Uitkomsten Cybersecurity Health Check:

Digitale weerbaarheid kleine en middelgrote organisaties nog niet op niveau

Baker Tilly onderzoekt cybersecurity

Een kleine 200 klanten van Baker Tilly, kleine en middelgrote Nederlandse organisaties, uit verschillende sectoren vulden de Cybersecurity Health Check van de Nederlandse Beroepsorganisatie van Accountants (NBA) in. Baker Tilly analyseerde hun antwoorden over cyberveiligheid en komt tot de conclusie dat deze organisaties nog veel kunnen winnen in het tijdig detecteren van zwaktes in de eigen beveiliging en in het voorbereiden op hoe te reageren bij een cyberincident.

Bewustwording cybersecurity vergroten

De organisaties beoordeelden zichzelf op cyberveiligheid, aan de hand van een vragenlijst. Baker Tilly voerde de analyse uit om met kleine en middelgrote organisaties het gesprek over cybersecurity aan te gaan. Het doel van de Cybersecurity Health Check van de NBA is om in Nederland de bewustwording op dit dossier te vergroten.

Uitkomsten Cybersecurity Health Check

Uit de analyse van de respons op de Cybersecurity Health Check naar cyberveiligheid blijkt dat digitale weerbaarheid bij kleine en middelgrote organisaties steeds meer aandacht heeft, maar nog niet op het benodigde niveau is. Een aantal positieve èn minder positieve bevindingen springen in het oog.

Meest opvallende bevindingen
Onderstaande bevindingen laten zien welke aspecten van cybersecurity de nodige aandacht vereisen. Hier hebben Nederlandse organisaties echt nog iets te doen:

- **Bijna 60% test beveiliging van gevoelige applicaties niet regelmatig**
  Slechts 41% van de organisaties voert periodiek penetratietesten uit op gevoelige applicaties en applicaties die benaderbaar zijn via internet. Met deze testen kunnen organisaties toetsen of de beveiliging afdoende is. Opvallend is dat met name de deelnemende zorginstellingen, handel- en productiebedrijven en bouwbedrijven laag scoren (slechts 20% toetst beveiliging periodiek).
- **Bijna 50% voert kwetsbaarheidsscans niet (regelmatig) uit**
  Een kwetsbaarheidsscan toetst of tijdig de benodigde patches (lees: beveiligingsupdates voor software) worden doorgevoerd in de systeemomgeving. Slechts iets meer dan de helft van de deelnemende organisaties voert regelmatig een kwetsbaarheidsscan uit.
- **Slechts 30% van mkb-bedrijven checkt leveranciers op cybersecurity**
  Veel deelnemende organisaties zijn (groten)deels afhankelijk van partners en leveranciers voor hun operatie. Slechts de helft van de deelnemende organisaties geeft aan bij leveranciers, service providers en partners te informeren in welke mate zij cyberrisico's afdekken en of zij hier verantwoording over kunnen afleggen. Mkb-bedrijven trekken hier het gemiddelde nog verder naar beneden. Slechts ongeveer 30% van de mkb-bedrijven geeft aan dit te doen.

Respondenten per sector:
48 gemeenten | 42 handel- of productiebedrijven
20 bouwbedrijven | 17 bedrijven in zakelijke dienstverlening
15 zorginstellingen | 14 woningcorporaties | 34 overig.

Organisaties op goede weg
Daarnaast toont de analyse aan dat op een aantal andere onderwerpen de deelnemende organisaties op de goede weg zijn:

- **Cybersecurity op agenda van directie**
  Een grote meerderheid (84%) heeft de verantwoordelijkheid voor cybersecurity inmiddels op directieniveau belegd. Bij ruim 75% van de deelnemende organisaties is ook iemand uitvoerend verantwoordelijk gemaakt voor cybersecurity. De meeste organisatie (63%) hebben een cybersecuritybeleid, het onderwerp wordt periodiek besproken binnen de directie (62%) en de belangrijkste risico's en dreigingen zijn (in ieder geval informeel) in kaart gebracht (61%).
- **Back-up procedures op orde**
  Bij veruit de meeste organisaties zijn de back-up procedures op orde en worden de back-upvoorzieningen zodanig ingericht dat getroffen systemen snel en efficiënt hersteld kunnen worden. Niet beschikbaarheid is ook het cyberrisico dat het meeste wordt genoemd in onze gesprekken over de check, zeker bij de mkb-bedrijven die de check hebben ingevuld.
- **Endpoint security effectief ingezet**
  De meeste organisaties hebben inmiddels effectieve maatregelen in gebruik voor endpoint security (beveiliging van werkplek en telefoon). Een aantal deelnemende zorginstellingen blijft nog wel achter op het treffen van effectieve maatregelen voor endpoint security, wat toch opvallend te noemen is.
- **Twee-factor authenticatie op externe toegang**
  Meer dan de helft (55%) van de organisaties maakt gebruik van twee-factor-authenticatie om de externe toegang tot hun netwerk en/of gegevens te beveiligen. Het zorgelijke is echter, dat dit betekent dat ook een groot deel van de organisaties twee-factor authenticatie nog helemaal niet inzet.

Vijf aspecten van cybersecurity

Baker Tilly gebruikt de Cybersecurity Health Check om organisaties inzicht te geven in de staat van cyberbeveiliging binnen hun organisatie. De analyses vormen de basis voor het identificeren van de belangrijkste cyberrisico's.

Vijf aspecten cybersecurity
De check bestaat uit vijf aspecten van cybersecurity waarop organisaties zichzelf beoordelen. Wanneer geen adequate maatregelen zijn genomen op een van deze vijf aspecten, ontstaan risico's op het gebied van cybersecurity.

1. Identificatie
Organiseren van het onderwerp en identificatie van de relevante cyberrisico's voor de organisatie.
Risico: dreigingen worden niet onderkend, het is onduidelijk welke maatregelen getroffen moeten worden.

2. Bescherming
Het treffen van preventieve beveiligingsmaatregelen met als doel het voorkomen van cyber incidenten.
Risico: aanvallers krijgen voet aan de grond in de organisatie.

3. Detectie
Het treffen van detectieve beveiligingsmaatregelen om zwakke plekken in de beveiliging op de sporen en om tijdig cyber incidenten te detecteren.
Risico: incidenten worden niet tijdig opgemerkt.

4. Reactie
Het voorbereiden op hoe te reageren op een potentieel cyber incident.
Risico: impact van cyberincidenten zijn groter dan noodzakelijk.

5. Herstel
Het verzekeren dat bij (aanzienlijke) schade als gevolg van een cyber incident de organisatie zo spoedig mogelijk weer de normale gang van zaken kan hervatten.
Risico: impact van cyberincidenten zijn groter dan noodzakelijk.

Aandachtsgebieden: detectie en reactie
Op de aspecten detectie en reactie scoren de organisaties uit het onderzoek lager, in vergelijking met de andere aspecten van cybersecurity. Juist detectie en reactie geven inzicht in waar uw organisatie daadwerkelijk staat op het gebied van cybersecurity. Óf en hoe u zich voorbereidt op een mogelijk incident.

Een aantal tips om cybersecurity op het gewenste niveau te krijgen:

- Introduceer periodieke kwetsbaarheidsscans op uw externe en interne digitale assets. Voer deze scans minimaal tweemaal per jaar uit en maak dit proces onderdeel van uw standaard IT-processen;
- Introduceer periodieke beveiligingstesten in uw organisatie en uw belangrijkste digitale assets. Laat de frequentie afhangen van het risicoprofiel van uw organisatie;
- Breng in kaart welke leveranciers kunnen leiden tot een cyberrisico voor uw organisatie. Bevraag die leveranciers over hun digitale weerbaarheid. Vraag een auditrapport indien mogelijk over hun digitale weerbaarheid;
- Test of u daadwerkelijk uw bedrijfsvoering (snel) kunt doorzetten als zich een cyberincident voordoet, bijvoorbeeld als al uw werkplekken zijn besmet met ransomware. Mocht deze test u toch onvoldoende comfort opleveren, pak daar dan direct op door.

Meer weten?
Neem dan contact op met de cybersecurity specialisten Baker Tilly:
Rob Havermans, director IT Advisory
r.havermans@bakertilly.nl | 06 11 98 67 79

Baker Tilly
Fascinatio Boulevard 200-300
3065 WB Rotterdam • The Netherlands
T +31 (0) 10 253 59 00
www.bakertilly.nl

bakertilly