Bild: Pixabay

Gemäss einer TÜV-Studie werden organisierte Kriminalität (55 Prozent) und staatliche Hacker (47 Prozent) als Hauptbedrohungen identifiziert.

Cybersecurity Studien 2025

Täglich wird in den Medien über erfolgreiche Hacker-Angriffe berichtet. Zu den möglichen Folgen zählen unter anderem Daten-Diebstahl, Zahlung bei Ransomware oder sogar die Insolvenz. Drei aktuelle Studien liefern spannende Einblicke in die momentanen Entwicklungen: die TÜV Cybersecurity Studie 2025, der Deloitte Cyber Security Report 2025 und die Schweizer Cyberstudie der Mobiliar. Alle drei Studien zeichnen ein umfassendes Bild davon, in welcher Position sich Unternehmen aktuell befinden, welche potenziellen Gefahren sie identifizieren und wie sie auf aktuelle Herausforderungen reagieren.

Die TÜV-Studie kommt zu dem Ergebnis, dass Cybersicherheit für drei von vier Unternehmen in Deutschland von hoher Bedeutung ist. Dieser Aspekt ist insbesondere bei Grossunternehmen spür- und sichtbar. Deloitte betont weiter die Rolle von Governance und des CISO: Unternehmen mit klar verankerten Strukturen sind deutlich resilienter gegenüber den Gefahren aus dem Internet. Beide Studien zeigen, dass kleine und mittlere Unternehmen (KMU) im Bereich der Cybersicherheit Nachholbedarf haben. Die Situation in der Schweiz ist vergleichbar. Laut der Mobiliar-Studie fühlen sich 43 Prozent der befragten Unternehmen zwar unsicher, sehen jedoch nur ein geringes Risiko eines erfolgreichen Cyberangriffs innerhalb der nächsten zwei bis drei Jahre, der den Betrieb mindestens einen Tag ausser Kraft setzt.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

Erfolgreiche Angriffe und deren Folgen

Gemäss der TÜV-Studie werden organisierte Kriminalität (55 Prozent) und staatliche Hacker (47 Prozent) als Hauptbedrohungen identifiziert. Deloitte ergänzt, dass hybride Angriffe – also die Kombination von Cyberattacken mit Desinformationskampagnen – stark zunehmen. Deloitte betont zudem die zunehmende Professionalisierung der Angreifer, die sich immer stärker wie wirtschaftlich agierende Unternehmen organisieren. In allen drei Studien spielen Phishing und Ransomware die Hauptrolle, während andere Angriffsarten wie Insider-Bedrohungen eher unterschätzt werden.

Der TÜV hat in der Studie festgehalten, dass 15 Prozent der Unternehmen in den letzten zwölf Monaten Opfer erfolgreicher Angriffe geworden sind. Tendenz langsam, aber steigend. Deloitte weist zudem darauf hin, dass die finanziellen und regulatorischen Folgen oft unterschätzt werden. Nicht der unmittelbare Schaden, sondern der Reputationsverlust oder auch Bussen können langfristig entscheidend sein. In der Schweiz zeigt sich ein ähnliches Bild: Nur wenige KMU verfügen über Notfallpläne, sodass Angriffe schnell existenzbedrohend werden können.

KI: Gefahr und Verteidigungsinstrument

Laut der TÜV-Studie erfolgte jeder zehnte Angriff über Zulieferer. Deloitte warnt vor systemischen Risiken in komplexen Lieferketten. Zwar werden von den angefragten Unternehmen entsprechende Anforderungen formuliert, doch diese werden selten überprüft. In der Schweiz tritt dieses Thema weniger prominent auf, dennoch stellen gerade ausgelagerte IT-Dienstleistungen einen Schwachpunkt dar. Der gemeinsame Nenner ist: Ohne klare Regeln und vor allem ohne regelmässig durchgeführte Audits bleibt die Lieferkette ein erhebliches Risiko.

Laut TÜV geht mehr als die Hälfte der deutschen Unternehmen davon aus, dass Angreifer bereits KI einsetzen und für Angriffe nutzen. Deloitte warnt zusätzlich vor «AI-as-a-Service», das auch unerfahrenen Kriminellen mächtige Werkzeuge an die Hand gibt. Die Mobiliar betont, dass Phishing-Angriffe in Schweizerdeutsch mittlerweile ebenfalls von KI erstellt werden.

Auf der anderen Seite setzen laut den Studien jedoch nur wenige Unternehmen KI gezielt zur Abwehr ein. Deloitte betont daher die Chancen: KI kann nicht nur zur Angriffserkennung, sondern auch für automatisierte Incident Response und zur Vorhersage möglicher Angriffe eingesetzt werden.

Massnahmen zur Verbesserung: Anspruch und Wirklichkeit

Die TÜV-Studie zeigt, dass viele Unternehmen ihre eigene Sicherheit als «gut» einschätzen, jedoch nur selten praxisnahe Tests, wie beispielsweise Penetrationstests oder Notfallübungen, durchführen. Deloitte ergänzt, dass Investitionen oft auf Technik fokussiert sind, während Mensch und Prozesse zu kurz kommen. In der Schweiz bestätigt sich dieses Bild: Backups und Firewalls sind weit verbreitet, doch Notfallpläne und Security-Awareness-Programme fehlen häufig. Die Mobiliar schreibt dazu, dass IT-Dienstleister das Risiko eines Cyberangriffs für

Links zu den Studien

- https://www.tuev-verband.de/fileadmin/user_upload/Content_local/Studien_local/2025_TUEV-Verband_Cybersecurity-Studie_Studienbericht.pdf
- https://www.mobiliar.ch/studie/cybersicherheit-schweiz
- https://www.deloitte.com/at/de/services/risk-advisory/research/deloitte-cyber-security-report.html

Schweizer KMU deutlich höher einschätzen als die Unternehmen selbst (68 Prozent gegenüber 12 Prozent). Dies zeigt eine grosse Diskrepanz zwischen der eigenen Selbstwahrnehmung und der Einschätzung externer IT-Fachleute.

Der TÜV warnt vor «Geräteleichen» und privaten Endgeräten. Deloitte weitet diesen Aspekt auf Cloud-Umgebungen aus. Demnach sind Fehlkonfigurationen und mangelnde Transparenz in Multi-Cloud-Setups eine der häufigsten Ursachen für Sicherheitsvorfälle. In der Schweiz richtet sich die Aufmerksamkeit stärker auf die klassischen KMU-Strukturen, in denen private Geräte und einfache Passwortpraktiken weiterhin weit verbreitet sind.

Normen, Standards und Regulierung

Der TÜV betont die Bedeutung von Standards wie ISO 27001, jedoch wird von den Unternehmen der hohe Aufwand und die damit verbundenen Kosten bemängelt. Deloitte verweist zusätzlich auf das NIST-Framework und Zero-Trust-Architekturen, die oft nur teilweise umgesetzt werden. In beiden Berichten wird die europäische NIS2-Richtlinie als grosser Treiber genannt. Auffällig ist jedoch, dass laut TÜV nur die Hälfte der deutschen Unternehmen die Richtlinie kennt. Deloitte unterstreicht dies und zeigt, dass internationale Konzerne deutlich besser auf die regulatorischen Vorgaben vorbereitet sind als KMU.

Aus den Erkenntnissen der TÜV-, Deloitte- und Mobiliar-Studie ergeben sich folgende Handlungsempfehlungen:

1. Governance stärken: Cybersicherheit muss Chefsache sein, mit klarer Verantwortung (zum Beispiel mit dem Einsatz eines CISO).
2. Awareness fördern: Mitarbeitende regelmässig schulen und Sicherheitskultur etablieren.
3. Notfallpläne entwickeln: Incident-Response- und Business-Continuity-Pläne erstellen und regelmässig üben.
4. Technik konsequent einsetzen: Backups, Firewalls und KI-gestützte Tools nutzen, Assets sauber erfassen und aktuell halten.
5. Lieferkette absichern: Anforderungen an Partner formulieren und durch Audits überprüfen.
6. Standards und Regulierung umsetzen: ISO 27001, NIS2 oder den IKT-Minimalstandard nicht nur kennen, sondern aktiv implementieren.

Fazit

Alle drei Studien zeichnen ein ähnliches Bild: Das Bewusstsein für Cybersicherheit wächst, doch die Umsetzung hinkt hinterher – insbesondere bei KMU. Während deutsche und internationale Reports den Fokus auf Governance, wirtschaftliche Folgen und Technologie legen, zeigt die Schweizer Studie deutlicher, mit welchen Problemen kleine Unternehmen in der Praxis zu kämpfen haben. Die Handlungsempfehlungen sind universell gültig: Wer Cybersicherheit nicht nur technisch, sondern auch organisatorisch und kulturell verankert, schafft eine erhöhte Resilienz gegenüber den zunehmend professionelleren Angriffen aus dem Internet.