SECURITY

‘KLASSIEKE CYBERSECURITY VOLDOET NIET IN DE CLOUD’

René van Buuren,
directeur Cybersecurity bij Thales Nederland

Na jaren van aarzeling is eindelijk de kogel door de kerk. Bedrijven omarmen de cloud. Dat het veiliger is om gegevens in de cloud dan in eigen beheer op te slaan, dringt inmiddels tot bedrijven door, blijkt in een gesprek met directeur Cybersecurity René van Buuren bij Thales. “Wel vraagt de overstap naar de cloud om investeringen in andere en nieuwe vormen van security.”

door: de redactie

In haar gepubliceerde jaarlijkse Data Threat Report roept Thales Cybersecurity op tot bewustwording over de risico’s van cloudomgevingen. “De opmars van cloud computing brengt verschillende security-vraagstukken met zich mee. Steeds meer gegevens worden online opgeslagen en gedeeld. Dit maakt ze toegankelijker, maar niet veiliger”, zegt directeur Cybersecurity René van Buuren bij Thales Nederland. “Juist het gebruik van een online omgeving vraagt om een herbezinning van het security-beleid van ondernemingen.”

Verwachtingen vs. realiteit

Uit het rapport komt onder meer naar voren dat bijna twee derde, 63 procent, van de ondervraagde ondernemingen die nieuwe technologie implementeren, niet eerst goed naar de beveiliging daarvan kijkt. Bij cloud computing komt dit vooral doordat bedrijven ervan uitgaan dat de beveiliging van cloudcentra zo goed op orde is, dat er geen aanvullende maatregelen hoeven te worden genomen. Het gevolg is helaas dat zij niet de garantie krijgen dat hun gegevens goed beschermd zijn.

Van Buuren adviseert bedrijven hun verwachtingen te controleren en naar zowel de beveiliging van de cloud providers als de eigen beveiligingsmaatregelen te kijken. “Welke beveiliging biedt een cloud provider precies? Klopt dat met de verwachtingen? Hebben eindgebruikers onder meer zeggenschap over log-gegevens? Loggegevens worden door veel cloud providers niet zomaar (en zeker niet gratis) afgegeven, maar ze zijn wel nodig voor monitoring en detectie. Het is dus belangrijk te bekijken of de diensten van de cloud provider aansluiten op de security wensen die organisaties hebben.”

Zwakke schakel

Van Buuren geeft aan dat bij een security check ook goed naar het eigen personeel moet worden gekeken. Uit het rapport blijkt dat 58 procent van de ondervraagde bedrijven hun personeel als mogelijke kwetsbaarheid ziet. Zwakke wachtwoorden, onoordeelkundig gebruik en identiteitsdiefstal maakt dat cybercriminelen standaard security-maatregelen kunnen omzeilen en toegang kunnen krijgen tot gevoelige gegevens. “Gezien de belangen die er spelen, moet ervan worden uitgaan dat criminelen een manier zullen zoeken én vinden om toegang te krijgen tot gegevens”, aldus Van Buuren. Zo neemt identiteitsdiefstal via phishing de laatste jaren toe. “Als dat lukt, valt de bodem weg onder alle klassieke beveiligingsmethoden.”

Klassieke beveiligingsmethoden zijn er voornamelijk op gericht aanvallers door protectie buiten de deur te houden. Maar als aanvallers eenmaal binnen zijn, vaak door menselijke fouten, ligt de informatie voor het oprapen. Alleen protectie is dus onvoldoende als bescherming tegen dreigingen van buitenaf. Detectie, het opsporen van verdacht verkeer binnen organisaties, is onmisbaar.

Investeren in detectie is een belangrijke aanvulling op security binnen cloudomgevingen en onmisbaar in de cyberveiligheidsstrategie van bedrijven. “Het vertrouwen van de markt in de veiligheid van de eigen organisatie is cruciaal. Dat vertrouwen kunnen bedrijven alleen behouden als ze kunnen aantonen dat ze weten wat er werkelijk gebeurt met de gegevens die ze gebruiken.” «