De financiële risico’s van een slechte cyberweerbaarheid

De financiële risico's van een slechte cyberweerbaarheid

Het idee dat alleen grote bedrijven aantrekkelijk zijn voor cybercriminelen is een misverstand. Uit onderzoek blijkt dat 1 op de 5 ondernemers, groot en klein, jaarlijks te maken krijgt met een cyberincident. Met antivirussoftware en een firewall kun je veel ellende voorkomen. Maar om alle malware, phishing en ransomware buiten de deur te houden, moet je je cyberweerbaarheid kritisch onder de loep nemen.

Top 5 meest voorkomende kwetsbaarheden

Uit onderzoek van EZK in Beeld van het Ministerie van Economische Zaken en Klimaat komt naar voren dat bedrijven vooral kwetsbaar zijn als gevolg van:

- Onzorgvuldig gebruik van procedures en wachtwoorden
- Slecht beveiligde routers en firewalls
- Onbeveiligde SSL-certificaten of webstatistieken
- Achterstallig onderhoud aan mail- en webservers
- Gehackte servers en websites

De financiële risico's

Hoe groot de rol van hardware en software in je onderneming ook is, cybercrime heeft altijd financiële consequenties.

1. **Kosten voor losgeld**
   Ransomware is malware die systemen, netwerken of data achter slot en grendel zet. In ruil voor losgeld (vaak cryptocurrency) beloven criminelen de zaken weer vrij te geven. Maak je het geld over dan weet je niet zeker of je ook daadwerkelijk weer toegang krijgt. Bovendien laat het zien dat ransomware loont.

2. **Verlies van klanten**
   Zodra internetcriminelen toegang krijgen tot jouw digitale systemen en data kunnen ze ook bij eventuele klantgegevens. Je zult je klanten van dergelijke hacks op de hoogte moeten brengen. Dat kan voor jouw klant aanleiding zijn om over te stappen naar de concurrent.

3. Imagoschade
Vertrouwen komt te voet en gaat te paard. Cybercrime in het algemeen maar bijvoorbeeld identiteitsfraude kan grote invloed hebben op je zorgvuldig opgebouwde naam en goede imago.

4. Kosten intellectuele eigendom
Intellectuele eigendommen vertegenwoordigen een aanzienlijke waarde. Diefstal door hackers kan grote economische gevolgen hebben voor het bedrijf. Denk bijvoorbeeld aan de kosten voor juridische ondersteuning.

> “Preventief aandacht voor je cyberweerbaarheid loont

5. Personeelskosten
Afhankelijk van de grote van je bedrijf, het delict en de omvang van de schade moet je meer of minder mankracht vrijmaken voor onderzoek naar de oorzaak en herstel. Zowel intern als extern maak je hierdoor extra kosten.

6. Herzien van je digitale veiligheidsbeleid
Als de productie weer is opgestart en de schade is hersteld, is het tijd om eens kritisch te kijken naar je cyberweerbaarheid. Je kwetsbaarheid mag immers nu op orde zijn, maar hoe is dat in de toekomst.

7. Poliskosten cyberverzekering
Als je je digitale veiligheidsbeleid onder de loep neemt kun je ook overwegen om een cyberverzekering af te sluiten. Veel verzekeraars vergoeden niet alleen de schade, maar ondersteunen je ook bij het voorkomen van cybercriminaliteit.

8. Omzetverlies
Imagoschade en verlies aan klanten lijden indirect tot omzetverlies. Ook direct kan een cyberaanval gevolgen hebben voor je inkomsten. Denk bijvoorbeeld een DDos-aanval waardoor je website of webshop niet meer bereikbaar is voor klanten. Uit onderzoek van verzekeraar Hiscox in 2020 onder bedrijven die te maken hebben gehad met cyberincidenten en -lekken zijn de mediane kosten in Nederland gestegen naar 74.000 dollar. Een stijging met 12.000 dollar ten opzichte van het jaar ervoor.

Breng risico's in kaart

Preventief aandacht voor je cyberweerbaarheid loont. Met de Cyberweerbaarheid Scan van DataLOQ brengen we alle digitale risico's in kaart. Tijdens de scan lichten we 6 domeinen door. Naast de organisatie kijken we ook naar de techniek, het onderhoud, de huisvesting, de privacy en de continuïteit. We stellen je in staat om sneller te anticiperen op dreigingen en geven je bedrijf tools in handen om te herstellen van de gevolgen.

5 tips om je organisatie cyberweerbaar te maken:

1. Duidelijke richtlijnen opstellen voor informatieveiligheid en privacybescherming. Een goede weerbaarheid begint bij duidelijke richtlijnen voor jouw organisatie.
2. Train je medewerkers en creëer bewustzijn in je bedrijf. Dat betekent bijvoorbeeld dat wachtwoorden niet op het prikbord hangen en altijd tweestapsverificatie gebruiken om in te loggen.
3. Zorg voor duidelijke rollen. Leg vast wie toegang heeft tot welke bestanden.
4. Installeer, het liefst automatisch, updates voor je besturingssystemen, programma's en beveiligingssoftware. Naast up-to-date software voor laptops en desktops geldt dat natuurlijk ook voor randapparatuur en smartphones.
5. Maak regelmatig back-ups van je data. Gebruik hiervoor verschillende systemen, zowel binnen als buiten (cloud) je eigen bedrijf.

Boek de Cyberweerbaarheid Scan met korting

Wil je inventariseren of de databeveiliging in jouw organisatie nu voldoet en praktische handvaten krijgen voor verbetering, dan is een Cyberweerbaarheid Scan verstandig. DataLOQ biedt jou graag de mogelijkheid om een scan uit te voeren. Samen met één van onze consultants doorloop je een vragenlijst om de cyberweerbaarheid van jouw bedrijf in kaart te brengen. Met het rapport krijg je inzicht in de dataveiligheid van je organisatie en geven we je onafhankelijk advies over de verbeterslagen die je kunt maken.

Er loopt een tijdelijke kortingsactie van € 100,- waardoor je voor deze scan slechts € 395 betaalt.

Boek hier de Cyberweerbaarheid Scan

DataLOQ
DataLOQ.nl
info@dataloq.nl