oneconsult
together against cyberattacks



Cyberresilienz durch physische Angriffssimulationen

Warum Ihre Firewall nichts bringt, wenn die Tür offen ist

Juli 2026

Abstract

Physische Sicherheitsdefizite spielen eine messbare Rolle in der heutigen Bedrohungslandschaft: Laut IBM Cost of a Data Breach Report 2025 sind sie für rund 9% aller erfolgreichen Angriffe verantwortlich. Allein deutsche Unternehmen erlitten laut der Bitkom-Studie «Wirtschaftsschutz 2025» Schäden in Höhe von rund 87 Milliarden Euro durch analoge Angriffe. Industriespionage und Sabotage sind somit kein Randphänomen mehr und die Dunkelziffer dürfte deutlich höher liegen.

Zunehmend stehen ausländische Nachrichtendienste im Verdacht, immer kriminellere werdende Organisationen und Privatpersonen gezielt zu rekrutieren, um ihre operative Reichweite zu erhöhen. Gleichzeitig greifen digitale Schutzmassnahmen allein häufig zu kurz: Die Hybridisierung der Bedrohungsakteure führt zu immer professionelleren Angriffen, denen einseitige Schutzstrategien nicht mehr gerecht werden.

Echte Sicherheit entsteht erst durch das abgestimmte Zusammenspiel menschlicher, baulich-technischer, digitaler und organisatorischer Massnahmen.

Dieses Whitepaper analysiert die aktuelle Bedrohungslage im Kontext physischer Risiken im Bereich Informations- und Kommunikationstechnik (IKT) und zeigt die Grenzen isolierter Schutzansätze auf. Es erläutert, wie physische Angriffssimulationen eine realistische Bewertung der Sicherheitslage ermöglichen, beschreibt deren Ablauf und definiert die Voraussetzungen einer erfolgreichen Durchführung.

Das Whitepaper richtet sich an Führungskräfte von Unternehmen, die mit der Verantwortung für Informationssicherheit betraut sind. Praxisbeispiele und Erfahrungswerte aus zahlreichen Projekten von Oneconsult unterstützen dabei, den eigenen Schutzstatus kritisch zu hinterfragen. Konkrete Handlungsempfehlungen zeigen, wie physische Angriffssimulationen erfolgreich in die Sicherheitsstrategie integriert werden können.

03 **Auf physischem Wege direkt ins Netzwerk**

04 - 07 **Industriespionage und Sabotage – eine reale Bedrohung**
Risikolage in Zahlen, Staatliche Akteure und organisierte Kriminalität

08 - 13 **Technisch stark – systemisch verwundbar**
Menschlich, baulich-technisch, digital und organisatorisch

14 - 16 **Angriffssimulationen als Lösungsstrategie**
Ablauf und Voraussetzungen einer physischen Angriffssimulation

17 - 18 **Erkenntnisse und Handlungsempfehlungen**

Auf physischem Wege direkt ins Netzwerk

Es ist ein gewöhnlicher Dienstagmorgen. Vor dem Hintereingang eines grossen Unternehmens stehen zwei Personen in Business-Kleidung mit einem Kaffee in der Hand und führen eine angeregte Unterhaltung. Beide tragen gut sichtbar einen Mitarbeitenden-Badge – ein chiploses Imitat, erstellt auf Basis eines YouTube-Videos. Als der Hauswart das Gebäude verlässt, wird er freundlich gegrüsst, hält die Tür offen und lässt die vermeintlichen Mitarbeitenden eintreten.

Durch unverschlossene Innentüren gelangen die Angreifer an einen unbesetzten Arbeitsplatz. Sie schliessen ein vorbereitetes Rogue Device – ein manipuliertes Gerät, kaum grösser als ein USB-Stick – zwischen Netzwerk und Computer an. Das Gerät umgeht mittels NAC-Bypass die Schutzvorkehrungen und baut einen verschlüsselten Tunnel nach aussen auf. Ab diesem Moment besteht Remote-Zugang zum internen Netzwerk – ohne die Firewall zu umgehen, ohne Exploit, ohne Alarm. Nach 13 Minuten verlassen die Angreifer das Gebäude, ohne Spuren zu hinterlassen.

Der Aufwand der Angreifer: wenige hundert Schweizer Franken. Der potenzielle Schaden: Zugang zu sämtlichen internen Systemen, zu Kundendaten, zu Forschungs- und Entwicklungsunterlagen, zu vertraulicher E-Mail-Kommunikation – und ein Schaden in Millionenhöhe.



Dieses Szenario ist nicht fiktiv. Es basiert auf realen Erfahrungen aus physischen Penetration Tests und zeigt eine Realität, die viele Organisationen unterschätzen: Während Investitionen in technische Cybersicherheit steigen, bleiben physische und menschliche Angriffsvektoren häufig vernachlässigt.

Angreifer denken nicht in Silos. Sie suchen den Weg des geringsten Widerstands – und dieser führt nicht nur durch eine Firewall, sondern auch durch die Tür. Laut IBM Cost of a Data Breach Report 2025 sind physische Sicherheitsdefizite bereits für gut 9 % aller erfolgreichen Angriffe verantwortlich.[1] Mit der voranschreitenden technischen Härtung der IKT-Systeme dürften Social-Engineering-Angriffe – insbesondere durch physischen Zutritt – in Zukunft eher noch weiter zunehmen.

Dieses Whitepaper analysiert, warum physische Angriffe eine reale und zunehmend professionelle Bedrohung darstellen, welche Schwachstellen Organisationen besonders verwundbar machen und wie physische Angriffssimulationen – sogenannte Physical Penetration Tests – dazu beitragen können, die Cyberresilienz zu stärken.

Industriespionage und Sabotage – eine reale Bedrohung

Industriespionage und Sabotage sind keine abstrakten Risiken, sondern ein reales und branchenübergreifendes Problem – auch wenn sie in vielen Organisationen nach wie vor nicht als prioritäres Geschäftsrisiko behandelt werden. Insbesondere Unternehmen der DACH-Region mit wertvollem geistigem Eigentum, fortschrittlichen Fertigungsverfahren und strategisch relevanter Forschung stehen im Fokus. Als Standort führender Unternehmen in Bereichen wie Pharmazie und Chemie, Maschinen- und Anlagenbau, Finanz- und Versicherungswesen sowie Halbleitertechnik sind Unternehmen im DACH-Raum ein attraktives Ziel.

Dieses Kapitel zeigt auf, wie sich die aktuelle Risikolage präsentiert, weshalb die Gefahren systematisch unterschätzt werden und wieso Unternehmen gut beraten sind, sich auch gegen physische Angriffsvektoren zu schützen.

Risikolage in Zahlen

Die jährliche Bitkom-Studie «Wirtschaftsschutz» liefert die umfassendste Erhebung zur Bedrohungslage der deutschen Wirtschaft. Auch wenn physische Angriffsvektoren 2025 hinter digitalen zurücklagen, lassen die Ergebnisse aus der Befragung aufhorchen:

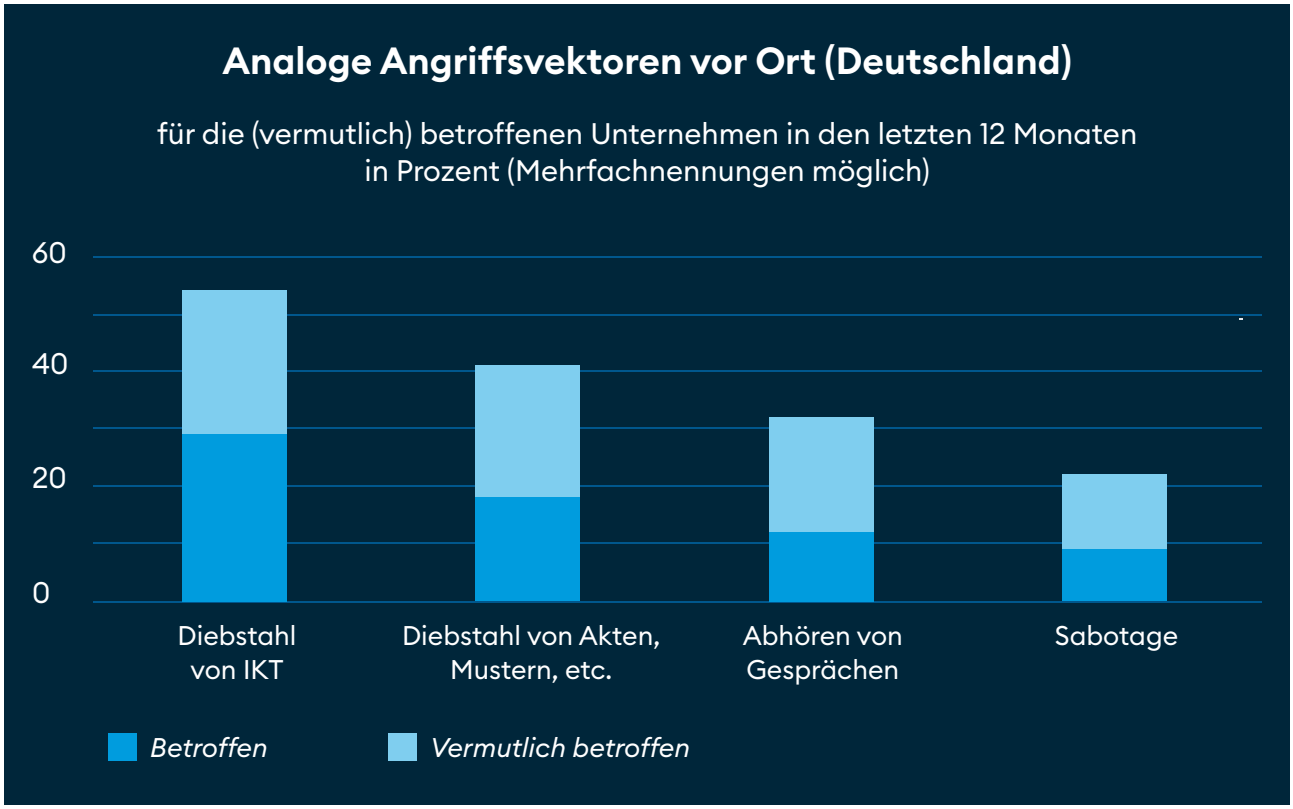


Tabelle 1: Analoge Angriffsvektoren vor Ort (Quelle: Bitkom-Studienbericht «Wirtschaftsschutz 2025», S. 11)



Das Motiv für den Diebstahl von Informations- und Kommunikationstechnik (IKT) ist nicht eindeutig. Es ist anzunehmen, dass in vielen Fällen der Weiterverkauf im Vordergrund steht. Die Auswirkungen auf die Informationssicherheit lassen sich – sofern Diebstähle rechtzeitig bemerkt werden – meist begrenzen.

Den anderen drei Kategorien liegt jedoch das Motiv der Industriespionage bzw. Sabotage zugrunde, wobei hier nicht mehr von einem Randphänomen gesprochen werden kann.

Zudem gab knapp jedes zweite Unternehmen an, in den letzten zwölf Monaten von (teilweise auch remote durchgeführten) Social-Engineering-Angriffen als Vorbereitung für Datendiebstahl, Industriespionage oder Sabotage betroffen gewesen zu sein.[2]

Der Gesamtschaden aller Angriffe stieg auf 289,2 Milliarden Euro – ein erneuter Rekordwert. Davon entfallen zwar 202,4 Milliarden Euro auf Cyberangriffe. Immerhin rund 87 Milliarden Euro resultieren jedoch aus analogen Angriffen, darunter physischer Diebstahl und Sabotage vor Ort.[3] Darin enthalten sind ebenfalls nur schwer quantifizierbare Schäden wie Reputationsverluste, Umsatzeinbussen infolge verlorener Wettbewerbsvorteile sowie Auftragsverluste etc.

Fehlende Statistik bedeutet nicht fehlendes Risiko

Ein zentrales Problem bei der Bewertung des Ausmasses analoger Angriffe ist die mangelnde Datenverfügbarkeit, da nur wenige Länder entsprechende öffentliche Statistiken führen. Die Bitkom-Studie stellt hier eine Ausnahme dar. Dies zeigt sich exemplarisch in der Schweiz: Seit dem 1. April 2025 besteht eine Meldepflicht für Cyberangriffe auf kritische Infrastrukturen. Analoge Vor-Ort-Angriffe werden jedoch nicht erfasst.

Vor einer freiwilligen, nicht anonymisierten Publikation von analogen Sicherheitsvorfällen scheuen sich Organisationen unter anderem aus Reputationsgründen. Die Zahlen für Studien und Statistiken stammen daher primär aus Befragungen, wobei Vorsicht in der Interpretation der Resultate geboten ist, da sie auf Selbstangaben und subjektiver Wahrnehmung der Befragten basieren.

Hinzu kommt, dass ein Angriff zunächst erkannt werden muss, um statistisch erfasst zu werden. Dies ist insbesondere dann schwierig, wenn zwischen dem Angriff und der Auswirkung eine grosse räumliche, zeitliche oder thematische Distanz besteht. Wird beispielsweise in China ein identisches Produkt auf den Markt gebracht, lässt sich der zugrunde liegende Informationsabfluss der Konstruktionspläne oft nur schwer eindeutig nachvollziehen oder zweifelsfrei zuordnen.

Erschwerend kommt die Abgrenzung zwischen Cybervorfällen und physischen Vorfällen hinzu, insbesondere wenn mehrere Angriffsvektoren kombiniert eingesetzt werden. Ein typisches Beispiel ist ein Passwort auf einem Notizzettel unter der Tastatur: Dieses kann im Rahmen eines physischen Zutritts in einem unbeobachteten Moment ausspioniert werden, während der eigentliche Systemzugriff remote erfolgt. Der Vorfall wird in der Praxis häufig als Cybervorfall klassifiziert, obwohl die zugrunde liegende Schwachstelle physischer Natur war.

In der Konsequenz ist davon auszugehen, dass die Anzahl analoger Angriffe in Studien deutlich zu tief ausgewiesen ist. Entscheidungsträger sind daher gut beraten, sich von der statistischen Unterrepräsentation nicht dazu verleiten zu lassen, das physische Angriffsrisiko zu unterschätzen.

Staatliche Akteure und organisierte Kriminalität

Selbst wenn zivilgesellschaftliche Aktivisten kreativ agieren, fehlen ihnen in der Regel sowohl die Mittel als auch die Kenntnisse für komplexe Angriffe auf IKT-Infrastrukturen, die Vor-Ort- und Cyber-Operationen kombinieren. Sie zielen zudem meist auf punktuelle Störungen und nicht auf langfristige Spionagekampagnen ab. Diese Tätergruppe ist zwar nicht irrelevant, jedoch liegt der Fokus im vorliegenden Whitepaper auf Akteuren, die in der Lage sind, über längere Zeit unentdeckt in IKT-Systemen zu persistieren und qualifizierte Informationen abfliessen zu lassen.

Dazu gehören insbesondere staatliche Akteure, die über grosse finanzielle sowie personelle Ressourcen verfügen, einen hohen Organisationsgrad haben und auch technische Mittel einsetzen können, die privat nicht beschaffbar sind. Angehörige und insbesondere diplomatisches Personal von Staaten, die für ihre extensive Spionage- und Sabotagetätigkeit bekannt sind[4], werden mittlerweile auf ihre Sicherheitsrisiken überprüft.[5/6] Die Ausdünnung des Agentennetzwerks in westlichen Ländern erschwert den Geheimdiensten zusehends ihre Aktivitäten vor Ort. Zur Kompensation setzen diese verstärkt und in völlig neuem Ausmass auf die Nutzung bestehender Strukturen der organisierten Kriminalität.[7] Zudem kommen vermehrt sogenannte «Wegwerf-Agenten» zum Einsatz – Privatpersonen, die oftmals über soziale Medien rekrutiert und für einzelne Einsätze vor Ort genutzt werden, jedoch nur schwer eindeutig mit staatlichen Akteuren in Verbindung gebracht werden können.[8]

Die zunehmende Konvergenz ist bemerkenswert: Staatliche Akteure nutzen kriminelle Gruppen sowie Privatpersonen als Werkzeuge, während diese dadurch ein Niveau an Professionalität erreichen, das früher staatlichen Akteuren vorbehalten war. Staatliche Akteure nutzen vermehrt kriminelle Gruppen für ihre Angriffe – dies erhöht die Komplexität der Bedrohungslage erheblich.

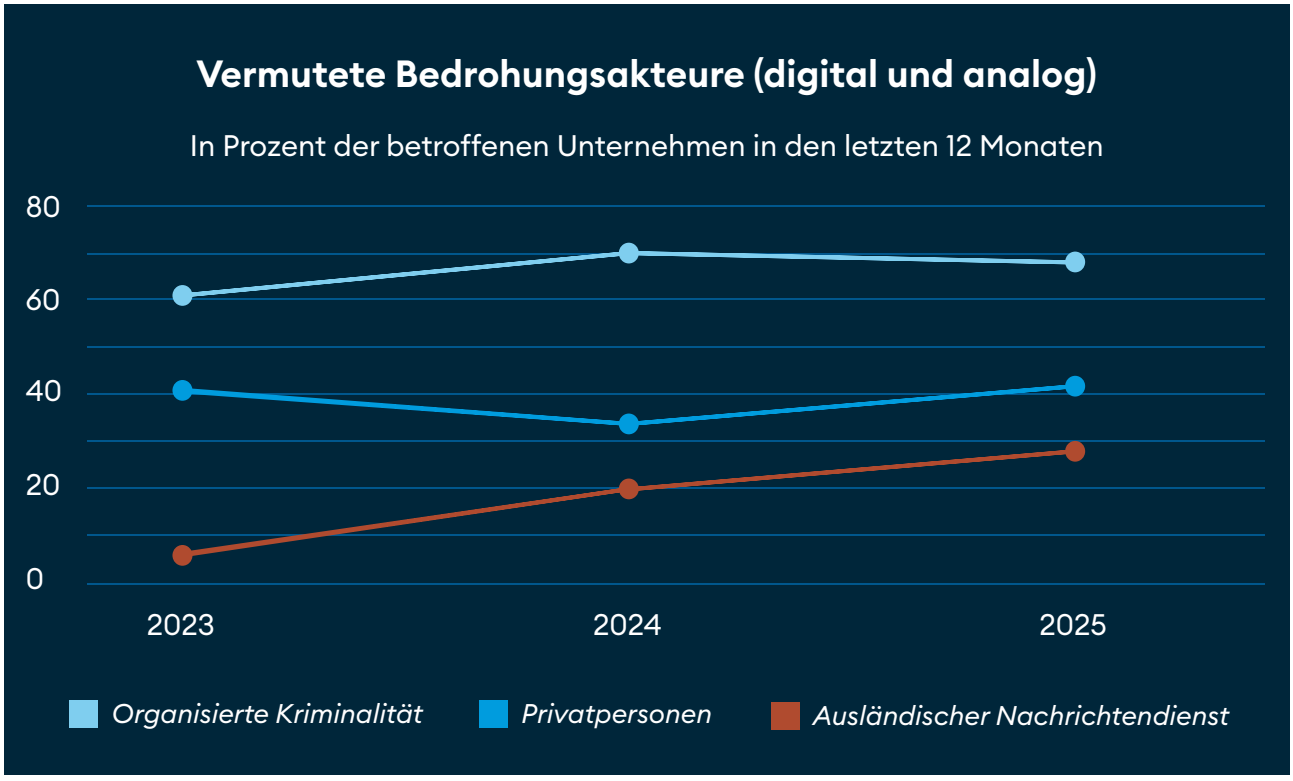


Tabelle 2: Bedrohungsakteure (Quelle: Bitkom Wirtschaftsschutz 2025, S. 13)

In der Bitkom-Studie werden genau diese drei Gruppierungen am häufigsten hinter Angriffen (digital und analog) vermutet. Interessant ist insbesondere die Zunahme der vermuteten Angriffe ausländischer Nachrichtendienste. Transparenterweise muss darauf hingewiesen werden, dass es sich um eine Wahrnehmung der Unternehmen handelt.

Spannend ist ebenfalls die Motivlage der Täterschaft. Laut Verizon Data Breach Investigations Report 2025, der sich jedoch nur auf Remote Social Engineering bezieht, war in ungefähr der Hälfte der Fälle Spionage das Ziel.[9]

Fazit zur Bedrohungslage

Die Risiken von Industriespionage und Sabotage für Unternehmen im DACH-Raum sind real. Faktische Schwierigkeiten in der Evaluierung von Sicherheitsvorfällen führen dazu, dass die tatsächliche Bedrohungslage wohl stark unterschätzt wird. Dies gilt insbesondere für analoge Angriffe vor Ort, die wesentlich schwieriger zu erkennen und nachzuvollziehen sind als reine Cyberangriffe. Durch die zunehmende Hybridisierung steigt das Potenzial verschiedener Bedrohungsakteure, hochprofessionelle Angriffe auszuführen. Weil viele Unternehmen ihre Cyberabwehr mittlerweile stark ausgebaut haben, ist zu vermuten, dass Angreifer in Zukunft vermehrt auf analoge Vektoren vor Ort und Social Engineering setzen werden – als Teil einer komplexen Angriffskette.

"Staatliche Akteure nutzen vermehrt kriminelle Gruppen für ihre Angriffe - dies erhöht die Bedrohungslage erheblich."



Technisch stark – systemisch verwundbar

Die Investitionen in die Cybersicherheit haben in den letzten Jahren ein beachtliches Niveau erreicht. Viele Organisationen verfügen über einen ausgereiften Perimeterschutz, leistungsfähige SIEM-Systeme, mehrstufige Authentifizierung und regelmässige Vulnerability Scans. Diese Massnahmen sind essenziell – doch sie adressieren primär technische Angriffsvektoren aus der Ferne.

Nachfolgend werden für die (IKT-)Sicherheit vor Ort wichtige Schutz- bzw. Risikofaktoren beleuchtet. Zudem werden typische Schwachstellen dargestellt, denen Oneconsult im Rahmen von Projekten bereits häufig begegnet ist. Die Ausführungen sind nicht abschliessend zu betrachten.

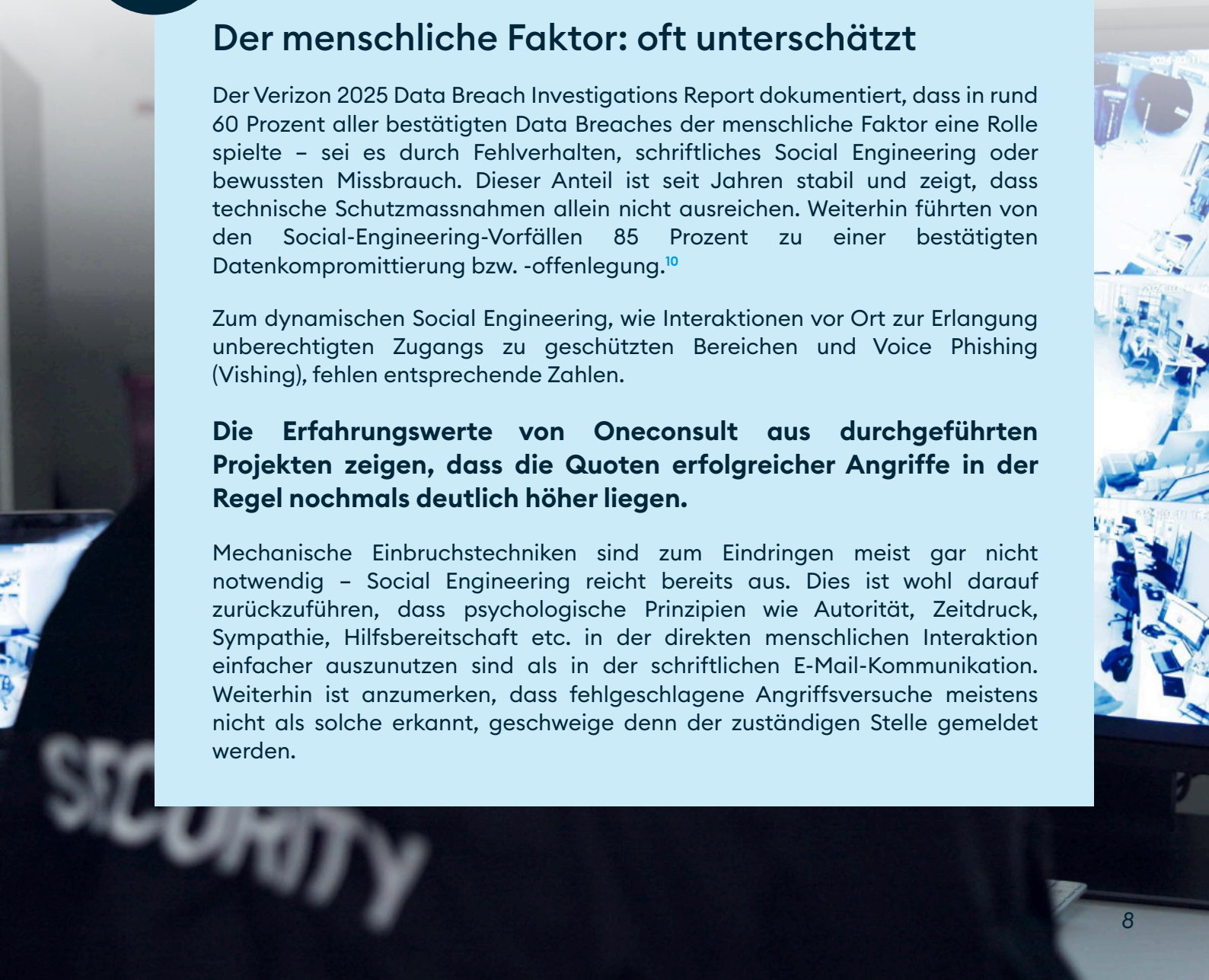
Der menschliche Faktor: oft unterschätzt

Der Verizon 2025 Data Breach Investigations Report dokumentiert, dass in rund 60 Prozent aller bestätigten Data Breaches der menschliche Faktor eine Rolle spielte – sei es durch Fehlverhalten, schriftliches Social Engineering oder bewussten Missbrauch. Dieser Anteil ist seit Jahren stabil und zeigt, dass technische Schutzmassnahmen allein nicht ausreichen. Weiterhin führten von den Social-Engineering-Vorfällen 85 Prozent zu einer bestätigten Datenkompromittierung bzw. -offenlegung.[10]

Zum dynamischen Social Engineering, wie Interaktionen vor Ort zur Erlangung unberechtigten Zugangs zu geschützten Bereichen und Voice Phishing (Vishing), fehlen entsprechende Zahlen.

Die Erfahrungswerte von Oneconsult aus durchgeführten Projekten zeigen, dass die Quoten erfolgreicher Angriffe in der Regel nochmals deutlich höher liegen.

Mechanische Einbruchstechniken sind zum Eindringen meist gar nicht notwendig – Social Engineering reicht bereits aus. Dies ist wohl darauf zurückzuführen, dass psychologische Prinzipien wie Autorität, Zeitdruck, Sympathie, Hilfsbereitschaft etc. in der direkten menschlichen Interaktion einfacher auszunutzen sind als in der schriftlichen E-Mail-Kommunikation. Weiterhin ist anzumerken, dass fehlgeschlagene Angriffsversuche meistens nicht als solche erkannt, geschweige denn der zuständigen Stelle gemeldet werden.



Der baulich-technische Faktor: oft überschätzt

Während Organisationen erhebliche Mittel in digitale Sicherheitslösungen investieren, bleiben physische Schutzsysteme häufig auf einem veralteten Stand von vor einem Jahrzehnt oder mehr. Zutrittskontrollsysteme werden zwar implementiert, jedoch erst am Ende ihres Lebenszyklus überprüft. In der Zwischenzeit entwickeln sich Angriffstechniken weiter, sodass solche Systeme etwa durch das Klonen veralteter Zutrittsmedien unter Umständen umgangen werden können.

Der Nutzen von Videoüberwachung wird häufig überschätzt. Zwar kann sie auf Gelegenheitstäter abschreckend wirken, bei professionellen Gruppen ist dieser Effekt jedoch stark begrenzt. Ohne aktives Monitoring und definierte Interventionsprozesse entfaltet sie kaum präventive Wirkung und dient primär der nachträglichen Aufklärung – sofern ein Vorfall rechtzeitig erkannt wird und Aufnahmen aufgrund der strengen gesetzlichen Aufbewahrungsfristen in der DACH-Region noch verfügbar sind.

Moderne Einbruchmeldeanlagen, normgerecht installiert, bieten grundsätzlich ein hohes Schutzniveau. Einschränkend ist jedoch zu berücksichtigen, dass Angriffe im Bereich Industriespionage und Sabotage häufig während der Betriebszeiten erfolgen, wenn derartige Anlagen teilweise deaktiviert sind.

In Hinsicht auf die Türfachplanung ist festzuhalten, dass Türen für Unternehmensgebäude heutzutage sehr robust gebaut werden. Klassische Öffnungstechniken wie *Lockpicking** und der *Checkkarten-Trick** werden durch mechanische Sicherheitsvorkehrungen verhindert. Sie sind Angreifern nur noch in Altbauten oder bei der Öffnung von Kellertüren, unkritischen Lagern etc. nützlich. Am ehesten ist das *Under Door Tool (UDT)** erfolgsversprechend, da Türen für das effiziente Funktionieren von Lüftungs- und Klimaanlagen teilweise über eine gewisse Bodenluft (Türspalt) verfügen müssen.

Die Gefahr geht aber nicht ausschliesslich von der Schwäche der Systeme aus, sondern vom blinden Vertrauen, das in sie gesetzt wird. Einerseits ist oft zu beobachten, **dass sich Mitarbeitende stark auf die getroffenen baulich-technischen Sicherheitsvorkehrungen verlassen und dadurch ihre Awareness gegenüber Social-Engineering-Angriffen leidet.** Wird im internen Bereich eine unbekannte Person angetroffen, erfolgen keine kritischen Nachfragen, da ein Zutrittskontrollsystem vorhanden ist. Dass sich die Person initial durch Tailgating* oder Piggybacking* Zutritt zum internen Bereich verschafft haben könnte, daran denken in diesem Moment die wenigsten Personen.

**Erklärungen zu den Begriffen im Glossar.*

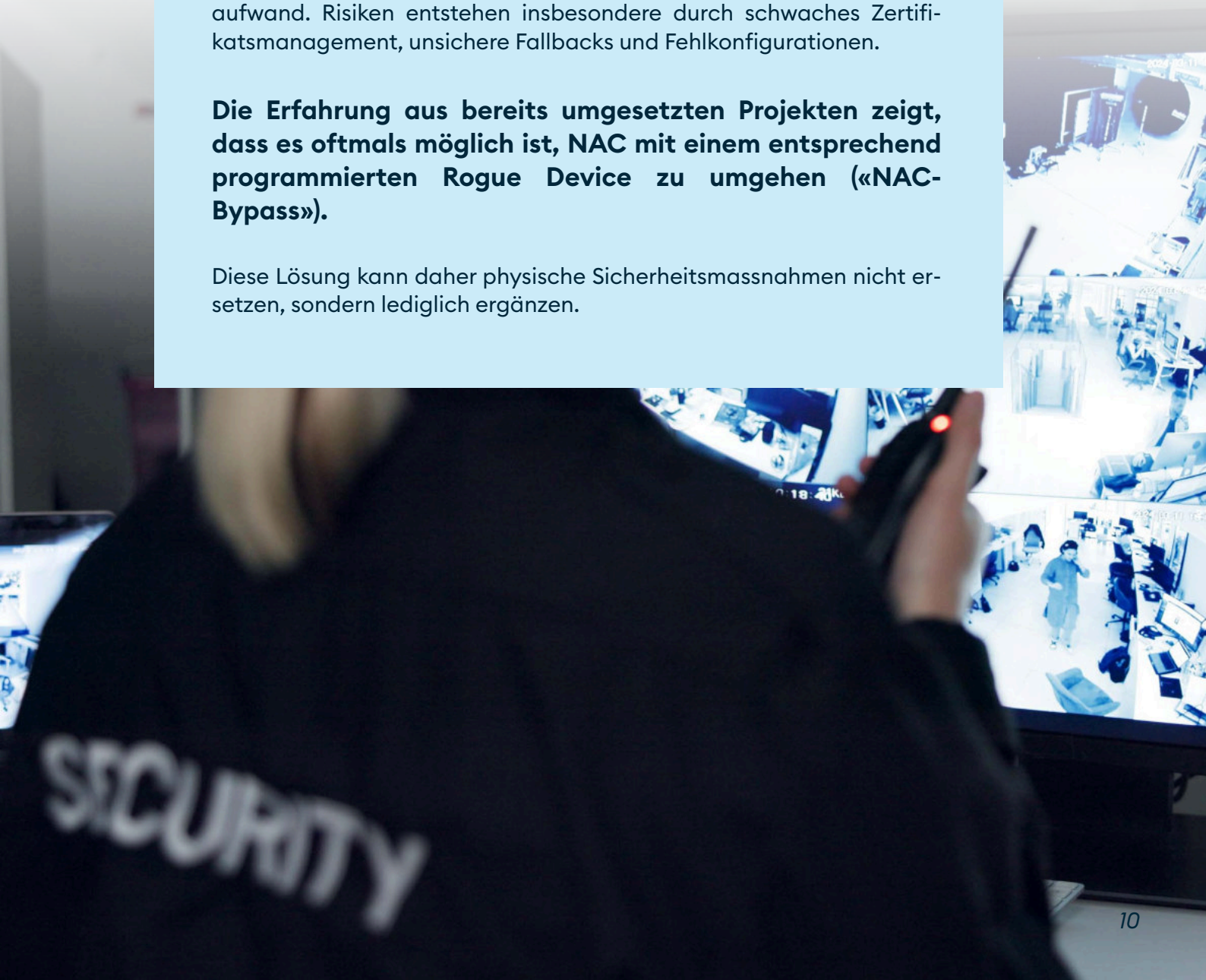
Der digitale Faktor: oft unsicher

Network Access Control (NAC) regelt den Zugriff auf Unternehmensnetzwerke anhand von Identität, Gerät und Sicherheitsrichtlinien. In der Praxis basiert dies meist auf 802.1X mit zertifikatsbasierter Authentisierung, ergänzt durch Fallback-Mechanismen wie den MAC Authentication Bypass (MAB).

Die Einführung von NAC ist anspruchsvoll, da heterogene Systeme, mobile Arbeitsumgebungen und komplexe Richtlinien die Umsetzung erschweren. Häufige Einschränkungen ergeben sich durch Legacy-Infrastrukturen, fehlende Standardisierung und einen hohen Betriebsaufwand. Risiken entstehen insbesondere durch schwaches Zertifikatsmanagement, unsichere Fallbacks und Fehlkonfigurationen.

Die Erfahrung aus bereits umgesetzten Projekten zeigt, dass es oftmals möglich ist, NAC mit einem entsprechend programmierten Rogue Device zu umgehen («NAC-Bypass»).

Diese Lösung kann daher physische Sicherheitsmassnahmen nicht ersetzen, sondern lediglich ergänzen.



Der organisatorische Faktor: oft vernachlässigt

Oft werden die vorgenannten Schutzfaktoren – menschlich, baulich-technisch und digital – isoliert betrachtet. Dies liegt zum einen daran, dass die Verantwortlichkeiten in Unternehmen häufig auf verschiedene Personen verteilt sind. Zum anderen ist nicht in allen Bereichen die erforderliche Expertise vorhanden, wenn alle Fachgebiete einer einzelnen verantwortlichen Person zugeordnet sind.

Ein typisches Beispiel sind Defizite in Zonen- und Berechtigungskonzepten. Ein Zonenplan entspricht nicht automatisch einem physischen Berechtigungskonzept: Bereiche, die im Zonenkonzept einheitlich klassifiziert sind, werden häufig ohne zusätzliche physische Barrieren für alle Mitarbeitenden dieser Zone zugänglich gemacht. Sind Angreifer einmal eingedrungen, können sie sich so weitgehend ungehindert innerhalb des internen Bereichs bewegen. Auch interne Risiken, etwa durch einen «Malicious Insider», werden dadurch verstärkt, da Mitarbeitende Zugriff auf Bereiche erhalten, die für ihre Tätigkeit nicht erforderlich sind. In der Praxis erfolgt die Vergabe von Badge-Berechtigungen häufig hierarchisch statt nach dem Prinzip «Need-to-Go», wodurch selbst administrative Rollen Zugriff auf kritische Infrastrukturbereiche wie die Stromversorgung erhalten, ohne dass eine operative Notwendigkeit besteht.

Auch das Besuchermanagement weist regelmässig Schwächen auf. Begleitende Fachbereiche sind oft nicht ausreichend informiert, wodurch soziale Kontrolle kaum möglich ist. Teilweise werden nur Eintrittszeiten registriert, Austritte jedoch nicht dokumentiert. Unzureichende Übergaben im Schichtbetrieb sowie papierbasierte Protokolle erschweren zudem die Übersicht über Personen im Gebäude. Diese Lücken beeinträchtigen nicht nur die operative Sicherheitskontrolle, sondern können im Brandfall oder etwa bei Evakuierungen sicherheitskritische Auswirkungen haben.

Selbst wenn Sicherheits- und Überwachungssysteme wie eine Videoüberwachung installiert sind, fehlt oft eine klar definierte Interventionsorganisation. Personelle Reserven für aussergewöhnliche Situationen existieren selten. Muss das Sicherheitspersonal auf einen Vorfall reagieren, bleibt der überwachte Bereich in dieser Zeit unkontrolliert. Dies eröffnet die Möglichkeit des unberechtigten Eindringens durch Ablenkungsmanöver.

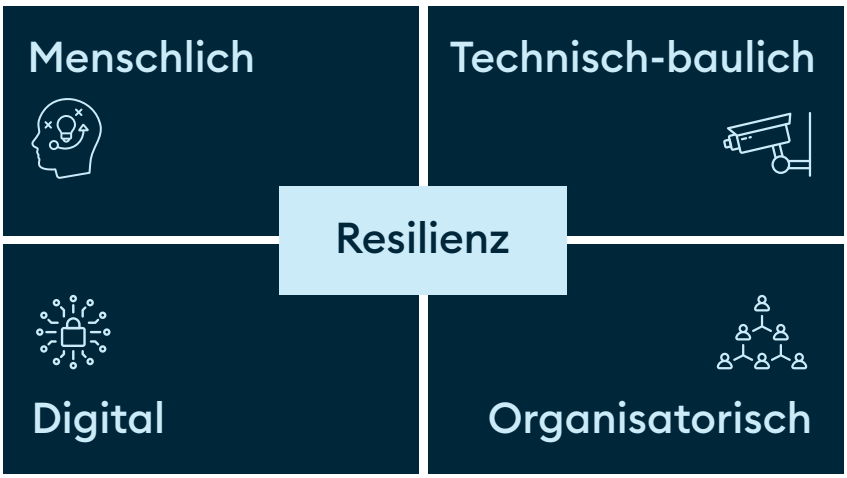
Abschliessend ist zu beachten, dass organisatorische und technische Sicherheitsmassnahmen einem kontinuierlichen Wandel unterliegen: Bauliche Vorgaben werden angepasst, Räume umgenutzt und Schutzsysteme ersetzt. Ohne regelmässige Überprüfung können dadurch unerkannte Sicherheitslücken entstehen. In der Praxis erfolgt die Anpassung bestehender Konzepte jedoch oft nur im Rahmen grösserer Revisionen. Eine kontinuierliche Überprüfung und Nachführung ist daher entscheidend, um die Wirksamkeit der Sicherheitsarchitektur dauerhaft sicherzustellen.



Fazit zu den Schutzfaktoren

Einzelne Schutzfaktoren entfalten für sich nur eine begrenzte Wirkung. Sicherheit entsteht erst, wenn die Massnahmen aufeinander abgestimmt sind. Da jeder Schutzfaktor Schwächen oder Angriffsmöglichkeiten aufweisen kann, ist eine faktorübergreifende, redundante Umsetzung essenziell. Andernfalls können Angreifer durch das gezielte Ausnutzen einzelner Schwachstellen einen Pfad bis zum kritischen Zielbereich finden. Das Versagen eines einzelnen Schutzfaktors kann in solchen Fällen das gesamte Sicherheitskonzept in seiner Wirksamkeit beeinträchtigen.

Besonders entscheidend sind organisatorische Massnahmen und das gelebte Sicherheitsverhalten der Mitarbeitenden im Alltag. Umfangreiche Investitionen in technische und bauliche Sicherheitsmassnahmen entfalten nur begrenzte Wirkung, wenn Awareness und organisatorische Prozesse nicht berücksichtigt werden. Unternehmen sollten daher ihre finanziellen Ressourcen ausgewogen einsetzen, um eine wirksame und nachhaltige Sicherheitsarchitektur zu gewährleisten.



Um die Wirksamkeit dieser Schutzfaktoren im Zusammenspiel sicherzustellen, sollten sie nicht nur isoliert, sondern auch gemeinsam getestet werden. Physische Penetration Tests bieten hierfür einen praxisnahen Ansatz, weil sie das Zusammenwirken aller Massnahmen unter realistischen Bedingungen überprüfen. Da sich Sicherheitsarchitekturen kontinuierlich verändern, können solche Tests nicht als einmalige Massnahme verstanden werden. Vielmehr sollten sie regelmässig und nach wesentlichen Veränderungen durchgeführt werden, um ein belastbares Bild des aktuellen Sicherheitsniveaus zu gewährleisten.

10 typische Schwachstellen in Unternehmen

Aufenthaltsbereiche in Türnähe	Aufenthaltsbereiche (z. B. Raucherbereiche) befinden sich oft in unmittelbarer Nähe von Aussentüren. Dies erlaubt es Angreifern, sich mit legitimem Anschein dort aufzuhalten und gezielt Tailgating-Versuche durchzuführen.
Tiefgarage zu Fuss zugänglich	Wird die Zufahrt für Fahrzeuge kontrolliert, wird der Bereich von Mitarbeitenden oft als interne Zone wahrgenommen. Unbefugte Personen werden daher selten hinterfragt und erhalten mitunter Zutritt zum Gebäude.
Einbruchmeldeanlage nur im Erdgeschoss	Fehlt die Absicherung für höher gelegene Stockwerke, können Angreifer über Fenster oder alternative Zugänge (z. B. mit Leitern) unbemerkt in das Gebäude eindringen.
Unzureichende Bildqualität der Videoüberwachung	Reicht die Bildqualität nicht aus, kann dies eine Identifikation von Personen im Nachhinein unmöglich machen. Die forensische Wirkung der Anlage ist somit stark eingeschränkt.
Von aussen einsehbare Informationen	Sensible Informationen auf Bildschirmen, Whiteboards oder Flipcharts können durch das Fenster eingesehen und mit technischen Hilfsmitteln erfasst werden.
Aufzug ohne Zugangskontrolle	Auch wenn der Aufzug nur per Badge gesteuert werden kann, ermöglicht ein freier Zugang zur Kabine Angreifern das ungehinderte Einsteigen. Durch das Abwarten eines entsprechenden Zielrufs können sie so in interne Bereiche gelangen.
Orientierungstafeln und Raumbeschriftungen	Orientierungstafeln und Raumbeschriftungen erleichtern Angreifern die Orientierung im Gebäude und ermöglichen ein zielgerichtetes Vorgehen. Interne Mitarbeitende sind auf diese Informationen meist nicht angewiesen.
Unverschlossene Kellerräume	Wenig genutzte Räume können als Rückzugs- oder Warteräume dienen. Angreifer können sich dort verstecken und sich ausserhalb der Betriebszeiten ungestört im Gebäude bewegen.
Zentrale Schlüsselboxen	Häufig unzureichend gegen Aufbrechen oder Abreissen gesichert. Nach erfolgreicher Öffnung ermöglichen sie Angreifern den Zugang zu einer Vielzahl von Räumen oder Behältnissen.
Offene Dokumentenablagen	Vertrauliche Informationen sind frei zugänglich, sobald sich Angreifer im internen Bereich befinden. Dies ermöglicht einen direkten Informationsabfluss ohne zusätzliche Sicherheitsbarrieren.

oneconsult
together against cyberattacks

Angriffssimulationen als Lösungsstrategie

Unternehmen, die tatsächliche Sicherheit und nicht nur die Erfüllung von Compliance-Anforderungen anstreben, kommen nicht umhin, ihre Sicherheitsmassnahmen in ihrer Gesamtheit zu testen. Denn Angreifer benötigen nicht viele bzw. keine grossen Sicherheitslücken – ihnen reicht der eine Angriffspfad, der sie zu den Kronjuwelen des Unternehmens führt.

Mit Angriffssimulationen können Angriffe auf eine Organisation unter kontrollierten Bedingungen realitätsnah nachgestellt werden, um Schwachstellen zu identifizieren. Sie kombinieren Methoden aus der physischen Sicherheitsprüfung, dem Social Engineering und der Cybersicherheit, um ein möglichst realistisches Bild der tatsächlichen Sicherheitslage zu erhalten.

Hierbei können einzelne Angriffsphasen isoliert oder als integraler Angriffszyklus evaluiert werden, zum Beispiel:

Erlangen von physischem Zugriff auf das Netzwerk durch ein **Physical Access Assessment**

Erlangen von Zugangsdaten für einen initialen Zugriff auf die IT-Infrastruktur durch **Vishing**

Kompromittieren kritischer Unternehmensdaten und -systeme durch **technisches Red Teaming**

Ablauf einer physischen Angriffssimulation

Eine professionelle physische Angriffssimulation folgt einem strukturierten Prozess, der sich an der Vorgehensweise realer Angreifer orientiert:



Nachfolgend werden die vier operativen Hauptphasen näher erläutert.



Open Source Intelligence (OSINT) bezeichnet die systematische Sammlung, Auswertung und Analyse von frei zugänglichen Informationen aus öffentlichen Quellen, um daraus verwertbare Erkenntnisse zu gewinnen. Dabei werden beispielsweise die offiziellen Auftritte des Unternehmens, aber auch die privaten Profile von Schlüsselmitarbeitenden auf nützliche Informationen überprüft. Insbesondere Unternehmensvideos und öffentlich zugängliche Videoinhalte sowie Stellenausschreibungen erlauben oftmals Rückschlüsse auf die Gebäudestruktur, die eingesetzte Sicherheitstechnik und die Betriebsabläufe. Weiterhin sind Ausschreibungen eine wertvolle Quelle, da sie häufig Hinweise auf eingesetzte Systeme beinhalten. Die einzelnen Informationen sind für sich meist unkritisch und entfalten ihr sicherheitsrelevantes Potenzial erst als Ganzes.

Nicht zu unterschätzen sind auch öffentliche Erwähnungen des Unternehmens durch Drittparteien wie Lieferanten und Servicebeauftragte, wodurch sich das Netz der Geschäftsbeziehungen oft relativ genau abbilden lässt. Im Rahmen von Projekten dient dies primär der Erstellung eines Pretext . Reale Angreifer nutzen dieses Wissen über Drittparteien für Supply-Chain-Angriffe , um über indirekte Wege in das System des Zielunternehmens zu gelangen oder dieses zu schädigen. So berichten 41 Prozent der betroffenen deutschen Unternehmen von spürbaren Folgen – etwa Lieferausfällen oder Reputationsschäden – wenn ein Zulieferer von Datendiebstahl, Industriespionage oder Sabotage betroffen war.[11]

OSINT bietet Angreifern den Vorteil einer effizienten und sicheren Fernrecherche. Bei opportunistischen und primär monetär getriebenen Akteuren entscheidet die festgestellte Angriffsfläche nicht zuletzt darüber, welches Unternehmen überhaupt angegriffen werden soll. Ein bewusster Umgang mit öffentlich verfügbar gemachten Informationen ist daher ein wichtiger präventiver Schutzfaktor für ein Unternehmen.



Die Objektaufklärung, d. h. die Zielaufklärung vor Ort, bildet zusammen mit der OSINT-Recherche die Grundlage für die operative Planung einer aussagekräftigen Social-Engineering-Kampagne. Sie dient dazu, Informationen über die aktuellen lokalen Gegebenheiten sowie die tatsächlich gelebten Prozesse der Mitarbeitenden zu gewinnen.

Professionelle Angreifer gehen bisweilen noch einen Schritt weiter: Sie observieren Schlüsselpersonen über längere Zeit hinweg auch im privaten Umfeld. Dadurch erstellen sie detaillierte Personen- und Persönlichkeitsprofile. Mithilfe dieser Informationen können beispielsweise Passwörter gezielter erraten, Personen erpresst oder verdeckte Kontaktaufnahmen vorbereitet werden.[12]



Reale Angriffe sind oftmals komplex und mehrstufig. Mit **Vorausaktionen** werden die Grundlagen für ein erfolgreiches Eindringen in das Unternehmen vorbereitet. Hierzu können zum Beispiel Vishing-Anrufe am Empfang dienen, um unter einem Vorwand den Code für die Eingangstür zu erlangen oder durch geschickte unauffällige Fragen Informationen zum genauen Anlieferungsprozess von Waren zu gewinnen.



Nach mehreren Wochen Vorbereitung findet der eigentliche physische Zutritt vor Ort statt. Dieser **physische Penetration Test** beinhaltet die Phase Infiltration, Lateral Movement und Exfiltration. Wie einleitend erwähnt, kann die Verweildauer im Gebäude äusserst kurz – teils nur einige Minuten – sein, wenn der Einsatz gut geplant ist und die situativen Umstände günstig sind.

Unter Verwendung verschiedener Social-Engineering- und technischer Methoden werden Zugangsmöglichkeiten zu internen Bereichen getestet, indem Schwachstellen im Mitarbeitendenverhalten, in betrieblichen Prozessen sowie in baulich-technischen Vorkehrungen kombiniert ausgenutzt werden. Nach dem Erreichen der mit dem Kunden vereinbarten Einsatzziele (Flags) erfolgt in der Regel die verdeckte Exfiltration. Alternativ kann auch bewusst die Reaktion des Abwehrteams provoziert werden, um Interventions- und Eskalationsprozesse zu testen.

Voraussetzungen für eine gute Angriffssimulation

Physische Angriffssimulationen liefern Erkenntnisse, die mit keiner anderen Evaluationsart gewonnen werden können: eine realistische Bewertung der tatsächlichen Sicherheitslage unter Bedingungen, die einem echten Angriff nahekommen. Sie ermöglichen es, Schwachstellen zu identifizieren, bevor reale Angreifer dies tun, und bilden die Grundlage für gezielte und priorisierte Verbesserungsmassnahmen.

Der Mehrwert solcher Tests ist hoch, jedoch mit entsprechendem Planungs- und Ressourcenaufwand verbunden. Eine strukturierte Vorbereitung ist daher entscheidend, um die Wirksamkeit der Simulation zu gewährleisten und den Nutzen der Ergebnisse zu maximieren.

Erkenntnisse & Handlungsempfehlungen

Die in diesem Whitepaper dargestellten Ergebnisse führen zu einer klaren Schlussfolgerung: Physische Angriffe sind real, messbar und zunehmend professionell. Sie nutzen menschliche, baulich-technische, digitale und organisatorische Schwachstellen kombiniert aus. Organisationen, die ihre Sicherheitsstrategie ausschliesslich auf digitale Massnahmen stützen, übersehen systematisch einen erheblichen Teil der tatsächlichen Bedrohungslandschaft.

Sicherheit ist systematisch: Jedes Unternehmen ist sowohl Leistungsbezieher als auch Leistungserbringer. Schwächen innerhalb einer Organisation können sich entlang der Wertschöpfungskette auf weitere Akteure auswirken.

Mangelnde operative IKT-Resilienz ist kein reines Cyberproblem: Die Bedrohungslandschaft umfasst digitale, menschliche und physische Dimensionen, die gleichwertig berücksichtigt werden müssen.

Angreifer denken hybrid: Moderne Angreifer kombinieren Methoden aus verschiedenen Bereichen. Eine Verteidigungsstrategie, die in Silos organisiert ist, wird diesem Ansatz nicht gerecht.

Die tatsächliche Sicherheitsmaturität zeigt sich erst im integralen Test: Isolierte Prüfungen einzelner Schutzmassnahmen geben nur begrenzt Aufschluss über die reale Widerstandsfähigkeit. Erst durch ganzheitliche Angriffssimulationen wird sichtbar, wie effektiv die Schutzfaktoren im Zusammenspiel funktionieren.

Physische Angriffssimulationen adressieren spezifische Realitätslücken: Sie machen insbesondere jene Schwachstellen sichtbar, die durch menschliches Verhalten, baulich-technische Gegebenheiten und organisatorische Abläufe entstehen, und liefern damit eine unverzichtbare Grundlage für gezielte Verbesserungsmassnahmen.



Konkrete Handlungsempfehlungen

Bedrohungsakteure evaluieren: Bewerten Sie, welche Angreifergruppen für Sie relevant sind und über welche Fähigkeiten diese verfügen bzw. wie diese typischerweise vorgehen. Lassen Sie gegebenenfalls einen Threat Intelligence Report erstellen.

Schutzmassnahmen auf Ihre IKT-Relevanz prüfen: Beurteilen Sie systematisch, wie sich physische und menschliche Schwachstellen auf Ihre Informationssicherheit auswirken. Behandeln Sie diese mit der gleichen Priorität wie Cybergefahren.

Angriffssimulationen durchführen: Lassen Sie die Wirksamkeit von Schutzmassnahmen im Zusammenspiel testen, um reale Schwachstellen sichtbar zu machen. Wiederholen Sie solche Assessments regelmässig.

Compliance-Anforderungen erfüllen: Auch regelmässige physische Sicherheitsüberprüfungen werden von verschiedenen Regulatoren gefordert. Unter anderem im ISO-2700x-Standard, in der NIS-2-Direktive oder aber im Rahmen von DORA für den EU-Finanzsektor und seinen IKT-Dienstleistern.

oneconsult
together against cyberattacks

Schützen Sie Ihr Unternehmen

Eine realistische Bewertung der Sicherheitslage erfordert die Identifikation verbleibender Schwachstellen, bevor diese durch reale Angreifer ausgenutzt werden. Angriffssimulationen unterstützen dabei, die Resilienz unter realitätsnahen Bedingungen systematisch zu überprüfen.

Physical Access Assessment

Im Rahmen eines Black-Box-Testansatzes wird das bestehende Abwehrdispositiv unter realen Bedingungen evaluiert. Dadurch entsteht eine ganzheitliche Sicherheitsbewertung, die unterschiedliche physische, organisatorische und technische Angriffsvektoren berücksichtigt.

Die Ergebnisse werden in einem strukturierten Bericht mit priorisierten Schwachstellen und konkreten Handlungsempfehlungen aufbereitet.

› Jetzt mehr erfahren

Gerne unterstützen wir Sie bei der Einordnung Ihrer aktuellen Sicherheitslage und der Planung geeigneter Testansätze.

Für einen vertraulichen und unverbindlichen Austausch stehen Ihnen unsere Fachexperten zur Verfügung.



Antonio Rainelli

Senior Client Services Manager

antonio.rainelli@oneconsult.com
T +41 43 377 22 52
M +41 79 630 36 78
Termin buchen: calendly.com/antonio-rainelli

Glossar

Checkkarten-Trick	Einfach gebaute Türen können durch Zurückdrücken der Falle mit einer flexiblen Karte geöffnet werden.
Lockpicking	Lockpicking bezeichnet die Manipulation eines Schliesszylinders bzw. das Öffnen einer Tür durch spezielles Werkzeug.
Piggybacking	Beim Piggybacking wird eine unbefugte Person von einer berechtigten Person bewusst hereingelassen, beispielsweise weil sie vorgibt, ihren Badge vergessen zu haben.
Pretexting	Pretexting bezeichnet eine Methode des Social Engineering, bei der Angreifer eine glaubhafte Geschichte («Pretext») konstruieren, um das Vertrauen einer Zielperson zu gewinnen und sie zur Preisgabe sensibler Informationen oder zur Durchführung bestimmter Handlungen zu bewegen.
Supply-Chain-Angriff	Bei einem Supply-Chain-Angriff nutzen Angreifer gezielt Schwachstellen in der Lieferkette eines Unternehmens aus – etwa bei Software, Hardware, Dienstleistern oder Drittanbietern –, um indirekt Zugang zu einem Zielsystem zu erlangen.
Tailgating	Tailgating bezeichnet das unauffällige Nachfolgen einer berechtigten Person durch eine gesicherte Tür.
Under Door Tool (UDT)	Das UDT ist ein Werkzeug zum Betätigen von Türgriffen von aussen, das durch die Bodenluft unter der Tür durchgeschoben wird.

Quellenverzeichnis

1. **SPAC Alliance.** (September 2025). IBM Cost of a Data Breach Report 2025 – Analyse, S. 17.

2. **Bitkom/Bundesamt für Verfassungsschutz.** (September 2025). Wirtschaftsschutz 2025, S. 24. https://www.bitkom.org/sites/main/files/2025-12/bitkom-studienbericht-wirtschafts-schutz-2025_2.pdf

3. **Bitkom/Bundesamt für Verfassungsschutz.** (September 2025). Wirtschaftsschutz 2025, S. 19. https://www.bitkom.org/sites/main/files/2025-12/bitkom-studienbericht-wirtschafts-schutz-2025_2.pdf

4. **Bitkom/Bundesamt für Verfassungsschutz.** (September 2025). Wirtschaftsschutz 2025, S. 16. https://www.bitkom.org/sites/main/files/2025-12/bitkom-studienbericht-wirtschafts-schutz-2025_2.pdf

5. **Tagesanzeiger.** (Oktober 2025). ETH hat 80 Bewerber aus dem Ausland abgewiesen. https://www.tagesschau.de

6. **Tagesschau.** (April 2024). Geheimprojekt "Harmonie". https://www.tagesschau.de/investigativ/ndr-wdr/spionage-technik-russland-deutschland-100.html

7. **Brombacher & Vorrath.** (Juli 2025). Die Transformation transnationaler organisierter Kriminalität - Neue Risiken verlangen neue Antworten von Europa, S. 4. SWP-Aktuell, Nr. 37. https://www.swp-berlin.org/publications/products/aktuell/2025A37_transnationale_organisierte_kriminalitaet.pdf

8. **Norddeutscher Rundfunk NDR.** (Oktober 2025). Verfassungsschutz: So wirbt der russische Geheimdienst Agenten an. https://www.ndr.de/nachrichten/niedersachsen/verfassungsschutz-so-wirbt-der-russische-geheimdienst-in-deutschland-agenten-an,verfassungsschutz-176.html

9. **Verizon.** (2025). Data Breach Investigations Report (DBIR), S. 46. https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf

10. **Verizon.** (2025). Data Breach Investigations Report (DBIR), S. 20. https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf

11. **Bitkom/Bundesamt für Verfassungsschutz.** (September 2025). Wirtschaftsschutz 2025, S. 15. https://www.bitkom.org/sites/main/files/2025-12/bitkom-studienbericht-wirtschafts-schutz-2025_2.pdf

12. **Nachrichtendienst des Bundes.** (Mai 2016). "Im Visier" – Wirtschaftsspionage in der Schweiz. https://www.youtube.com/watch?v=ad6td7NNsAc&list=PLAorZm3BkjdC6qDb-4Pr6vlXpO6E79jJt&index=6

Weiterführende Ressourcen

Blogbeiträge

- Höhere Cyberresilienz durch Angriffssimulationen nach DORA und TIBER
- Social Engineering – Einführung und Methoden (Teil 1)
- Social Engineering – Gefahren und Prävention für Unternehmen (Teil 2)

Webinar

- Inside the Mind of a Social Engineer

Podcast

- Der Mensch als Schwachstelle (Cyberfunk)