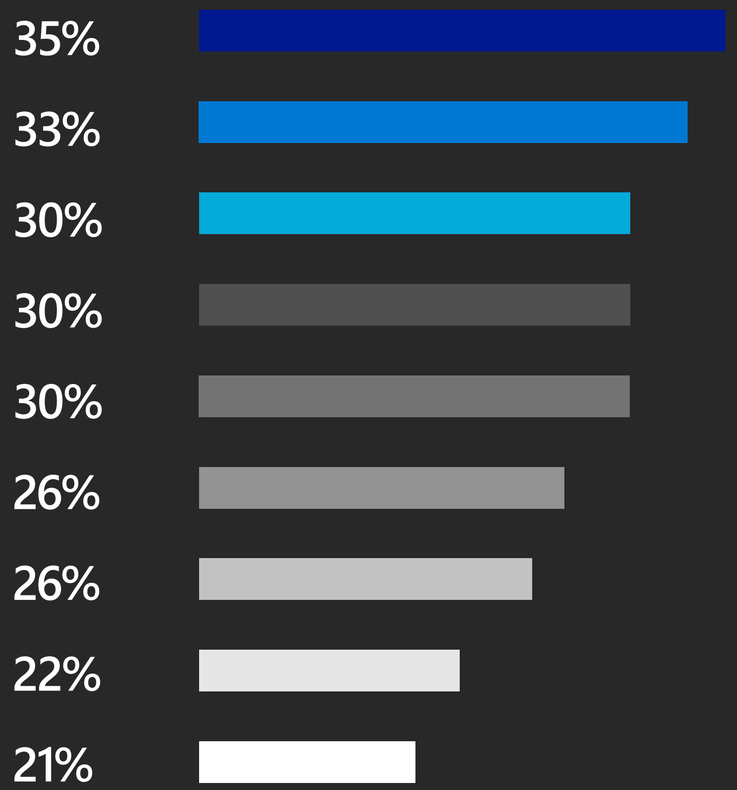
Meer dan 50% van de bedrijven meldt dat ze hun software regelmatig updaten (64%) en het gebruik van sterke en unieke wachtwoorden afdwingen (54%).[2]

58% Eindpuntantivirussoftware tegen virussen, malware en spyware

52% Antiphishingsoftware voor het identificeren en blokkeren van phishinginhoud in websites, e-mail, enz.

44% Versleutelde en geautomatiseerde back-ups in de cloud

43% E-mailencryptie om te voorkomen dat de inhoud wordt gelezen door anderen dan de beoogde ontvangers



- **Preventie van dataverlies (DLP)** om te voorkomen dat gebruikers per ongeluk gevoelige gegevens lekken
- **Classificatie en encryptie van** gevoelige documenten
- **Meervoudige verificatie (MFA)** om te verifiëren of de gebruiker is wie hij of zij zegt te zijn, door twee of meer bewijzen zoals een pincode, token, persoonlijke vraag, irisscan, vingerafdruk, enz. te combineren
- **Voorwaardelijke toegang,** waarmee bij het inloggen dynamisch en automatisch verschillende bevoegdheidsniveaus worden toegewezen aan medewerkers, gebaseerd op een aantal factoren zoals locatie, risico, rol, groepstoewijzing, enz.
- **Geavanceerde detectie van bedreigingen (ATP)**, een hoger beveiligingsniveau om de volgende generatie bedreigingen te voorkomen, detecteren en daarop te reageren
- **Beheer van mobiele apparaten (MDM)** om de toegang tot bedrijfsdata en -software op persoonlijke apparaten te beheren en in te trekken
- **Geautomatiseerd herstel,** waarmee waarschuwingen automatisch worden onderzocht en zonder menselijke tussenkomst tegen bedreigingen wordt opgetreden
- **Een dashboard** om gepersonaliseerde aanbevelingen over de meest effectieve cyberbeveiligingsmaatregelen te volgen en geven
- **Cloud app security broker (CASB)** om het gebruik van cloudapps te monitoren en beheren

Bereid je voor op het ergste

Als je behoort tot een van de 41% van de bedrijven in het mkb dat in het afgelopen jaar slachtoffer was van een cyberbeveiligingsincident [2], weet je al dat cyberbeveiliging belangrijk is. Je bent waarschijnlijk al aanvullende maatregelen aan het plannen. De beste manier om de kans te voorspellen dat een bedrijf tijd en middelen in cyberbeveiliging zou gaan steken, was door te kijken of het bedrijf in het afgelopen jaar was aangevallen. [2]

Een groter budget	45%	Aangevallen
	18%	Niet aangevallen
Officiële IT-verantwoordelijkheden	36%	Aangevallen
	22%	Niet aangevallen
Reactieplannen implementeren	44%	Aangevallen
	31%	Niet aangevallen
Trainingen bevorderen	42%	Aangevallen
	27%	Niet aangevallen

Bedrijven die zijn aangevallen, komen er snel achter dat het goedkoper is om in bescherming te investeren dan om van een aanval te herstellen. Bovendien is de kans groter dat ze hun budget voor beveiliging verhogen dan bij bedrijven die niet zijn aangevallen. Er zijn ook goedkope en gratis methoden om je beveiligingsstatus te verbeteren. Bedrijven die het doelwit van een aanval zijn geweest, verbeteren vaak de controleerbaarheid door de beveiligingsverantwoordelijkheden voor de belangrijkste IT-resources vast te leggen. Trainingen kunnen veel risico's verkleinen en bedrijven die het slachtoffer werden van een incident begrijpen dit. Ze zijn hun medewerkers gaan trainen op het detecteren en melden van verdachte links, bijlagen en e-mails, het vermijden van schadelijke websites en dat ze alleen geverifieerde applicaties mogen downloaden.

Een aanval is een chaotische en ontwapenende situatie. Eerder aangevallen bedrijven ontwikkelen vaker een reactieplan waarmee hun bedrijf tijdens een aanval strategisch kan reageren in plaats van ad hoc. Deze werkwijze kan ervoor zorgen dat kwaadwillenden korter toegang hebben tot gevoelige gegevens. Een goed reactieplan bevat een controlelijst met maatregelen waarin de rollen en verantwoordelijkheden tijdens een incident zijn vastgelegd. Het kan zaken bevatten zoals een contactenlijst voor technische, juridische en complianceresources, de hiërarchie voor het nemen van snelle beslissingen en een communicatieplan voor het op de hoogte brengen van belanghebbenden.

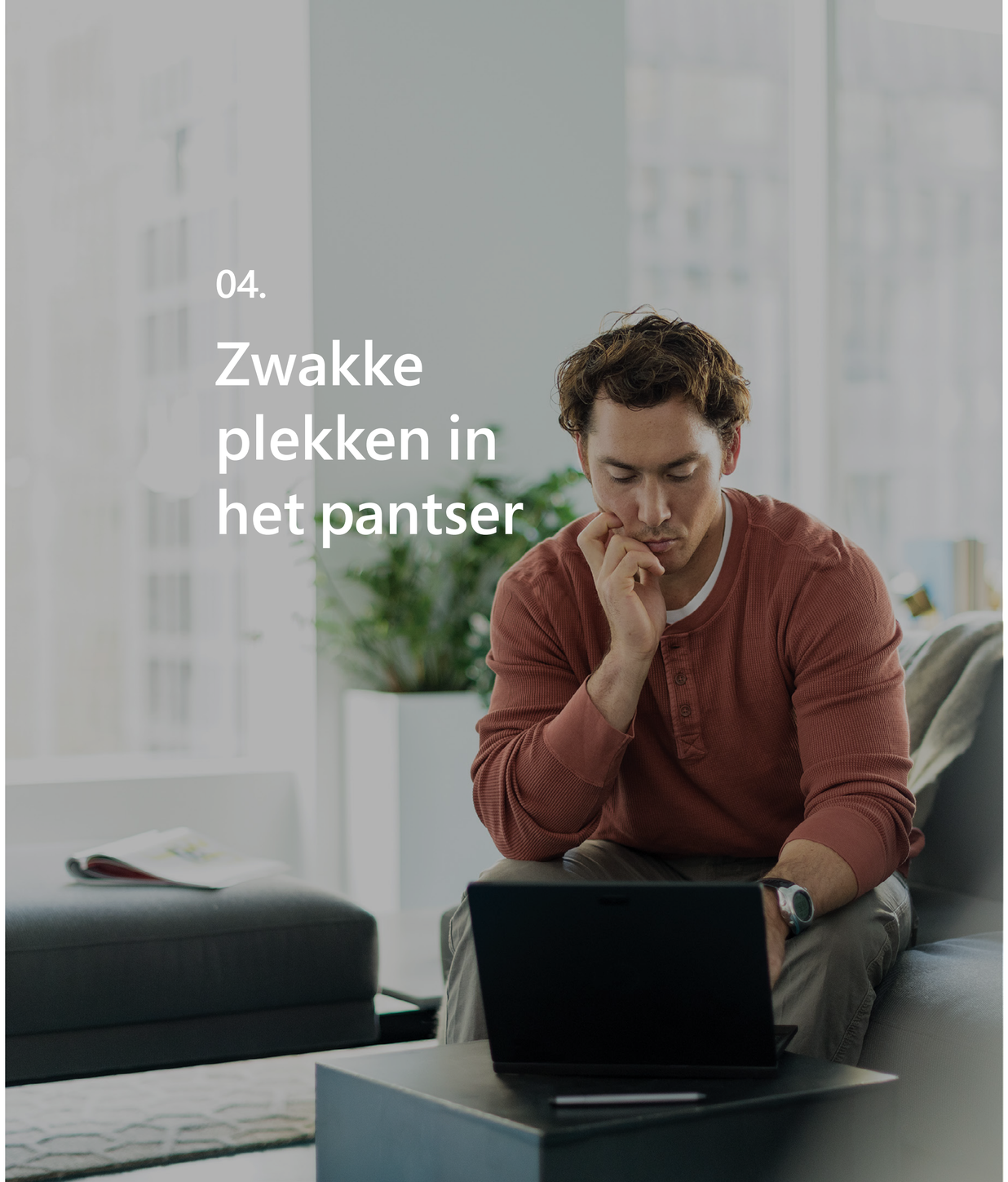
Om een beveiligingsbewuste mentaliteit te ontwikkelen, hoef je niet te wachten tot je wordt aangevallen. Of je nu drie maanden of drie jaar geleden bent aangevallen, of tot de gelukkigen behoort die nog geen doelwit zijn geweest: je kunt al beginnen om deze lessen bij je bedrijf in de praktijk te brengen.

“Je hebt geen tien miljoen dollar gewonnen.”

De directeur IT van een bedrijf in huishoudelijke artikelen en import beschrijft hoe hij humor gebruikt om medewerkers best practices voor beveiliging te leren.

Aanbevelingen

- Een beveiligingsbewuste mentaliteit aannemen
- Verantwoordelijkheden voor IT-beveiliging vastleggen en toewijzen
- Een speciaal budget voor beveiliging hebben
- Regelmatige trainingen voor medewerkers instellen
- Een reactieplan voor incidenten implementeren



04.
Zwakke plekken in het pantser

Als eigenaar van een bedrijf in het mkb word je met veel van dezelfde bedreigingen geconfronteerd als grote ondernemingen, maar ook met unieke uitdagingen.

Maar de meeste bedrijven in het mkb hebben niet dezelfde middelen om zich hiertegen te beschermen als grote ondernemingen. Gelukkig zijn er oplossingen en strategieën op maat die zijn ontworpen om de unieke kwetsbaarheden van kleinere bedrijven het hoofd te bieden.

Meer doen met minder

Als beslisser moet je kiezen hoe je de beperkte middelen van je bedrijf, zoals geld, mensen en tijd, effectief inzet. Maar omdat cyberbeveiliging een van de vele prioriteiten is, sta je onder grote druk om meer risico's te nemen.

Het goede nieuws is dat je niet zelf de expert hoeft te zijn. Veel consultants zijn gespecialiseerd in het helpen van bedrijven in het mkb bij het verbeteren van hun beveiliging. En het partnerprogramma van Microsoft kan je helpen bij het vinden van een vertrouwde leverancier van beveiligingsoplossingen die de ervaring heeft om je cyberbeveiligingsbehoeften aan te pakken.

72% van de bedrijven is het erover eens dat het meestal meer kost om van een cyberaanval te herstellen dan om deze te voorkomen

61% gelooft dat cyberbeveiliging belangrijk is, maar heeft er niet altijd genoeg budget voor

77% van de bedrijven zegt dat ze zouden profiteren van meer kennis over best practices voor cyberbeveiliging

59% heeft zelf geen tijd om proactief meer over cyberbeveiliging te weten te komen [2]

"Besteed uit wat je kunt uitbesteden."

Een eigenares van een bedrijf met 20 medewerkers legt uit hoe ze beveiligingsbeheer efficiënt aanpakt.

Budgetbeveiliging

Het goede nieuws is dat een effectieve beveiligingsstrategie niet duur of tijdrovend hoeft te zijn. Met een paar eenvoudige, gratis of goedkope maatregelen kun je een grote invloed op het algehele beveiligingsprofiel van je bedrijf hebben:

Wachtwoordbeleid: sterke wachtwoorden moeten uniek en anders dan persoonlijke wachtwoorden zijn. Niemand mag ze opschrijven of delen.

Regelmatige updates moeten verplicht zijn voor alle medewerkers op al hun hardware, software en services.

Wijzig gebruikersnamen en wachtwoorden op routers, kopieerapparaten en andere met wifi verbonden apparaten: hackers kennen de standaardwachtwoorden vaak.

Aanbevelingen

- Wachtwoordbeleid
- Gebruik gratis online bronnen en netwerken zoals us-CERT, NIST, SANS Institute, Microsoft en het Better Business Bureau
- Installeer de nieuwste patches en updates van software en systemen
- Wijzig gebruikersnamen en wachtwoorden op met wifi verbonden apparaten

Wees een goede detective

Als er toch een aanval plaatsvindt, is het van cruciaal belang om de inbraak snel te detecteren. Anders kunnen de kosten van de stilstand al snel de pan uitrijzen. Van de bedrijven die de toegang tot hun data drie maanden of langer kwijtraakten, bleef slechts 35% winstgevend. [3]

Kwaadwillenden worden steeds geraffineerder, dus is het niet ongewoon dat ze weken of maanden onzichtbaar blijven, terwijl ze continu kleine beetjes data stelen en langzaam meer toegang tot je accounts, apparaten en bestanden krijgen. Hoewel grote ondernemingen in het nieuws komen als ze het slachtoffer van heimelijke hackers worden, lopen bedrijven in het mkb evenveel gevaar.

10%

Tien procent van de bedrijven in het mkb kwam er pas na meer dan vier maanden achter dat hun systeem was gecompromitteerd.

En nog eens 10% besefte niet eens dat ze waren aangevallen.[3] Meer dan 10% van de bedrijven merkt niet dat ze zijn aangevallen en het duurt gemiddeld vier maanden om de aanval te herkennen.[3]

Bedrijven in het mkb begrijpen dat het noodzakelijk is om hackers voor te blijven en meer dan de helft (54%) heeft een proces voor het monitoren en detecteren van bedreigingsinformatie en -waarschuwingen.[2] Maar minder dan een kwart investeert in oplossingen om de binnenkomende signalen, beveiligingswaarschuwingen en aanbevelingen te monitoren.[2]

Met zo veel apparaten, netwerken, documenten en kwetsbaarheden om te beschermen, kunnen er veel signalen en ruis over kwaadaardige bedreigingen bestaan. Automatiserings- en informatieoplossingen kunnen de efficiëntie van bedrijven met beperkte middelen verbeteren door ze een uitgebreid en realtime overzicht van nuttige beveiligingsdata en -activiteiten te geven, waarbij valse signalen worden weggefilterd. Zorg er wel voor dat je binnenkomende waarschuwingen regelmatig leest, zodat je bedreigingen kunt vinden en tegenhouden voordat ze schade berokkenen.

Ten slotte moet je, hoe goed je detectietools en -strategieën ook zijn, waakzaam blijven en je gezonde verstand gebruiken. Blijf waakzaam voor verdacht gedrag en verdachte activiteiten, van ongebruikelijke transacties tot gebruikers die toegang hebben tot gevoelige netwerken die geen verband houden met hun rol.

Aanbevelingen

Investeer in een beveiligingsoplossing met de volgende detectiemogelijkheden:

- Realtime rapporten
- Geautomatiseerde en intelligente waarschuwingen
- Integratie van beveiligingsoplossingen in bedrijfsmiddelen

De grootste bedreigingen

Beveiligingsbedreigingen kunnen vele vormen aannemen, waarvan virussen, ransomware en phishingaanvallen het gevaarlijkst zijn. Maar gezien het aantal beveiligingsgevallen waarbij medewerkers betrokken zijn, lopen bedrijven het gevaar om te onderschatten welk risico ze lopen door medewerkers die data lekken of gevoelige informatie delen, zowel met opzet of per ongeluk.

Waargenomen beveiligingsbedreigingen

59% Verspreiding van virussen

27% Medewerkers die gevoelige data delen/lekken

46% Ransomware-aanval

14% Gestolen wachtwoorden van medewerkers

34% Phishingaanval

4% Overige

30% Diefstal van bedrijfs- en klantdata

Verspreiding van virussen | Ransomware | Phishing | Medewerkers die gevoelige data lekken en delen

Verspreiding van virussen

De verspreiding van virussen werd door bedrijven het meest genoemd als beveiligingszorg,[2] vanwege het enorme aantal apparaten en cloudapplicaties dat hackers kunnen infecteren. Als reactie hierop besloot 58% van de bedrijven om antivirussoftware te installeren. Antivirussoftware[2] wordt vaak bij een nieuwe pc geleverd. Een voorbeeld hiervan is Windows Defender Antivirus, dat bij het besturingssysteem Windows wordt geleverd. Zorg ervoor dat je software uitgebreide bescherming tegen malware, spyware en virussen in e-mails, applicaties, de cloud en op internet biedt.

60% **van de lekken is het gevolg van een gecompromitteerd eindpunt, zoals een laptop of telefoon**

Oplossingen voor mobiel apparaatbeheer (MDM) zoals Intune (onderdeel van Microsoft 365 Business) kunnen mobiele apparaten helpen beschermen, door te zorgen dat ze up-to-date zijn en veilige toegang tot e-mail, documenten en andere middelen hebben.

Bedrijven moet ook een oplossing voor identiteits- en toegangsbeheer gebruiken, zoals Azure Active Directory (ook een onderdeel van Microsoft 365 Business) dat single sign-on ondersteunt en medewerkers een enkele, veilige identiteit voor toegang tot netwerkbronnen geeft.

Verspreiding van virussen

Ransomware

Phishing

Medewerkers die gevoelige data lekken en delen

Zorg ook voor meervoudige verificatie (MFA), waarbij gebruikers zich moeten identificeren aan de hand van iets dat ze weten, zoals een wachtwoord, en een aanvullende verificatiemethode, zoals een biometrisch kenmerk of een vingerafdruk. Het hebben van een sterke MDM, IAM en MFA zal de beveiliging flink verbeteren en productiviteit op elke plek en elk apparaat mogelijk maken.

Aanbevelingen

- Installeer antivirussoftware
- Beveilig privéapparaten en zakelijke apparaten:
  - Mobiel apparaatbeheer (MDM)
  - Identiteits- en toegangsbeheer (IAM)
  - Meervoudige verificatie (MFA)

Verspreiding van virussen

Ransomware

Phishing

Medewerkers die gevoelige data lekken en delen

Ransomware

Ransomware is een soort malware dat toegang beperkt, bestanden versleutelt en je er zelfs van weerhoudt om je pc's te gebruiken. Vervolgens probeert het je te dwingen om losgeld te betalen om de toegang terug te krijgen. Net als een virus kan ransomware het bedrijf via onveilige eindpunten of nietsvermoedende gebruikers binnendringen.

Het bewaren van data op een externe, versleutelde en geteste locatie, bij voorkeur in de cloud, kan de schade van een ransomware-aanval beperken. Overweeg tools zoals BitLocker en OneDrive for Business van Microsoft te gebruiken. En als je binnen je bedrijf niet over de nodige kennis beschikt: ransomware is een ernstige bedreiging voor je bedrijf. Schakel een beveiligingsconsultant in met ervaring in het beschermen tegen ransomware.

Aanbevelingen

- Versleutel gevoelige data en maak er back-ups van in de cloud
- Huur iemand in die ervaring met ransomware heeft.

Verspreiding van virussen

Ransomware

Phishing

Medewerkers die gevoelige data lekken en delen

Phishing

Veel mensen hebben zich door een e-mail van een op het oog legitieme afzender laten misleiden om gevoelige informatie te verstrekken. En één bedrogen medewerker is genoeg om met een phishingcampagne grote schade toe te brengen.

Om je bedrijf tegen onveilige e-mails, bijlagen en links te beschermen, moet je antiphishingsoftware gebruiken, zoals de oplossing die onderdeel van Microsoft 365 Business uitmaakt. Phishing is ook een soort bedreiging waarbij het trainen van medewerkers veel verschil kan maken. 44% van de bedrijven in het mkb traint zijn medewerkers niet in het herkennen van phishingcampagnes, maar gelukkig is dit gratis op te lossen.

Aanbevelingen

- Schaf tools met antiphishingfuncties aan
- Train medewerkers hoe ze phishingmails, -bijlagen, -links en -websites kunnen herkennen

Verspreiding van virussen

Ransomware

Phishing

Medewerkers die gevoelige data lekken en delen

Medewerkers die gevoelige data lekken en delen

Zelfs de meest beveiligingsbewuste bedrijven zijn verrast door het volgende: de kans dat je door een intern iemand met een beveiligingsincident te maken krijgt is even groot als een externe bedreiging. De afgelopen 12 maanden was 53% van de organisaties het slachtoffer van een aanval van binnenuit.[4]

De bedreigingen van binnenuit kunnen verschillende vormen aannemen. Medewerkers of partners vinden het misschien handiger om gevoelige data via de persoonlijke e-mail of een onbeveiligde cloudopslag te versturen, zonder dat ze zich bewust zijn van de risico's voor je bedrijf. 30% van de beveiligingsincidenten wordt zelfs toegeschreven aan onzorgvuldige of ongeïnformeerde medewerkers.[5] Alarmerender is dat ongeveer 36% van de aanvallen werd uitgevoerd door een kwaadwillende medewerker die gevoelige data steelt.[5]

Maar er zijn goedkope manieren om je tegen bedreigingen van binnenuit te beschermen, terwijl medewerkers nog altijd de tools krijgen waarmee ze productief kunnen zijn. Omdat mensen, rollen en verantwoordelijkheden met de tijd veranderen, kan het bijvoorbeeld een goed idee zijn om regelmatig te evalueren wie toegang heeft tot welke data, systemen, apparaten en netwerken. Hoewel maar 36% van de bedrijven deze evaluaties uitvoert,[2] kan het een verschil maken.

Zorg ook dat gebruikers op basis van hun rol op het juiste moment het juiste toegangsniveau hebben. Iemand in personeelszaken heeft misschien voor een bepaald project toegang tot een financiële database nodig, maar zodra het project is voltooid niet meer. Zorg dat je de rechten intrekt van mensen die je organisatie hebben verlaten of een andere rol hebben gekregen en onderneem actie bij verdachte activiteiten die zijn gedetecteerd.

> Ons bedrijf weet nog altijd niet of het incident [doelbewust] door een medewerker werd veroorzaakt of door een phishingaanval. Het eindresultaat was dat het bedrijf een dag lang volledig werd stilgelegd, er tot geen enkel bestand toegang was en dat bestanden doelbewust offline waren gehaald en waren beschadigd. Daardoor moesten we veel kosten maken om [het] netwerk te herstellen en te zorgen dat het incident niet opnieuw zou gebeuren.

SMB, us[2]

Verspreiding van virussen

Ransomware

Phishing

Medewerkers die gevoelige data lekken en delen

Je kunt het risico op een datalek ook verminderen door een informatiebeschermingsoplossing met de volgende mogelijkheden te gebruiken:

- Met preventie van dataverlies kun je voor gevoelige data definities instellen, e-mails scannen op gevoelige gegevens en beleidsregels toepassen, zoals het blokkeren, versleutelen of het geven van een waarschuwing.

- Bescherming op documentniveau beschermt de documenten zelf. Stel beleid in waarin wordt vastgelegd wat voor soort informatie kan worden gedeeld of dat bepaalde soorten informatie automatisch worden versleuteld. Je kunt er ook mee voorkomen dat bepaalde personen toegang tot deze documenten krijgen. De auteurs van documenten kunnen ook wachtwoorden instellen of het bewerken of delen van bepaalde stukken beperken, zodat je er beter voor kunt zorgen dat documenten met gevoelige gegevens in de juiste handen blijven.

- Dataclassificatie zorgt er ook voor dat je op basis van de bron, context en inhoud labels kunt toevoegen als een document is aangemaakt of bewerkt. De classificatie kan volledig automatisch plaatsvinden, door gebruikers worden aangestuurd of op aanbevelingen worden gebaseerd.

Aanbevelingen

- Evalueer regelmatig welke gebruikers toegang tot data, apparaten en netwerken hebben

- Volg, verander en blokkeer toegang voor tijdelijke projecten en wanneer medewerkers het bedrijf verlaten

- Gebruik oplossingen voor informatiebescherming om je data overal te beschermen:
  - Preventie van dataverlies
  - Bescherming op documentniveau
  - Dataclassificatie

05.
Van een aanval herstellen

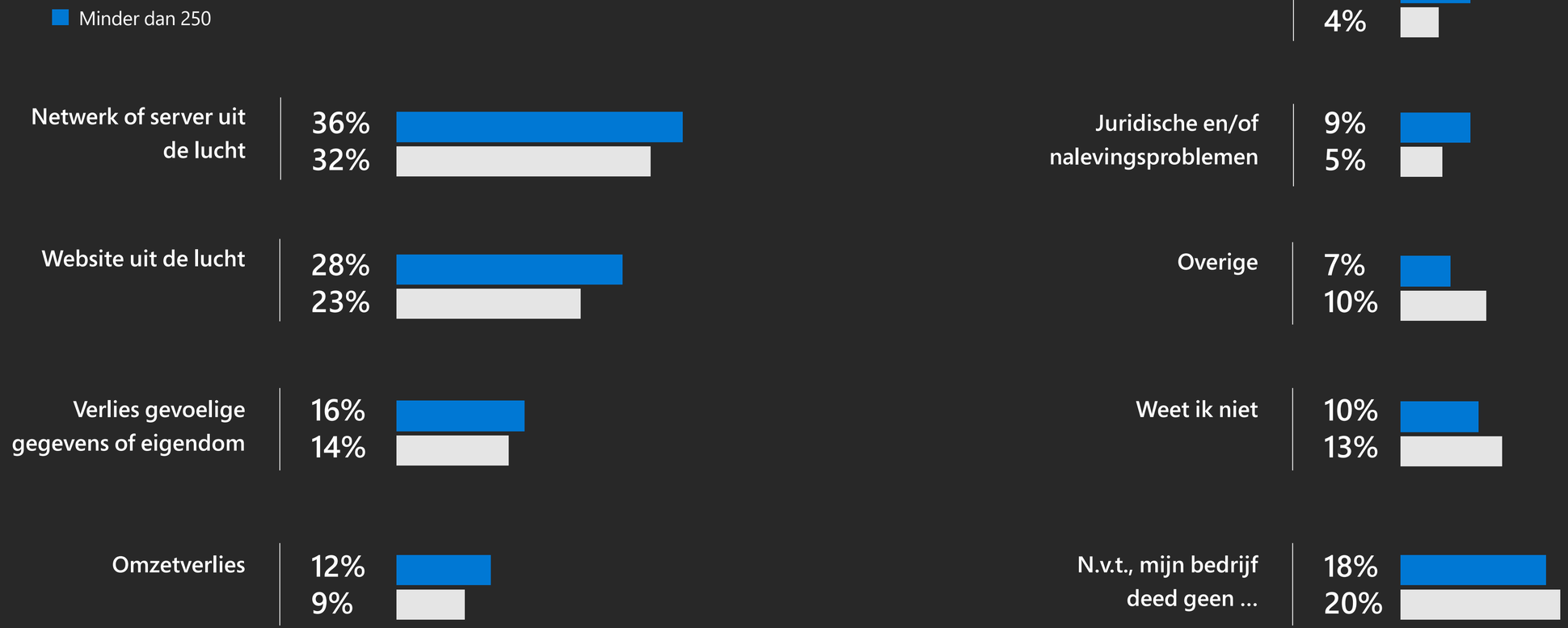
Als je het slachtoffer van een cyberaanval bent geweest, ben je niet de enige. 41% van de bedrijven in het mkb is het slachtoffer van een beveiligingsgebeurtenis geweest.[2]

Keer op keer blijkt dat geen bedrijf te klein is om een doelwit te zijn. Zelfs het kleinste bedrijf moet waakzaam zijn, vooral omdat een veiligheidsincident ongelooflijk verstorend en duur kan zijn. In de meest extreme gevallen moesten bedrijven vanwege een aanval sluiten. Als je erdoor wordt overvallen, kun je je beschadigd voelen of je gevoel van vertrouwen verliezen. Maar je kunt je ervan herstellen en als je je voorbereidt, kun je de schade beperken.

> Ik zou willen dat ik een beter idee had van wat er zou kunnen gebeuren … als je bedenkt dat ik, ergens in Nergenshuizen … ik had gewoon niet bedacht dat het mij zou kunnen overkomen. Het was een harde les. Ik ben net zo kwetsbaar als een groot bedrijf. Of het nu een miljoen mensen raakt of vier, het maakt niet uit. [Nadat je bent geraakt], heb je klanten die hun vertrouwen in je kwijt zijn. En ik wil niemands handel kwijtraken, zeker niet door iets waar ik iets tegen kan doen.

SMB Customer[5]

Wereldwijd is het meest voorkomende gevolg van een aanval dat het netwerk of de website uit de lucht gaat. Veel bedrijven raken ook gevoelige gegevens of omzet kwijt.



Hersteltijd eist zijn tol

Hoewel bedrijven in het mkb net zo kwetsbaar voor cyberaanvallen zijn als grote ondernemingen, hebben ze vaak niet de middelen beschikbaar om snel te reageren. Van de bedrijven in het mkb die werden aangevallen, kostte het 43% meer dan een week om te herstellen.[2] Dit kan in de papieren lopen. Aanvallen waarvan het langer dan een week duurt om te herstellen kosten gemiddeld $ 79.841.[4] Op de langere termijn kan een aanval de plannen om het bedrijf te laten groeien dwarsbomen en een zuurverdiende reputatie beschadigen, vooral als het om data van klanten gaat. Maar 35% van de bedrijven in het mkb dat meer dan drie maanden lang toegang tot zijn data verliest, blijft winstgevend.[5]

"De impact van CryptoLocker [een soort ransomware] was vrij groot: ongeveer $ 50.000."

Een directeur IT vertelt over de werkelijke kosten van een maar al te vaak voorkomende cyberaanval.

Waakzaam blijven

Een cyberaanval kan voor elk bedrijf een ernstige en ontwrichtende gebeurtenis zijn. Maar onthoud: je bent niet de enige. Bedrijven zoals dat van jou nemen maatregelen om hun mensen en data met succes te beschermen, door een mentaliteit aan te nemen waarmee ze op een beveiligingsincident zijn voorbereid. Het is goedkoper om vooruit te plannen, maar dat is niet het enige: het geeft je ook gemoedsrust. Als je wordt aangevallen, is de kans dat je het snel detecteert en ervan herstelt groter als je de juiste processen, mensen en systemen hebt. Gespecialiseerde tools, soms bekend onder de noemer advanced threat protection (ATP), waar 30% van het mkb gebruik van maakt, [2] kunnen hierbij helpen. ATP-oplossingen, zoals de oplossing in Microsoft 365 Business, bieden de volgende essentiële functies:

- Bescherming van identiteiten, e-mail, apps, netwerken, data en apparaten
- Bescherming tegen geavanceerde aanvallen zoals zero-daykwetsbaarheden en social engineering
- Zichtbaarheid en detectie van abnormaliteiten binnen je bedrijf en systemen, vooral met gedragsanalyse- en machine learning-mogelijkheden
- Reactie en herstel, zodat je de schade in het geval van een succesvolle inbraak kunt beperken

Aanbevelingen

- Gebruik een oplossing met advanced threat protection (ATP)

06.

Laat je bedrijf groeien met beveiliging in het achterhoofd

Cyberbedreigingen blijven voorlopig wel bestaan. Cybercriminaliteit is een grote bedrijfstak en blijft groeien. Cybercriminaliteit kost rond 2021 naar schatting $ 6 biljoen,[6] en de schade van alleen ransomware wordt al geschat op $ 11,5 miljard in 2019.[7]

De noodzaak om je bedrijf tegen deze criminelen te beschermen blijft toenemen. Maar je kunt de mentaliteit van de meest weerbare bedrijven overnemen door je op een beveiligingsincident voor te bereiden en de kans op en ernst van een aanval te verminderen. Als je de lessen opvolgt die in dit rapport worden gedeeld, kun je het risico minimaliseren en wat er op je afkomt het hoofd bieden.

De meest effectieve beveiligingsstrategieën zijn vaak de eenvoudigste

Het aanpakken van zelfs de meest complexe beveiligingsuitdagingen begint vaak met een zeer eenvoudige tactiek, zoals de tips die we in het rapport hebben besproken en hieronder samenvatten. Sommige zijn eenvoudig genoeg om snel en gemakkelijk in je dagelijkse routine te integreren. En dat is de sleutel tot de meest effectieve beveiliging: houd het eenvoudig voor medewerkers, houd ze op de hoogte met elementaire beveiligingsbewustzijn en -trainingen en automatiseer zoveel mogelijk.

Algemeen

- Leun niet achterover: ontwikkel basiskennis over algemene beveiligingsconcepten en -risico's
- Huur een partner met beveiligingskennis in om je specifieke beveiligingsbehoeften te bepalen en aan te pakken
- Geeft prioriteit aan wat het beste moet worden beschermd
- Stel een budget vast

Beschermen

- Plan regelmatige trainingen over algemene beveiligingspraktijken voor medewerkers
- Gebruik meervoudige verificatie die vereist dat gebruikers naast een gebruikersnaam en wachtwoord voor extra verificatie zorgen om hun identiteit te bevestigen
- Verander de gebruikersnamen en wachtwoorden van met wifi verbonden apparaten zoals routers en kopieerapparaten
- Zorg dat alle medewerkers sterke, unieke wachtwoorden gebruiken, of overweeg een wachtwoordloze benadering met gezichtsherkenning, vingerafdrukken en pincodes om veilig in te loggen.
- Antivirussoftware voor uitgebreide bescherming tegen malware, spyware en virussen in e-mails, applicaties, de cloud en op internet
- Maak back-ups van essentiële data, bij voorkeur in de cloud, en zorg voor een systeem om dit regelmatig te doen
- Informatiebescherming, waaronder preventie van dataverlies, documentbescherming en dataclassificatie

Detecteren

- Evalueer regelmatig de toegang, houd bij wie toegang tot informatie heeft en informatie deelt en trek toegang tot documenten, data en apps in als dat nodig is
- Stel een proces in voor het monitoren van waarschuwingen, wijs daar personeel voor aan en reageer als dat nodig is
- Implementeer een detectiesysteem om te zorgen dat je een uitgebreid en realtime overzicht van nuttige beveiligingsdata en -activiteiten hebt

Reageren

- Houd een reactieplan voor incidenten gereed voor het geval een cyberaanval succes heeft en deel het vóór (en niet na) een mogelijke aanval met je medewerkers
- Gebruik oplossingen met Advanced Threat Protection die reactie en herstel bieden, zodat je de schade bij een succesvol lek kunt beperken.

Tenzij je bedrijf toevallig een computerbeveiligingsbedrijf is, ben je je organisatie waarschijnlijk niet gestart of er niet gaan werken met de verwachting dat je, naast al je andere prioriteiten, ook beschermingen tegen cybercriminelen zou moeten opzetten of trainingssessies over phishing en meervoudige verificatie zou moeten houden. Dit is een nieuwe realiteit waar bedrijven in het mkb nu mee worden geconfronteerd. Gelukkig blijkt uit ons onderzoek dat bedrijven in het mkb hun mouwen opstropen en deze uitdaging met vertrouwen aangaan. Steeds meer bedrijven in het mkb merken dat ze een balans kunnen vinden tussen beveiliging en alle andere behoeften en verwachtingen van hun bedrijf.

Gewapend met de tips, oplossingen en werkwijzen in dit rapport, kun ook jij je bedrijf beveiligen!

Ontvang gepersonaliseerde aanbevelingen

Doe Microsofts beveiligingsevaluatie om specifiekere aanbevelingen voor het verbeteren van de beveiliging van je bedrijf te krijgen.

[1] Cybersecurity Statistics – Numbers Small Businesses Need to Know
[2] Microsoft's Global Security Survey for Small and Medium-Sized Businesses
[3] 2017 State of Cybersecurity Among Small Businesses in North America – Better Business Bureau
[4] Insider Threat 2018 Report
[5] SMB Security Qual
[6] The 2017 Official Annual Cybercrime Report by the Herjavec Group
[7] Ransomware Damage Report, 2017 door Cybersecurity Ventures