ConXioN

The new style of IT

CISCO

De ultieme checklist:

Voorkom en bestrijd virussen en malware

De ultieme checklist voor de preventie en bestrijding van ransomwareaanvallen

Whitepaper

3 op de 4 bedrijven is slachtoffer van een vorm van **cybercriminaliteit**. De schadekost daarvan loopt op tot gemiddeld **78.000 EUR**. Veel bedrijven denken nog vaak dat dit hen niet kan of zal overkomen. Helaas is de werkelijkheid anders. Cybercriminaliteit wordt steeds **complexer**, **slimmer** en **aggressiever**. Een goede beveiliging is dus echt een must. Ransom of hacking bestrijden doe je door een goede **verdediging**. Daarom bescherm je beter je **volledige IT-omgeving** en dat op zowel webniveau, netwerkniveau als op niveau van je toestellen en inbox.

1 Maak back-ups van al jouw gegevens

Een van de krachtigste wapens tegen dataverlies, is tijdig een back-up te nemen van je data en applicaties. Zo een back-up maakt herstel - en sneller terug operationeel zijn - mogelijk. Hou die back-up best extern, los van je toestel of syteem. Maak ook tijdig een 'image' van je systeem.

2 Patchen, patchen, patchen

Wie verouderde software gebruikt, is een heel dankbare prooi voor ransomware-aanvallers. Die vinden heel makkelijk kwestbare punten waar ze geruisloos je netwerk binnen dringen. Niet enkel voor jou een gevaar, maar voor je hele netwerkomgeving. Zorg er dus voor dat je altijd tijdig en juist patcht. Zo verklein je de kans op aanvallen.

3 Informeer jouw gebruikers over aanvalsbronnen

De gebruiker, de mens, blijft de zwakste schakel in de beveiligingsketen. Social Engineering, een slimme vorm van oplichten, speelt in op de mens, zijn omgeving en karaktereigenschappen zoals vertrouwen.
Informeer jouw gebruikers over vaakgebruikte technieken en hoe ze zich beter kunnen beveiligen.

Maak een lijst met tips die ze kunnen gebruiken zoals:

1. Ken ik de afzender?
2. Is het écht nodig dat ik dat bestand of link volg?
3. Heb ik écht iets besteld bij dit bedrijf?

4 Bescherm jouw netwerk

De beste manier om jouw netwerk te beveiligen, is een 'gelaagde beveiliging'. Zo bescherm je jouw web-omgeving, jouw netwerkomgeving, je e-mailomgeving én je toestellen. Zo ben je op elke IT-laag zeker qua veiligheid.

5 Segmenteer de netwerktoegang

Netwerksegmentering beperkt de hoeveelheid 'resources' waar een aanvaller toegang toe kan krijgen.
Je deelt je netwerk dus best in met verschillende segmenten zoals specifieke bedrijfsgegevens of applicaties, type users, enzovoort. Zo rem je aanvallen af en krijgt de aanvaller niet tot alles toegang.

6 Hou je netwerkactiviteit goed in de gaten

Je kan geen bescherming bieden voor wat je niet kan zien. Je netwerkactiviteit zichtbaar maken lijkt een grote klus, maar het is wel van cruciaal belang. Zo zie je in één oogopslag wat er zoal gebeurt in je netwerk en data-center en kan je tijdig zones afsluiten waar nodig ingeval van een aanval.

7 Voorkom initiële infiltratie

Soms openen je gebruikers in alle onschuld toch een besmet bestand, e-mailbericht of website. Daardoor kan malware je omgeving en systeem binnendringen en infecteren. Doorgaans gebeurt infectie via e-mailbijlages of kwaadaardige downloadbestanden. Zet een policy op die een bepaalde bestandsdeling 'promoot' die je medewerkers en partners kennen, en die veilig is.

8 Beveilig jouw endpoints

BYOD (Bring Your Own Device) op de werkplek is stevig ingeburgerd. Deze tablets of smartphones zijn echter niet altijd volgens dezelfde veiligheidsregels afgestemd als die van je bedrijf. Kijk daarom naar een beleid dat ervoor zorgt dat ook via deze devices aanvallers geen kans krijgen je systeem aan te vallen. Via MDM (Mobile Device Management) heb je betere controle over alle toestellen die aanwezig zijn in netwerk en kan je ook de activiteit ervan grotendeels zichtbaar maken. Een bijhorend policyset per account is aan te raden, om de gebruikte toestellen in je netwerk toch voldoende veilig te maken.

9 Real-time bedreigingsinformatie verkrijgen

Als je een bedreiging proactief wil bestrijden, moet je je vijand kennen. Talos, een van de grootste private threat intelligence groups wereldwijd en devisie binnen Cisco, scant continu en in real-time alle mogelijke bedreigingen. De kennis daarvan delen ze met hun partners, die daardoor proactief kunnen optreden en de nodige maatregelen nemen. Je kan als bedrijf hun aangeboden informatie raadplegen en een potentiële aanval voorkomen.

10 Zeg NEE tegen losgeld

Hoewel veel bedrijven in de verleiding komen om losgeld te betalen om terug controle te krijgen over hun systeem, is dat de allerlaatste optie die je moet overwegen. Neem eerst contact op met de bevoegde autoriteiten en vraag hun advies.

Vertrouw op een expert

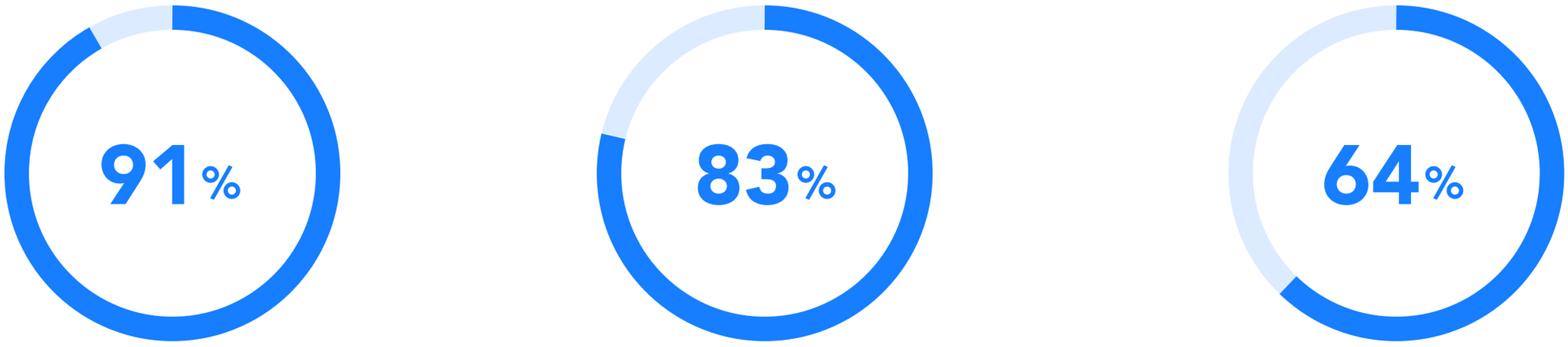
Met **ConXioN** kan je rekenen op een totaalpartner inzake security met een bewezen krachtige '**gelaagde beveiliging**'. Onze combinatie van beveiliging op web-, netwerk-, mail- én toestelniveau gecombineerd met proactieve monitoring zorgt voor de meest optimale beveiliging van jouw digitale werkplek en kantoor.

Onze **Security Experts** staan in dagelijks contact met onder meer Cisco Talos en scannen en patchen tijdig jouw systeem en toestellen. **Proactieve upgrades** voeren we uit zonder dat je hiervan hinder ondervindt tijdens het werken. Zo werk je in alle gemoedsrust en ben je zeker dat je systeem en toestellen altijd up-to-date en veilig zijn.

Managed Security Pack

3 op de 4 bedrijven is getroffen door cybercriminaliteit

Gemiddeld 35 cyberattack-cases per dag & schadekost cyberaanval **€ 78.000**



Managed Security Pack

Proactieve beveiliging, beheer en monitoring van alle toestellen

Gold

PACK

Geniet van optimale veiligheid via '**Layered Security**'. Aan de hand van diverse tools zoals Web Layer Security, E-mailsecurity, Anti-malware protection, Proactive monitoring & Patch Management

Populair

Platinum

PACK

Bovenop het MSP Gold pakket biedt MSP Platinum een geavanceerde bescherming op **besturingssysteem met encryptie** met daarbij een geavanceerd identiteits- en toegangsbeheer

Contacteer ons

vrijblijvend voor meer informatie of een offerte.

056/ 73 11 21

Hoogstraat 134, 8540 Deerlijk

www.conxion.be

info@conxion.be