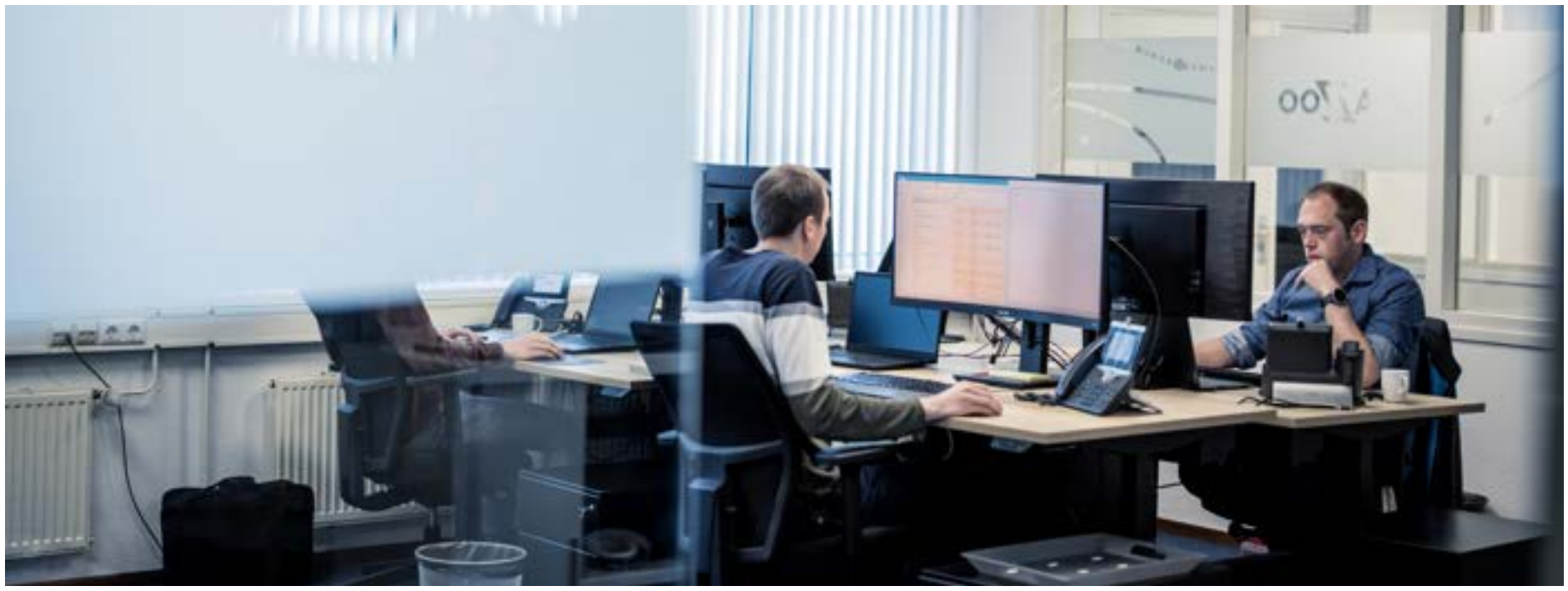

Wie de sleutel heeft, hoeft niets te forceren

Traditionele beveiligingsmaatregelen zoals firewalls en antivirus volstaan niet langer als enige verdedigingslaag. Organisaties investeerden jarenlang in het versterken van hun digitale buitenmuur. Maar criminelen passen zich aan. In plaats van muren te doorbreken, stelen ze sleutels. Digitale identiteiten, zoals de inloggegevens van medewerkers, systemen en externe partijen, zijn uitgegroeid tot het primaire doelwit van cyberaanvallen.

Gert-Jan de Boer,
IT security expert en netwerkarchitect,
aaZoo B.V.

Dat een aanvaller kan binnenkomen, staat bijna vast. Het gaat erom dat organisaties het merken wanneer iemand met een gestolen identiteit opereert binnen hun omgeving. Gert-Jan de Boer, IT security expert en netwerkarchitect bij aaZoo B.V., legt uit: “In 100% van de cyberaanvallen is een vorm van identiteit betrokken. Elke aanval manifesteert zich uiteindelijk als een vorm van toegang binnen systemen. Wie identiteiten niet monitort, accepteert een fundamentele blinde vlek in zijn risicobeheersing.”

aaZoo adviseert organisaties, van middelgrote ondernemingen tot corporates met vijftienduizend medewerkers, over het inrichten van veilige IT-omgevingen vanuit een zero trust-benadering. Die benadering gaat uit van één principe: vertrouw niets en niemand, en verifieer continu identiteit, apparaat en gedrag.

Nederland scoort internationaal redelijk op het gebied van cybersecurity, tussen de zes en zeven op een schaal van tien, maar het midden- en kleinbedrijf blijft achter. “Veel organisaties hebben nog geen compleet beeld van hun cybersecurityomgeving. Ze nemen vooral preventieve maatregelen, maar aan de inzichtkant en monitoring ontbreekt nog heel veel”, aldus De Boer. Die blinde vlek heeft consequenties. Als een medewerker onbewust zijn inloggegevens prijsgeeft via een phishingmail, kan een aanvaller ongemerkt via legitieme toegang het netwerk betreden.

Het onderschatte probleem van identity sprawl

Een van de meest onderschatte risico’s is ‘identity sprawl’, de wildgroei aan digitale identiteiten verspreid over tientallen systemen en applicaties. Veel organisaties denken dat ze hun identiteitsbeheer op orde hebben omdat ze een centrale omgeving als Microsoft Active Directory of Entra ID gebruiken. Maar de realiteit is complexer. “Door de opkomst van SaaS-applicaties en tooling die eigen identiteitsbronnen gebruiken, hebben veel organisaties identiteitsbronnen aan elkaar gekoppeld, maar verliezen ze daarmee juist het centrale overzicht en de controle. Accounts worden soms aangemaakt maar nooit verwijderd, multifactorauthenticatie (MFA) wordt niet overal ingeschakeld en service-accounts worden niet gemonitord”, legt De Boer uit.

Een praktijkvoorbeeld maakt het tastbaar. aaZoo ondersteunt een containeroverslagbedrijf met managed detection en response. Daarbij werd ontdekt dat negentig procent van de externe gebruikers met toegang tot bedrijfssystemen nooit inlogden. Die slapende accounts hadden desondanks volledige autorisaties. “Op het moment dat je dat soort dingen kunt zien, kun je ze ook aanpakken. Wat je niet ziet, kun je niet beschermen.” Slapende accounts zijn voor aanvallers aantrekkelijke doelwitten: weinig activiteit betekent weinig monitoring, en dus weinig kans op detectie.

> *In 100% van de aanvallen is er een identiteit betrokken*

Multifactorauthenticatie is geen eindpunt

Een veelgemaakte aanname is dat MFA het beveiligingsprobleem oplost. “Veel organisaties denken dat als ze multifactorauthenticatie hebben ingeregeld, het geregeld is. Maar ze weten niet zeker of het op alle accounts is ingeschakeld, of hoeveel mensen het al geactiveerd hebben”, zegt De Boer. “Bovendien treedt er bij medewerkers vermoeidheid op. Wie tientallen keren per dag een goedkeuringsverzoek op zijn telefoon krijgt, klikt uit automatisme op akkoord, ook als het verzoek van een onbekende locatie komt. Daarnaast zien we een sterke toename van aanvallen waarbij aanvallers hun eigen apparaat registreren als vertrouwde MFA-factor, waardoor ze blijvende toegang krijgen zonder dat de gebruiker dit merkt.”

De oplossing ligt in het combineren van drie pijlers: monitoring van endpoints, netwerkverkeer en identiteiten. “Door die drie te combineren heb je een volledig overzicht.” aaZoo zet hiervoor oplossingen in die integreren met bestaande identiteitsbronnen en continu gedrag monitoren. Het systeem signaleert afwijkingen, identificeert inactieve gebruikers, controleert of MFA actief is en beoordeelt of inlogpogingen afkomstig zijn van vertrouwde locaties en apparaten. Denk aan een intelligente firewall, maar gericht op identiteiten.

Verantwoordelijkheid ligt bij de organisatie

Wanneer identiteitsgegevens worden misbruikt, wijzen organisaties soms naar de medewerker zelf. De Boer noemt dat ‘victimblaming’. “De kwaliteit van phishingmails is enorm vooruitgegaan. Wij trappen er zelf ook regelmatig in. Je moet de scope beperken, zodat je een lek snel in de gaten hebt en de schade beperkt blijft.” Bewustwordingstrainingen alleen zijn onvoldoende. Technische maatregelen en continue monitoring zijn geen luxe, maar een noodzakelijke basis.

Het goede nieuws is dat de drempel lager is dan veel organisaties denken. Implementatie begint met inzicht: een audit van bestaande identiteiten, gevolgd door continue monitoring op gedrag en toegangspatronen. “Het is een koppeling die je legt of een scan die je uitvoert op je bestaande systeem. De gebruiker merkt er niets van, maar je krijgt wel heel veel zaken onder controle.” Wie identiteiten serieus neemt, houdt de regie over zijn beveiliging. En dat begint met zien wat er al jarenlang onzichtbaar bleef.