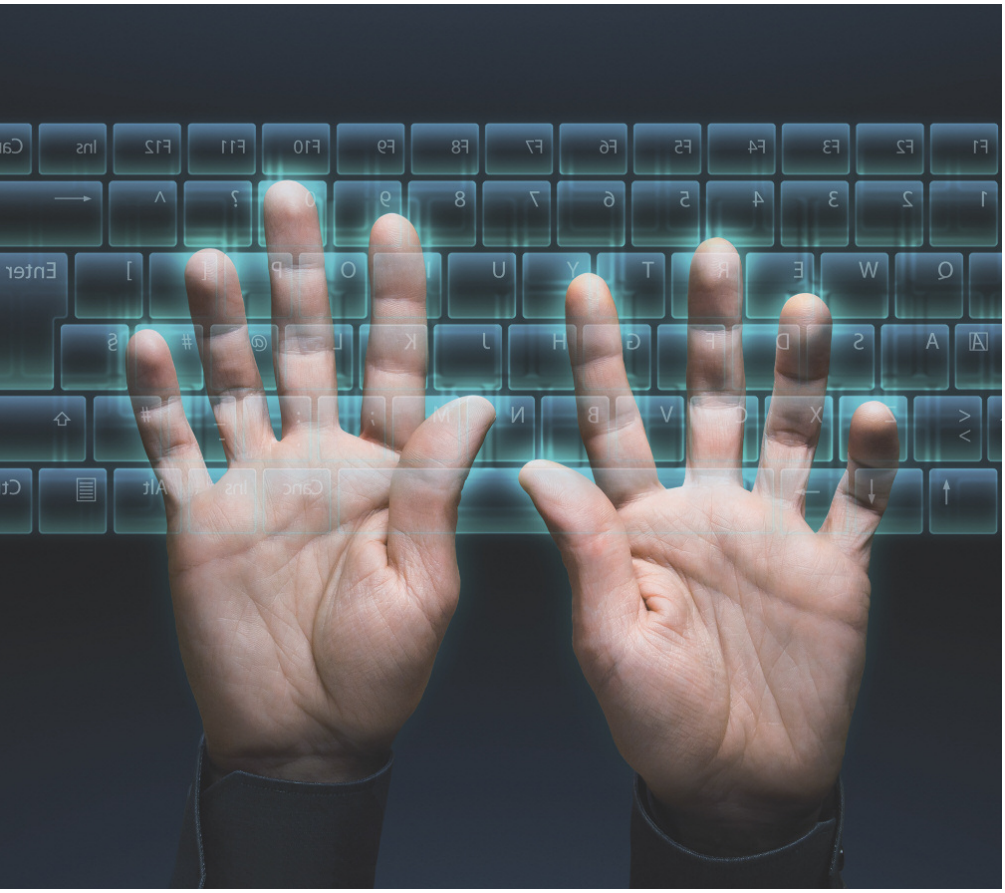
CYBERCRIME: DATENKLAU IN UNTERNEHMEN



Die Bedrohung durch Cyberkriminalität ist in den letzten Jahren dramatisch gewachsen. Die Bedrohung geht zunehmend von professionell aufgestellten, technisch versierten und hochgradig wirtschaftlich orientierten Personen aus. Diese organisieren sich oft in Gruppen und werden immer häufiger von Staaten oder dem Organisierten Verbrechen unterstützt. Was diese Angreifer für Schäden verursachen, bleibt vielen Unternehmen häufig lange verborgen – wenn Angriffe und ihre Folgen überhaupt aufgedeckt werden.

In der Regel verfolgt Cyberkriminalität das Ziel, Wissen, zum Beispiel im Zusammenhang mit Industriespionage oder Konkurrenzausspähung aus Unternehmen zu stehlen. In der Studie „Geschützt vor Datenklau" geht Bodo Meseke, Partner, Assurance - Fraud Investigation & Dispute Services Lead Partner Forensic Technology & Discovery Services Germany Forensic Technology & Discovery Services EMEIA Cyber Investigation Leader Expert Witness in IT-Security & IT-Forensics bei Ernst & Young, unter anderem der Frage nach, wie Unternehmen diese, in dieser digitalen Form vergleichsweise jungen Gefahrenmomente einschätzen, was sie gegen Datenklau und Industriespionage tun und wie sie sich dagegen schützen. Das Ergebnis zeigt ein alarmierendes Bild: Nach wie vor wird die Risikowahrnehmung der deutschen Manager dem vorherrschenden Bedrohungspotenzial nicht gerecht! Dabei können die Folgen von Datenklau und Industriespionage existenzbedrohend sein: Verlust von Technologieführerschaft, Produktionsausfälle, verloren gegangene Ausschreibungen oder auch die Schadenersatzhaftung von Führungskräften. Gerade in der deutschen Wirtschaft lautet der große Erfolgsfaktor Wissen. Entsprechend geschützt wird dieses Wissen aber im seltensten Fall.

Gefahrenbewusstsein zu gering

Aktuellen Enthüllungen und der veränderten Informationslage zum Trotz: Weiterhin sorgen sich aktuell zu wenig deutsche Manager um die Gefahren durch Datenklau und Cyberangriffe. Öffentlichkeitswirksame Warnsignale gab es bereits reichlich – spätestens seit der erfolgreichen Attacke auf das IT-Netz des Deutschen Bundestags. Trotz der Gelassenheit erwarten allerdings acht von zehn Managern, dass die Bedeutung künftig zunehmen wird.

Großunternehmen und Finanzbranche besonders risikobewusst

Großunternehmen mit Jahresumsätzen von mehr als 1 Mrd. Euro schätzen das Risiko, Opfer von Cyberangriffen zu werden, als eher sehr hoch ein. Kleine und mittlere Unternehmen sind deutlich weniger risikobewusst. Dabei befürchten Unternehmen in Deutschland laut Studie vor allem, Opfer von organisiertem Verbrechen, ausländischen Geheimdiensten / staatlichen ausländischen Stellen oder Hacktivisten zu werden.

Attacken aus Russland und China

Die Sorge vor Attacken aus China und Russland nimmt damit stark zu – auch die USA werden vermehrt gefürchtet. Russland ist in den letzten zwei Jahren verstärkt in den Fokus gerückt: Das Land wird heute fast dreimal so oft als Risikoherd genannt wie noch vor zwei Jahren. Das Gefahrenbewusstsein

gegenüber den USA hat hingegen nur vergleichsweise schwach zugenommen.

Zahl der entdeckten Attacken gestiegen

14 Prozent der befragten Unternehmen haben in den vergangenen drei Jahren konkrete Hinweise auf Spionageattacken und /oder Datenklau entdeckt, das sind immerhin doppelt so viele wie noch vor zwei Jahren. Aber Achtung, die Dunkelziffer dürfte beim Datenklau sehr hoch sein. In der Umsatzklasse ab einer Milliarde Euro hat in den vergangenen drei Jahren jedes fünfte Unternehmen einen Angriff auf die eigenen Daten erlebt, 18 Prozent waren sogar mehrfach betroffen. In der darunterliegenden Umsatzklasse ab 50 Millionen Euro können immerhin 16 Prozent von entsprechenden Erfahrungen berichten. Lediglich zehn Prozent der Unternehmen mit bis zu 50 Millionen Euro Umsatz haben Hinweise auf Spionage oder Datenklau entdeckt.

Der Befund im Hinblick auf die vorherigen Feststellungen ist also eindeutig: Da mit der Unternehmensgröße auch die Sensibilität für unternehmerische Risiken wächst und damit einhergehend mehr in Schutzmechanismen investiert wird, decken größere Firmen Angriffe eher auf.

Finanz- und Energie Sektor sind besonders betroffen

Unternehmen sind unterschiedlich stark vom Datenklau betroffen – je nach Größe und Branche. So werden Unternehmen der Energie- und der Finanzbranche am häufigsten Opfer attackiert. In drei von vier Fällen handelte es sich bei den Attacken um Hackerangriffe auf die EDV-Systeme, oft wurden IT-Systeme vorsätzlich lahmgelegt. Deutlich seltener wurden Kunden oder Arbeitnehmerdaten ausgespäht. In den meisten Fällen ließ sich der Täter nicht zuordnen, er blieb unerkannt. Fast jeder zweite Spionagefall bleibt unaufgeklärt.

Tatort Vertrieb

Die mit Abstand meisten Attacken gab es in den vergangenen drei Jahren im Vertrieb: Mehr als jeder dritte Betroffene berichtet von Angriffen auf diese Abteilung. Auch die Personalabteilung ist in den Unternehmen eine besonders heikle Stelle, gefolgt von Management und Geschäftsleitung. Diese Befunde überraschen nicht: Liegen doch in Vertrieb, Personalabteilung und der Führungsetage die sensibelsten und damit für Angreifer die wertvollsten Unternehmens- und Mitarbeiterdaten. „Ein Sicherheitssystem, das lediglich auf die herkömmlichen Schutzmaßnahmen setzt, öffnet Hackern bereitwillig die Tore!" so Bodo Meseke.

Interne Kontrolleinrichtungen bringen Angriffe ans Licht

In der Hälfte der Fälle half ein internes Kontrollsystem bei der Aufdeckung der Spionageangriffe und/oder von Datenklau. Dabei ist bemerkenswert, dass trotz interner Kontrollmechanismen und staatlicher Aktivitäten jeder fünfte Angriff rein zufällig bekannt wird. 53 Prozent der entdeckten, kriminellen Handlungen kamen durch ein internes Kontrollsystem ans Licht. In 21 Prozent der Fälle half der Zufall und bei 19 Prozent waren es interne Routineprüfungen. Hinter drei von zehn Angriffen steckt der Wunsch, sich einen Wettbewerbsvorteil zu verschaffen. Genauso viele Angriffe zielen auf die Schaffung eines finanziellen Vorteils ab.

Firewall, Passwörter, Antiviren-Programme

Unternehmen setzen vor allem auf einfache Sicherheitsvorkehrungen. Jeweils mehr als 80 Prozent der befragten Unternehmen der Studie setzen zur Vorbeugung von Ausspähungsattacken weiter nur auf Firewalls, Antivirensoftware und gute Passwörter Umfassendere Schutzvorkehrungen sind in den Unternehmen oft Mangelware: Ein Intrusion-Detection- bzw. Prevention System, das Hinweise auf die Aktivitäten von Eindringlingen geben kann, leisten sich immer noch nur 30 Prozent der Unternehmen der befragten Unternehmen. Umfassendere Maßnahmen wie die vollumfängliche Aufklärung von Cybervorfällen und Krisensimulationen von Angriffsszenarien sind nur von wenigen geplant.

Die anhaltende Sorglosigkeit vieler Unternehmen überrascht. Viele denken, sie seien ausreichend geschützt oder würden kein Ziel für Datenklau und Cyberangriffe darstellen. Dabei zeigen Enthüllungen immer wieder, dass so gut wie jedes Unternehmen Ziel solcher Attacken werden kann und sich die gängigen Schutzmechanismen häufig umgehen lassen. Wird ein Unternehmen Opfer einer Cyberattacke, heißt es, schnell und reaktiv zu handeln. Unterbleiben Konsequenzen, kann die Sicherheitslücke ein Einfallstor für weitere Angriffe bieten. Gerade große und namhafte Unternehmen sind durch Datenklau und Industriespionage massiv gefährdet. Es dürfte kaum einen deutschen Top-Konzern geben, der nicht schon Opfer einer Cyberattacke wurde. Deshalb stellt sich nicht nur die Frage, wie sich solche Attacken abwehren lassen. Genauso wichtig sind Strategien zur richtigen Reaktion in derartigen Fällen. Wird ein Angriff bemerkt, kommt es auf die schnellstmögliches Handeln an. Nur so lassen sich weitere Schäden vermeiden. Dabei ist anzunehmen, dass viele Angriffe nur deshalb unbemerkt bleiben, weil die Sicherheitssysteme den Angriff nicht entdecken. Oft fällt der Schaden erst dann auf, wenn es schon zu spät ist; wenn sensible Daten an anderer – beziehungsweise falscher – Stelle wieder auftauchen. In einer immer enger vernetzten Welt ist völlige Sicherheit ohnehin nicht zu gewährleisten. Umso wichtiger ist es, Datendieben den Zugriff auf wichtige Informationen so schwer wie möglich und damit unattraktiv zu machen.

> ***„Ein Sicherheitssystem, das lediglich auf die herkömmlichen Schutzmaßnahmen setzt, öffnet Hackern bereitwillig die Tore!"***
>
> **Bodo Meseke**
> **Partner bei Ernst & Young.**

Die gesamte Studie von Ernst & Young „Datenklau, virtuelle Gefahr und echte Schäden!" finden Sie hier im Download.

Manuela Micheli-Liebsch