Kwetsbaarheidsscan

Periodiek inzicht in de kwetsbaarheden van belangrijke IT-systemen

Kleine fouten met grote gevolgen
Een kleine fout in informatiebeveiliging is snel gemaakt. Vaak met grote gevolgen. Regelmatig liggen persoonlijke gegevens van gebruikers op straat. Veel ondernemers zijn zich niet bewust van de risico's voor hun organisatie.

Zwakke plekken
Naast het gebruik van onveilige wachtwoorden is een van de meest voorkomende oorzaken van cyberincidenten, dat cybercriminelen zwaktes in software gebruiken. Die zwaktes ontstaan, doordat bijvoorbeeld technische updates niet tijdig worden doorgevoerd. Ook wordt vaak vergeten om na het doorvoeren van nieuwe software-updates te controleren of belangrijke beveiligingsinstellingen nog goed staan.

Fouten herkennen
Het is daarom essentieel om periodiek uw IT-omgeving te scannen op niet-doorgevoerde updates en onveilige systeeminstellingen. De **kwetsbaarheidsscan van Baker Tilly** is een scan waarmee u de kwetsbaarheden van uw externe en interne IT-systemen in kaart kunt laten brengen. De resultaten van onze kwetsbaarheidsscan helpen u om tijdig bij te sturen op de zwakke plekken. Zo helpen wij uw omgeving veilig(er) te maken.

Betaalbare oplossing
Met de kwetsbaarheidsscan heeft u een betaalbare oplossing voor het periodiek scannen van uw IT-omgeving. U hoeft zelf niet te investeren in kostbare software.

‘Met een periodieke kwetsbaarheidsscan blijft u in control’

Periodieke kwetsbaarheidsscan
Wij zorgen met de kwetsbaarheidsscan voor inzicht op de kwetsbaarheden van uw externe maar ook interne systemen. Dit is een momentopname. Uw situatie verandert echter continu, bijvoorbeeld omdat u gaat werken met nieuwe software, interfaces en/of updates. Dagelijks komen er nieuwe kwetsbaarheden bij. Het is dan ook van belang om uw IT-omgeving periodiek te scannen. Wij adviseren de kwetsbaarheidsscan minimaal vier keer per jaar uit te voeren.

Systematische aanpak
Onze aanpak bestaat uit de volgende stappen:

Grip op risico’s geeft rust
De kwetsbaarheidsscan geeft u als (eind)verantwoordelijke:

- **periodiek meetbare resultaten,** omdat u na elke scan een helder overzicht ontvangt met de gesignaleerde kwetsbaarheden.
- **inzicht in hoeverre de getroffen maatregelen het gewenste effect** hebben om zo uw informatiebeveiliging verder te kunnen optimaliseren.
- **minder beveiligingsrisico’s**, omdat de kans op het verliezen of gijzelen van klant- en bedrijfsgegevens kleiner wordt.

Stap 1: richten	Bespreken van de risico’s die voor uw IT-omgeving van belang zijn en de scaninterval bepalen (van 4 tot 12 maal per jaar).
Stap 2: inrichten	Scanomgeving instellen op de gewenste assets/applicaties en op de afgesproken momenten.
Stap 3: verrichten	Scanning uitvoeren, rapporteren (minimaal technisch en indien gewenst een managementsamenvatting) en herhalen op de besproken momenten.
Stap 4: bespreken	Trendanalyse opstellen en beoordelen met een bespreking van de mogelijk te nemen maatregelen voor continue verbetering.

Waarom Baker Tilly
Als accountant kennen wij uw organisatie en denken we mee over de beheersing van risico’s. Naast de kwetsbaarheidsscan heeft Baker Tilly ook gespecialiseerde medewerkers die voor u klaar staan als u bijvoorbeeld passende AVG-maatregelen of een standaard als ISO 27001 / NEN 7510 wilt implementeren. Onze medewerkers adviseren over een goede implementatie van deze normen, inclusief het aantoonbaar maken van de werking van uw beheersmaatregelen.

Wilt u grip op de zwakke plekken in uw IT-omgeving?
Onze specialisten vertellen u graag meer over hoe u grip kunt krijgen op de kwetsbaarheden. Zij lichten graag toe wat de kwetsbaarheidsscan uw organisatie kan opleveren.

Neem voor meer informatie contact op met:

- **Wilco Brouwers, senior manager IT Advisory**
  w.brouwers@bakertilly.nl | 06 – 12 82 64 62
- **Remco Jansen, consultant IT Advisory**
  remco.jansen@bakertilly.nl | 06 – 25 73 15 86