

Firewall allein reicht nicht mehr

24.08.2026, 08:34 | Handel, Wirtschaft, Finanzen, Banken & Versicherungen

Pressemitteilung von: *Validato*



Firewall allein reicht nicht mehr

Weshalb Unternehmen mit kritischen Systemzugängen heute nicht nur Technik, sondern auch Personenrisiken absichern müssen.

Investitionen in Firewalls, Endpoint-Detection und Zero-Trust-Netzwerke gehören für deutsche Industrie- und IT-Unternehmen längst zum Standard. Trotzdem waren laut Bitkom-Studie „Wirtschaftsschutz 2025“ 87 Prozent der deutschen Unternehmen im vergangenen Jahr von Datendiebstahl, Spionage oder Sabotage betroffen. Für Validato, Schweizer Anbieter für Background-Checks und Human Risk Management, liegt darin ein deutliches Signal: Technische Abwehr und Personalrisiko-Management müssen zusammengedacht werden.

Was Firewalls tatsächlich abdecken

Netzwerksicherheit, Endpoint-Schutz und Intrusion-Detection zielen auf unautorisierten Zugriff von aussen. Sie erkennen Angriffe an der Systemgrenze – aber nicht, ob eine Person mit gültigen Zugangsdaten diese Grenze von innen überschreitet. Selbst Systeme zur Anomalieerkennung stossen an Grenzen, wenn sich ein Zugriffsmuster kaum von normalem Verhalten unterscheidet. Nach Einschätzung von Validato entsteht dadurch ein blinder Fleck genau dort, wo der potenzielle Schaden am grössten ist.

Kritische Systemzugänge als eigene Angriffsfläche

Administratoren, Entwicklerinnen und IT-Dienstleister mit privilegierten Rechten stellen nach Einschätzung von Validato eine Angriffsfläche dar, die von klassischer Netzwerksicherheit kaum erfasst wird, weil ihr Zugriff technisch legitim ist. Das gilt nach Beobachtung von Validato besonders für Rollen mit Wartungszugriff auf Produktionsanlagen oder zentrale Datenbanken. Ein einzelner kompromittierter oder unzuverlässiger Zugang kann hier weitreichendere Folgen haben als ein erfolgreicher externer Angriffsversuch.

Die Lücke zwischen Zero Trust und Praxis

Zero-Trust-Architekturen verifizieren Geräte, Identitäten und Netzwerkverbindungen kontinuierlich. Nach Beobachtung von Validato bleibt die Frage, wer diese Identität überhaupt erhalten hat und ob sie vertrauenswürdig ist, in vielen

Umsetzungen unterbelichtet. In der Praxis wird eine digitale Identität häufig einmalig beim Onboarding angelegt und danach kaum mehr hinterfragt. Validato sieht hier eine Parallele zur Personalebene: Auch eine einmal geprüfte Person bleibt nicht automatisch dauerhaft vertrauenswürdig.

Personenrisiko als zweite Verteidigungslinie

Background Checks und Human Risk Management ergänzen technische Massnahmen, indem sie bereits vor der Vergabe von Zugriffsrechten ansetzen – bei Neueinstellungen ebenso wie bei bestehenden Mitarbeitenden mit wachsender Verantwortung. Das betrifft nicht nur neue Mitarbeitende, sondern auch bestehendes Personal, das im Zuge einer Beförderung oder Versetzung neue Zugriffsrechte erhält. Validato empfiehlt, solche Übergänge als eigenen Prüfanlass zu behandeln, nicht nur den Zeitpunkt der Ersteinstellung.

Praxisempfehlung: Zugriffsrechte und Prüftiefe koppeln

Validato empfiehlt, die Prüftiefe eines Background Checks an die Systemrechte einer Position zu koppeln: Wer weitreichenden Zugriff auf sicherheitsrelevante Systeme erhält, sollte einer entsprechend vertieften und dokumentierten Prüfung unterliegen. Ein IT-Systemverantwortlicher mit Zugriff auf Kernsysteme benötigt demnach eine andere Prüftiefe als eine Position ohne administrative Rechte. Diese Zuordnung lässt sich laut Validato einmalig für jede Rollenkategorie festlegen und danach automatisiert anwenden.

Validato: Screening als Ergänzung zur technischen Sicherheit

Validato bietet dazu 18 einzeln wählbare Screening-Module auf einer ISO-27001-zertifizierten Plattform mit Schweizer Serverstandort. Unternehmen buchen dabei ausschliesslich die für eine Position tatsächlich benötigten Module, ohne Abonnementbindung oder Mindestabnahme – Ergebnisse liegen für die meisten Module innerhalb weniger Minuten vor. „Eine Firewall fragt nicht, wer am anderen Ende sitzt – genau das muss die Personalrisikoprüfung leisten“, so Reto Marti - Managing Partner von Validato. Die Plattform lässt sich sowohl für neu zu besetzende Positionen als auch für bestehende Mitarbeitende mit wachsendem Zugriff nutzen. Sicherheitsverantwortliche erhalten so laut Validato ein Werkzeug, das technische und personelle Massnahmen in einem gemeinsamen Prozess abbildet.

Validato AG

Claridenstrasse 34
8002 Zürich
Schweiz

RetoMarti (Managing Partner)

+41 44 515 77 77

reto.marti@validato.com

validato.com/de-de

Portrait

Die Validato AG mit Sitz in Zürich entwickelt und betreibt eine konfigurierbare Background-Screening- und Human-Risk-Management-Plattform mit Fokus auf den DACH-Markt. Über 18 Module deckt Validato den gesamten Lifecycle ab — von Pre-Employment-Screening über In-Employment- und Re-Screening bis hin zu Third-Party-Screening, Lieferantenprüfung und Due Diligence. Die Plattform arbeitet mit einem Pay-per-Use-Modell, ist vollständig DSGVO-

und nDSG-konform und auf die Rahmenwerke NIS2, DORA, KRITIS-Dachgesetz, DIN SPEC 14027:2026-04, BSI C5:2026, AI Act, LkSG sowie ISO 27001 ausgerichtet.

News-ID: 1321218 • Views: 160 (Stand: 13.10.2026)

Link zur Pressemitteilung:

<https://www.openpr.de/news/1321218/Firewall-allein-reicht-nicht-mehr.html>