# Industriespionage beginnt nicht immer mit einem Hackerangriff

28.08.2026, 09:49 | Handel, Wirtschaft, Finanzen, Banken & Versicherungen

Pressemitteilung von: *Validato*


Industriespionage beginnt nicht immer mit einem Hackerangriff

## Wie Unternehmen Forschung, Entwicklung und Produktions-Know-how auch auf personeller Ebene besser schützen können.

Laut Bitkom-Studie „Wirtschaftsschutz 2025" werden Angriffe auf deutsche Unternehmen besonders häufig organisierter Kriminalität (68 Prozent der betroffenen Unternehmen) sowie staatlichen oder staatsnahen Akteuren aus Russland und China (je 46 Prozent) und ausländischen Nachrichtendiensten (28 Prozent) zugeordnet. Für Validato, Anbieter für Background-Checks und Human Risk Management mit Sitz in Zürich, zeigt diese Verteilung, dass Industriespionage nicht zwangsläufig über einen technischen Hackerangriff erfolgt, sondern häufig auch über Personen mit legitimem Zugang zu sensiblen Informationen.

**Was die Bitkom-Zahlen über die Angreifer verraten**

Organisierte Kriminalität und staatliche Akteure verfügen laut Bitkom-Studie über vielfältige Mittel, um an sensible Informationen zu gelangen – der klassische Hackerangriff ist nur eines davon. Nach Einschätzung von Validato gehört die gezielte Ansprache oder Platzierung von Personen mit Zugang zu Forschung und Entwicklung ebenfalls dazu. Ein Teil dieser Aktivitäten richtet sich laut Bitkom gezielt gegen Unternehmen mit wertvollem technologischen Vorsprung, etwa in Schlüsselindustrien wie Maschinenbau oder Automotive. Nach Einschätzung von Validato zeigt das, dass Industriespionage kein abstraktes Risiko für einzelne Grosskonzerne ist, sondern eine reale Bedrohung für einen breiten Kreis deutscher Unternehmen.

**Der Fokus liegt oft einseitig auf Cyberabwehr**

Sicherheitsbudgets fliessen laut Validato überwiegend in technische Abwehrmassnahmen. Personelle Präventionsmassnahmen wie strukturierte Background Checks für Forschungs- und Entwicklungsrollen erhalten demgegenüber vergleichsweise wenig Aufmerksamkeit. Diese Schwerpunktsetzung ist nachvollziehbar, da technische Angriffe unmittelbar messbar und oft gut dokumentiert sind. Personelle Risiken lassen sich dagegen schwerer quantifizieren, was ihre Berücksichtigung im Sicherheitsbudget laut Validato erschwert.

**Wege der personellen Spionage**

Wer Zugang zu Forschungsdaten, Konstruktionsplänen oder Produktions-Know-how hat, kann Informationen ohne technischen Angriff weitergeben – etwa über frühere oder parallele Verbindungen zu Wettbewerbern, finanzielle Anreize oder gezielte Ansprache durch Dritte. Auch der schrittweise Aufbau von Vertrauen über einen längeren Zeitraum, etwa durch scheinbar harmlose Kontakte auf Fachkonferenzen oder in sozialen Netzwerken, zählt laut Validato zu den bekannten Vorgehensweisen. Ziel ist es dabei häufig, eine Person zu identifizieren, die aus finanziellen oder persönlichen Gründen empfänglich für eine Ansprache ist.

**Forschung, Entwicklung und Produktion als Zielbereiche**

Nach Beobachtung von Validato sind besonders Positionen in Forschung, Entwicklung und Produktion relevant, da dort unmittelbarer Zugang zu wettbewerbsrelevantem Wissen besteht – oft über mehrere Jahre und mit wachsendem Vertrauensvorschuss. Gerade in mittelständischen Unternehmen mit spezialisiertem Nischen-Know-how kann der Verlust einzelner Schlüsselpersonen mit Insiderwissen besonders schwer wiegen. Validato empfiehlt deshalb, diese Rollen nicht erst bei konkreten Verdachtsmomenten, sondern präventiv in ein Prüfkonzept einzubeziehen.

**Präventive Personalrisikoprüfung als Ergänzung**

Validato empfiehlt, sensible F&E- und Produktionsrollen nicht nur beim Onboarding, sondern auch während eines laufenden Beschäftigungsverhältnisses wiederkehrend zu überprüfen, um Veränderungen im Risikoprofil frühzeitig erkennen zu können. Ein sinnvoller Anlass für eine erneute Prüfung ist laut Validato etwa der Wechsel in eine neue Projektrolle mit weitergehendem Zugriff auf sensible Forschungsdaten. So lässt sich das Risikoprofil einer Person kontinuierlich an ihre tatsächliche Verantwortung anpassen.

**Validato: Personalebene als Ergänzung zur Cyberabwehr**

Validato bietet dafür In-Employment-Screening sowie Sanktionslisten- und Hintergrundprüfungen als Teil einer umfassenden Sicherheitsstrategie an. „Die wertvollste Information verlässt ein Unternehmen selten über eine Firewall-Lücke, sondern über eine Person, die Zugang dazu hatte", so Reto Marti - Managing Partner von Validato. Für besonders exponierte Rollen in Forschung und Entwicklung kombiniert Validato dabei typischerweise mehrere Module, etwa Identitätsprüfung, Sanktionslistenabgleich und eine vertiefte Referenzprüfung. So entsteht laut Validato ein Prüfprofil, das sich gezielt am tatsächlichen Spionagerisiko einer Position orientiert.

**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: 1321223 • Views: 100 (Stand: 30.08.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/1321223/Industriespionage-beginnt-nicht-immer-mit-einem-Hackerangriff.html