GROTE KLOOF BIJ NEDERLANDSE ORGANISATIES

tussen perceptie eigen digitale weerbaarheid en realiteit

In juli 2020 is in opdracht van Solvinity een onderzoek uitgevoerd door PanelWizard onder ruim 500 Nederlandse IT-verantwoordelijken bij bedrijven met 200 medewerkers en meer, om in beeld te brengen hoe Nederlandse organisaties aankijken tegen hun eigen digitale weerbaarheid. Daaruit blijkt dat het vertrouwen in de eigen weerbaarheid onder deze groep best groot is. Maar er zijn diverse aanwijzingen in het onderzoek die erop wijzen dat IT de eigen weerbaarheid vaak nog te rooskleurig inschat.

PERCEPTIE

88%

88% van de Nederlandse IT-verantwoordelijken zegt de beveiliging van de eigen organisatie onder controle te hebben

70%

70% denkt prima zelfstandig weerstand te kunnen bieden aan cybercrime

REALITEIT

1 Patches & updates

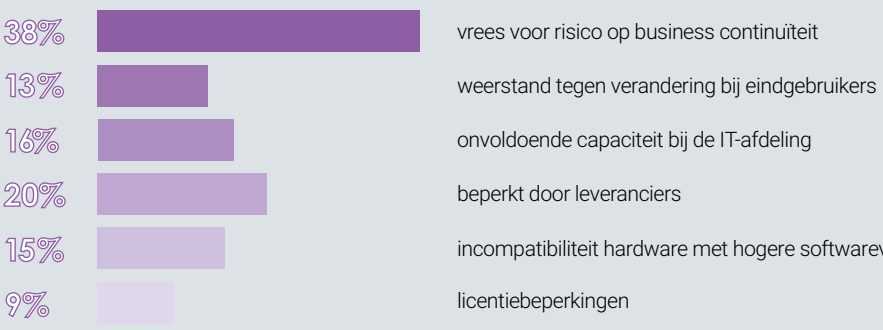
80% installeert niet alle patches en updates

80%

51%

51% laat weken of maanden voorbij gaan voordat patches en updates worden geïnstalleerd

Redenen om patches en updates soms niet te installeren



2 Shadow IT

63%

63% scant niet actief op software, hardware of diensten waarvan bekend is dat ze niet veilig zijn

51%

51% geeft toe niet goed op de hoogte te zijn van de eigen kwetsbaarheid, of daar in elk geval geen gerichte maatregelen op te hebben genomen

3 Security Awareness

48%

met IT in eigen beheer besteedt onvoldoende aandacht aan het informeren van medewerkers hoe veilig om te gaan met IT

40%

is niet bekend met hardening

OUTSOURCING

Een goed cybersecuritybeleid begint bij inzicht in je eigen kwetsbaarheid. Uit het onderzoek blijkt dat veel IT-afdelingen kampen met hoge werkdruk en een tekort aan goed opgeleid personeel, én dat IT-outsourcing de weerbaarheid van organisaties kan verhogen. Een Secure Managed Service Provider voert bewust een op security gericht beleid.

Meer weten?
Download het volledige rapport op **solvinity.com**

Solvinity
Secure Managed IT Services