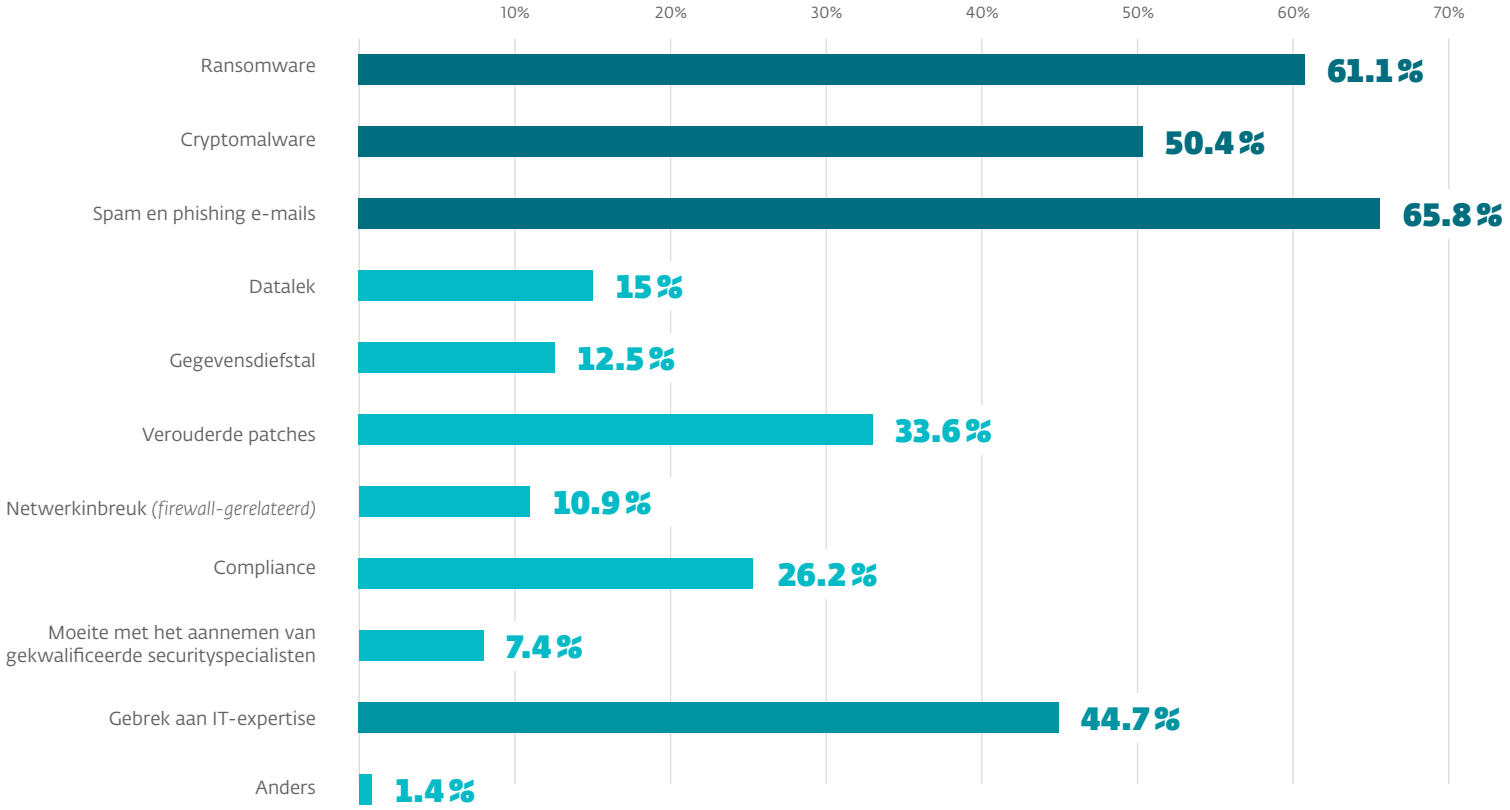
ESET MSP-PROGRAMMA

DE GROOTSTE BEVEILIGINGSUITDAGINGEN VOOR HET MKB

1. RANSOMWARE
2. SOCIAL ENGINEERING
3. ILLEGALE CRYPTOMINING
4. WACHTWOORDVEILIGHEID

Het aanpakken van de belangrijkste beveiligingsuitdagingen voor het mkb die door MSP'ers zijn geïdentificeerd

We hebben onze MSP-partners gevraagd naar de belangrijkste uitdagingen die zij tegenkomen bij het beschermen van hun klanten. Bijna 500 MSP'ers reageerden en gaven aan dat **ransomware**, **cryptomalware** en **social engineering-aanvallen** via spam en phishing e-mails — naast een **algemeen gebrek aan IT-expertise** — grote zorgen zijn. Daarom geven wij u advies over hoe u deze problemen kunt aanpakken.

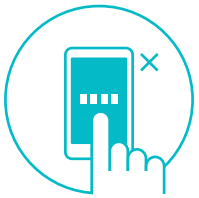


Bron: ESET poll onder 488 MSP-partners in 14 landen in juli 2019, via een online survey

1 Ransomware
Hoe werkt het?

Er zijn meerdere technieken die door ransomware-cybercriminelen worden gebruikt, waaronder:

Schermvergrendelings-ransomware
blokkeert toegang tot het scherm van een apparaat voor andere toepassingen dan om de gebruikersinterface van de malware te bekijken



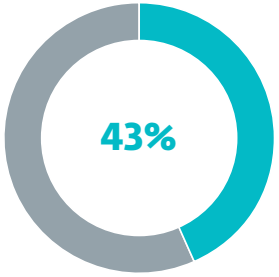
Pinvergrendelings-ransomware
verandert de toegangscode van het apparaat, waardoor de inhoud en functionaliteiten niet meer toegankelijk zijn

Schijfversleutelings-ransomware
versleutelt de MBR (Master Boot Record) en/of kritieke bestandssysteemstructuren en voorkomt hiermee dat de gebruiker toegang heeft tot het besturingssysteem

Crypto-ransomware
versleutelt gebruikers-bestanden die op de schijf zijn opgeslagen

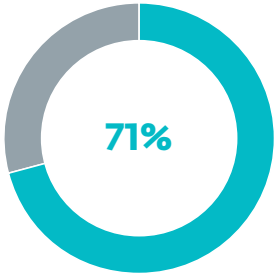
Waarom is dit belangrijk voor mkb'ers?

Kleine en middelgrote ondernemingen zijn een steeds aantrekkelijker doelwit voor cybercriminelen. Zij zijn waardevollere doelwitten dan consumenten en kwetsbaarder dan enterprises.



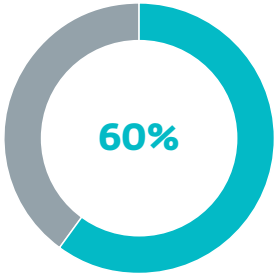
43% van de slachtoffers van gegevensdiefstal zijn mkb'ers.

Bron: Verizon 2019 Data Breach Investigations report (DBIR)



71% van de gevallen van gegevensdiefstal hebben een financiële drijfveer

Bron: Verizon 2019 Data Breach Investigations report (DBIR)



60% van de slachtoffers betaalde het gevraagde losgeldbedrag

Bron: Ponemon 2017 State of Cybersecurity in Small & Medium-Sized Businesses (SMB) survey

MSP'ers geven aan dat het **gemiddelde losgeldbedrag dat aan mkb'ers wordt gevraagd $ 4.300,- is** en dat de gemiddelde kosten van een ransomware-gerelateerde werkonderbreking neerkomen op $ 46.800,-.

Bron: Datto 2018 State of the Channel Ransomware Report

BETAAL NIET!

Er is absoluut geen garantie dat cybercriminelen hun deel van de afspraak zullen nakomen (soms kunnen ze dit niet eens, met opzet of als gevolg van onbekwame codering). ESET **raadt aan het geëiste bedrag niet te betalen** — in ieder geval niet voordat de technische supportafdeling van uw beveiligingsaanbieder is gebeld om te bespreken welke mogelijkheden er zijn voor ontsleuteling.

Hoe houdt u uw systemen veilig?

Basisaanbevelingen

Er zijn een aantal dingen die u kunt doen om te voorkomen dat ransomware uw dag verpest. Laten we beginnen met wat er vooraf kan worden gedaan om te voorkomen dat malware überhaupt op uw systeem terechtkomt en om de schade te minimaliseren als het toch gebeurt.

1. Maak regelmatig een **back-up van gegevens** en bewaar ten minste één volledige back-up van de meest waardevolle gegevens offline.
2. Houd alle software en apps – inclusief besturingssystemen – **gepatcht en geüpdatet.**
3. **Gebruik een betrouwbare, meerlaagse beveiligingsoplossing** en zorg ervoor dat ook deze gepatcht en up-to-date is.

Aanvullende beschermingsmaatregelen

- **Verminder het aanvalsoppervlak** door onnodige diensten en software uit te schakelen of te de-installeren
- **Scan netwerken** op risicovolle accounts die gebruikmaken van zwakke wachtwoorden en zorg ervoor dat deze worden verbeterd
- **Beperk of verbied het gebruik van Remote Desktop Protocol (RDP)** van buiten het netwerk, of schakel authenticatie op netwerkniveau in
- **Gebruik een Virtual Private Network (VPN)** voor toegang op afstand
- **Bekijk de instellingen van de firewall** en sluit alle niet-essentiële poorten die tot een infectie kunnen leiden
- **Beoordeel het huidige beleid voor verkeer** tussen interne bedrijfssystemen en externe netwerken
- **Bescherm de configuraties** van uw beveiligingsoplossingen met een wachtwoord
- **Segmenteer het LAN van het bedrijf in subnetten en sluit deze aan op firewalls** om de potentiële impact van aanvallen binnen het netwerk te beperken
- **Bescherm back-ups** met multifactorauthenticatie (MFA)
- **Train medewerkers** regelmatig in het herkennen van cyberdreigingen en ontwijken van social engineering-aanvallen
- **Beperk de toegang tot gedeelde bestanden/mappen** tot alleen degenen die het echt nodig hebben
- **Schakel detectie van potentieel onveilige/ongewenste applicaties (PUSA/PUA) in** om tools te blokkeren die door aanvallers misbruikt kunnen worden om de beveiligingsoplossing uit te schakelen

2 Social engineering
Het probleem definiëren

Social engineering is een categorie van niet-technische aanvalstechnieken die door cybercriminelen worden gebruikt om gebruikers door middel van manipulatie zover te krijgen dat zij de beveiligings- of andere bedrijfsprotocollen doorbreken, schadelijke acties uitvoeren of gevoelige informatie doorgeven.

- **Social engineering-technieken vereisen meestal niet veel technische vaardigheden** van de aanvaller, waardoor alle soorten cybercriminelen – van kleinschalige dieven tot gevorderde hackers – het kunnen proberen.

- De schade is reëel en omvangrijk, wat goed geïllustreerd wordt door het jaarverslag van het FBI Internet Crime Complaint Center (IC3), dat schat dat Amerikaanse bedrijven alleen in 2018 al **meer dan $ 2,7 miljard verloren aan cyberaanvallen**. $ 1,2 miljard daarvan werd toegeschreven aan Business Email Compromise (BEC) / Email Account Compromise (EAC), waarbij oplichters de controle over de legitieme e-mailaccounts van senior personeelsleden overnamen en deze misbruikten om ongeoorloofde geldtransacties te regelen/verrichten.

- Zelfs een aantal van de meest geavanceerde cyberaanvallen in de geschiedenis, zoals Black Energy, GreyEnergy of Industroyer, gebruikten phishing en andere vormen van social engineering als hun eerste aanvalsvectoren, wat de **doeltreffendheid van deze technieken** en hun populariteit onder cybercriminelen demonstreert.

100% stijging van wereldwijde verliezen als gevolg van gerichte BEC/ EAC-oplichting tussen mei 2018 en juli 2019

Bron: FBI Public Service Announcement, September 10, 2019.

Hoe cybercriminelen ons proberen te misleiden

Er zijn veel technieken die onder de parapluterm social engineering vallen. Deze komen het vaakst voor:

Spam
is elke vorm van ongevraagde massacommunicatie. Spam is meestal een commerciële e-mail die naar zoveel mogelijk gebruikers wordt verstuurd, maar kan ook via instant messages, sms'jes en sociale media worden verzonden. Spam is op zich geen social engineering, maar sommige campagnes maken gebruik van social engineering-technieken zoals phishing, spearphishing, vishing, sms-phishing of het verspreiden van kwaadaardige bijlagen of links.

Imitatie
door cybercriminelen wil zeggen dat zij handelen in naam van een vertrouwd persoon om slachtoffers te misleiden en acties te laten ondernemen die hen of hun organisaties schade berokkenen. Een typisch voorbeeld is een aanvaller die zich voordoet als CEO van een bedrijf die frauduleuze transacties aanvraagt en goedkeurt.

Phishing
is een cyberaanval waarbij de crimineel zich voordoet als een betrouwbare entiteit die het slachtoffer om gevoelige informatie vraagt, meestal per e-mail. Vectorspecifieke subtypes zijn onder andere **vishing** (**v**oice **phishing**), waarbij gebruik wordt gemaakt van frauduleuze telefoongesprekken, en **smishing** (**sm**s p**hishing**), waarbij gebruik wordt gemaakt van sms-berichten met kwaadaardige links of inhoud. Deze vormen van fraude proberen meestal een gevoel van urgentie te creëren, of maken het slachtoffer bang, om hen te dwingen aan de verzoeken van de aanvaller te voldoen. Phishing-campagnes kunnen zich richten op grote aantallen anonieme gebruikers, of op een specifiek slachtoffer of kleine groep van verbonden slachtoffers.

Spearphishing
is een gerichte vorm van phishing waarbij de aanvaller speciaal aangepaste berichten verstuurt naar een beperkte groep mensen, of zelfs naar een individu, met als doel hun gegevens te verzamelen of ze te manipuleren om schadelijke handelingen te verrichten.

Technical Support Scams
zijn meestal neptelefoongesprekken of -webadvertenties waarin aanvallers het slachtoffer ongevraagd technische ondersteuning aanbieden. In werkelijkheid proberen cybercriminelen geld te verdienen door valse diensten te verkopen en niet-bestaande problemen op te lossen.

Scareware
is software die gebruikmaakt van verschillende angst-veroorzakende technieken om slachtoffers te manipuleren om meer kwaadaardige code op hun apparaten te installeren, vaak terwijl er betaling wordt gevraagd voor niet-functionele of ronduit schadelijke software. Een typisch voorbeeld is een nep-antivirusproduct dat is ontworpen om gebruikers te laten denken dat hun apparaten zijn geïnfecteerd en dat ze moeten betalen voor de volledige versie met opschoonfunctionaliteit (dit kan dan juist weer een vector zijn voor verdere infiltratie).

Leer een social engineering-aanval herkennen

Gevoel van urgentie

De criminelen achter social engineering-campagnes proberen slachtoffers vaak actie te laten ondernemen uit angst, door gebruik te maken van angst-veroorzakende zinnen als “stuur ons direct uw gegevens, of uw pakket wordt weggegooid” of “als u uw profiel nu niet bijwerkt, sluiten wij uw account”. Banken, pakketbedrijven, openbare instellingen en zelfs interne diensten communiceren meestal op een neutrale en feitelijke manier. Als het bericht probeert de ontvanger te dwingen om snel te handelen, is het daarom aannemelijk dat het bericht kwaadwillend en mogelijk een gevaarlijke poging tot oplichting is.

Slechte taalvaardigheid

Meestal besteden aanvallers niet veel aandacht aan details en versturen zij berichten vol tikfouten, ontbrekende woorden en slechte grammatica. Een ander taalkundig element dat een aanvalspoging kan aanduiden is algemene begroetingen en formuleringen. Dus als een e-mail begint met “Beste ontvanger” of “Beste gebruiker”, wees dan op uw hoede.

Vreemd afzendadres

De meeste spammers nemen niet de tijd om de naam of het domein van de afzender te vervalsen om deze er betrouwbaar uit te laten zien. Als een e-mail afkomstig is van een adres dat een mix is van willekeurige getallen en karakters, of onbekend is bij de ontvanger, zou deze direct in de spam-map moeten worden geplaatst en gerapporteerd moeten worden aan de IT-afdeling.

Verzoeken om gevoelige informatie

Instellingen en zelfs andere afdelingen binnen uw eigen bedrijf zullen normaal gesproken niet om gevoelige informatie vragen via e-mail of telefoon – tenzij het contact is geïnitieerd door de werknemer.

Als iets te mooi klinkt om waar te zijn, dan is het dat waarschijnlijk ook

Dit geldt net zo voor ongevraagde giveaways op sociale media als voor die “geweldig, maar beperkt geldig zakelijk aanbod” die net in uw inbox terecht is gekomen.

Hoe kan uw organisatie zich beschermen tegen aanvallen?

Er zijn meerdere dingen die u en uw MSP'er kunnen doen om u te beschermen tegen social engineering:

- **Regelmatige cybersecurity-training voor ALLE medewerkers**, inclusief het management en IT-personeel. Onthoud dat zulke trainingen echte scenario's moeten bevatten of simuleren. Leerpunten moeten actiegericht zijn en vooral actief getest worden buiten de trainingsruimte: social engineering-technieken zijn effectief vanwege het lage cybersecurity-bewustzijn van hun doelwitten.

- **Scan op zwakke wachtwoorden** die mogelijk een open deur in het netwerk van uw organisatie kunnen worden voor aanvallers. Bescherm wachtwoorden daarnaast met een extra beveiligingslaag door het implementeren van multifactorauthenticatie.

- **Implementeer technische oplossingen om oplichtingscommunicatie aan te pakken**, zodat spam- en phishingberichten gedetecteerd, in quarantaine geplaatst, geneutraliseerd en verwijderd worden. Beveiligingsoplossingen, waaronder veel van de oplossingen die ESET biedt, hebben een aantal of al deze mogelijkheden.

- **Creëer een begrijpelijk beveiligingsbeleid** dat werknemers helpt om te bepalen welke stappen ze moeten nemen als ze in aanraking komen met social engineering.

- **Gebruik een beveiligingsoplossing en beheerconsole**, zoals ESET PROTECT, om de werkstations en netwerken van uw organisatie te beschermen door beheerders volledig inzicht te geven en de mogelijkheid te bieden potentiële bedreigingen in het netwerk te detecteren en te mitigeren.

3 Illegale cryptomining
Een verborgen dreiging

Een illegale cryptominer is potentieel ongewenste of schadelijke code die ontworpen is om de inactieve rekenkracht van een apparaat te kapen en te misbruiken om cryptocurrency te minen. De activiteit is meestal verborgen of draait zonder toestemming van de gebruiker of beheerder op de achtergrond.

Er zijn twee hoofdtypen illegale cryptominers:

Binair-gebaseerde cryptominers zijn schadelijke applicaties die op het doelapparaat worden gedownloaded en geïnstalleerd met het doel om cryptocurrency te minen. ESET-beveiligingsoplossingen categoriseren het merendeel van deze applicaties als Trojans.

Browser-gebaseerde cryptominers gebruiken schadelijk JavaScript ingebed op een webpagina of delen ervan, met het doel om cryptocurrency te minen via de browsers van websitebezoekers. Deze methode heet ook wel **cryptojacking** en wordt sinds mid-2017 steeds populairder bij cybercriminelen. ESET detecteert de meeste cryptojackingscripts als potentieel ongewilde applicaties (PUA's).

Wist u dat?

De meeste illegale cryptominers proberen Monero of Ethereum te minen. Deze cryptocurrencies bieden cybercriminelen meerdere voordelen ten opzichte van de beter-bekende bitcoin: ze hebben een hoger niveau van transactie-anonimiteit en, belangrijker nog, kunnen gemined worden met reguliere CPU's en GPU's in plaats van dure en speciale hardware.

De schade die cryptomining kan veroorzaken

Door hun betere prestaties zijn zakelijke hardware en netwerken waardevollere doelwitten dan consumentenapparatuur. Ze beloven aanvallers hogere inkomsten in een korter tijdsbestek.

Ondanks dat illegale cryptomining een minder ernstige bedreiging lijkt dan meer invasieve aanvallen, moeten organisaties het risico niet onderschatten. Mining kaapt meestal een groot deel van de rekenkracht van hardware.

Dit resulteert in:

1. **verminderde prestaties**
2. **lagere productiviteit**
3. **schade aan de doelwitapparaten** omdat het energieverslindende mining-proces extra stress uitoefent op hardwarecomponenten, waardoor hun levensduur wordt verkort.
4. **cryptominers stellen kwetsbaarheden bloot in de houding van een organisatie ten opzichte van cybersecurity,** die potentieel kunnen leiden tot ergere inbreuken en verstoringen.

50% van de MSP'ers identificeert cryptomalware als één van de grootste beveiligingsuitdagingen waar zij via hun klanten mee in aanraking komen.

Bron: ESET poll onder 488 MSP-partners in 14 landen in juli 2019, via een online survey

Op Android-apparaten veroorzaakt extra belasting van de rekenkracht:

- Kortere levensduur van de batterij
- Merkbare temperatuurstijging van het apparaat
- Lagere apparaatproductiviteit
- In het ergste geval: fysieke schade door het "opzwellen" van de batterij

Houd uw IT-infrastructuur vrij van cryptominers

- Beveilig werkstations, servers en andere apparaten door **betrouwbare en meerlaagse beveiligingsoplossingen** te implementeren die in staat zijn om potentieel ongewenste (PUA) cryptomining-scripts en cryptomining-Trojans te detecteren.

- Implementeer **Intrusion Detection Software (IDS)** die helpt bij het identificeren van verdachte netwerkpatronen en -communicatie die mogelijk gelinkt zijn aan illegale cryptomining (bijv. geïnfecteerde domeinen, uitgaande verbindingen op typische mining-poorten zoals 3333, 4444 of 8333, etc.).

- **Verhoog het netwerkinzicht** door gebruik te maken van een remote beheerconsole om een beveiligingsbeleid op te leggen, de systeemstatus te monitoren en werkstations en servers te beveiligen.

- **Train alle medewerkers** (inclusief management en netwerkbeheerders) in het onderhouden van goede cyberhygiëne en het creëren en gebruiken van sterke wachtwoorden met multifactorauthenticatie. Hiermee verhoogt u de beveiliging van bedrijfssystemen als wachtwoorden worden gelekt of gekraakt.

- Volg **het principe van de minste rechten**. Alle gebruikers zouden een gebruikersaccount moeten hebben met zo min mogelijk machtigingen, zolang zij hiermee in staat zijn hun dagelijkse taken uit te voeren. Deze aanpak verlaagt het risico dat gebruikers en beheerders gemanipuleerd kunnen worden om cryptominers of andere schadelijke software te openen of installeren op een apparaat dat verbonden is met het bedrijfsnetwerk.

- Gebruik **applicatieregelaars** en beperk de hoeveelheid software die tegelijk mag draaien tot een minimum om de installatie van cryptominingmalware te voorkomen.

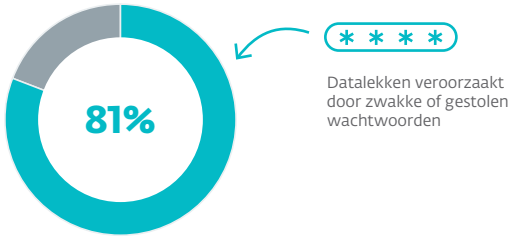
- Implementeer een **goed** update- en patchingbeleid om de kans dat een organisatie wordt gecompromitteerd via reeds bekende kwetsbaarheden significant te verlagen. Veel gevorderde cryptominers gebruiken bekende exploits, zoals EternalBlue, als voornaamste distributiemethode.

- **Monitor** bedrijfssystemen op **overmatig stroomgebruik** of andere afwijkingen in energieconsumptie die kunnen wijzen op illegale cryptomining-activiteiten.

4 Wachtwoordveiligheid
Wat staat er op het spel?

Het instellen van wachtwoorden is een basis-veiligheidsmaatregel, maar met de toenemende hoeveelheid en complexiteit wordt het steeds uitdagender om ze te beheren en veilig te gebruiken. Daarom zijn aanvullende beveiligingsoplossingen zoals multifactorauthenticatie nodig om de werking van wachtwoorden te versterken.

Bedrijven binnen het mkb zijn zeer aantrekkelijk voor cybercriminelen, omdat zij meer waardevolle data hebben dan consumenten, maar kwetsbaarder zijn dan enterprises, die grotere securitybudgetten hebben. Dit probleem wordt vergroot door het toenemende aantal organisaties dat 'slimme apparaten' in hun IT-infrastructuur integreert. Hoewel het Internet of Things (IoT) hen helpt om zakelijke activiteiten sneller en soepeler te laten verlopen, zijn deze apparaten vaak kwetsbaar en worden ze gebruikt met standaard admin-gebruikersnamen en -wachtwoorden. Dit vormt een risico dat kan leiden tot schadelijke gevolgen.



Volgens het Verizon 2017 Data Breach Investigation Report wordt **81% van alle datalekken veroorzaakt door zwakke of gestolen wachtwoorden.** Aangezien meer dan 5 miljard wachtwoorden online zijn gelekt, is standaard wachtwoordbeveiliging niet langer doeltreffend.

De consequenties van slechte wachtwoordveiligheid

De Europese Algemene Verordening Gegevensbescherming (AVG) stelt dat **organisaties van elke grootte ervoor moeten zorgen dat hun data veilig is** door "passende technische en organisatorische maatregelen" te implementeren. Als er een lek plaatsvindt en er alleen simpele, statische wachtwoorden in gebruik zijn, is het mogelijk dat er een fikse boete wordt uitgedeeld.

Manieren om uw wachtwoordveiligheid te vergroten

Implementeer een effectief wachtwoordbeleid. Medewerkers moeten getraind worden in het creëren van sterke wachtwoorden.

[8 stappen voor het creëren van sterke wachtwoorden]

IT-afdelingen moeten regels implementeren bij het instellen en handhaven van een zakelijk wachtwoordbeleid.

[6 basisregels voor een goed wachtwoordbeleid]

Gebruik multifactor-authenticatie (MFA) om gegevens beter te beschermen

[ESET Secure Authentication]

Nog sterkere beveiliging

Omdat mobiele apparaten vaak onderhevig zijn aan malware-aanvallen, gebruiken de meeste moderne MFA-oplossingen pushnotificaties, wat veiliger en gebruiksvriendelijker is, in plaats van SMS-verificatie. Om de veiligheid van het authenticatieproces nog meer te versterken kunnen organisaties **biometrie** inzetten — *iets dat de gebruiker is.*

OVERWIN
DE GROOTSTE BEVEILIGINGSUITDAGINGEN VOOR HET MKB

Pak ransomware aan, bestrijd social engineering, stop illegale cryptomining en versterk de veiligheid van wachtwoorden.

ESET Nederland
Trapezium 304, 3364 DL Sliedrecht

Ashley Schut
Solution Advisor MSP
ashley.schut@eset.nl
+31 (0)6 11 14 45 69
+31 (0)184 647 740

www.eset.com/nl

ESET CYBERSECURITY EXPERTS ON YOUR SIDE