Geschützt vor Datenklau

Leichte Beute

Datenklau – die neue Herausforderung für Unternehmen

„Ein Sicherheitssystem, das lediglich auf die herkömmlichen Schutzmaßnahmen setzt, öffnet Hackern bereitwillig die Tore!"

Inhaltsverzeichnis

Bodo Meseke
Partner
Leader Forensic Technology & Discovery Services/
EMEIA Central Zone
Business Integrity & Corporate Compliance

Vorwort |

Die Bedrohung durch Cyberkriminalität ist in den letzten Jahren dramatisch gewachsen. Schon längst haben es Unternehmen nicht mehr nur mit „Script Kiddies" zu tun, die Schwachstellen in Sicherheitssystemen aus eher banalen Gründen ausnutzen.

Vielmehr hat sich die Typologie der Angreifer im Cyberspace gewandelt. Heute geht die Bedrohung meist von professionell aufgestellten, technisch versierten und hochgradig wirtschaftlich orientierten Personen aus. Diese organisieren sich oftmals 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 den meisten Fällen verfolgt Cyberkriminalität das Ziel, Wissen, zum Beispiel im Zusammenhang mit Industriespionage (staatlich getrieben) oder Konkurrenzausspähung (durch ein anderes Unternehmen), aus Unternehmen zu stehlen.

Wie schätzen Unternehmen diese – in dieser digitalen Form – vergleichsweise jungen Gefahrenmomente ein?

Welche Branchen sind besonders gefährdet?

Was tun die Unternehmen schon heute gegen Datenklau und Industriespionage?

Wie wollen sie sich in Zukunft schützen?

All das sind Fragen, denen wir mit der vorliegenden Studie auf den Grund gehen wollen. Ihre Befunde deuten in eine klare Richtung: 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.

Kernaussagen
der Studie im Überblick

Immer häufiger werden deutsche Unternehmen Opfer von Datenklau-Attacken. Das Risiko wird aber weiterhin unterschätzt.

Jedes fünfte Großunternehmen war in den letzten drei Jahren Opfer von Spionage oder Datenklau – Tendenz steigend.

Die Dunkelziffer dürfte weit höher sein: In **jedem fünften** Unternehmen wurden die kriminellen Handlungen nur durch Zufall entdeckt.

Lediglich ein Drittel der deutschen Unternehmen sieht ein hohes Risiko.

Großunternehmen sowie die Energie- und Finanzbranche werden **besonders häufig attackiert**.

Besonders häufig ins Visier von Datendieben geraten Unternehmen mit mehr als einer Milliarde Euro Umsatz: Von ihnen hat **jedes fünfte** bereits konkrete Attacken festgestellt.

Sieben Prozent der deutschen Unternehmen haben sogar mehrfach Hinweise auf Spionage beziehungsweise Datenklau entdeckt.

Nach Meinung von knapp der Hälfte der Manager **(46 Prozent)** geht die größte Gefahr von China aus, Russland rückt zunehmend in den Fokus.

Umfassendere Schutzmaßnahmen, wie die vollumfängliche Aufklärung von Cybervorfällen und die Simulation von Angriffsszenarien, beabsichtigt nur **jedes fünfte Unternehmen**.

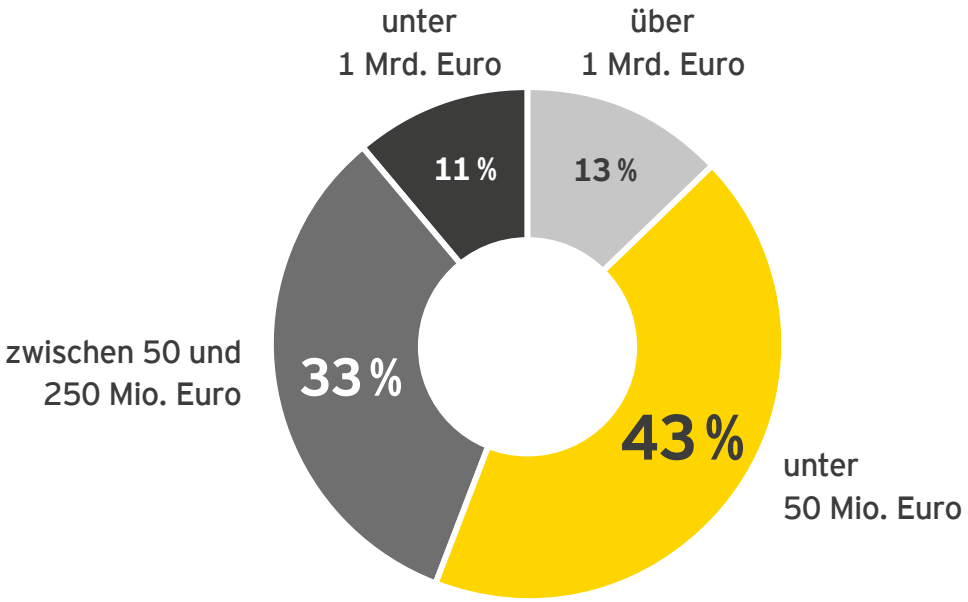
Studiendesign

Die vorliegende Studie fasst die Ergebnisse einer repräsentativen telefonischen Befragung von insgesamt 450 Geschäftsführern sowie Führungskräften aus den Bereichen IT-Sicherheit und Datenschutz deutscher Unternehmen zusammen.

Befragt wurden dabei unter anderem Geschäftsführer, Leiter Konzernsicherheit oder Leiter IT-Sicherheit von Unternehmen verschiedener Größen, gemessen an Mitarbeiterzahl und Umsatzstärke (s. Abbildung).

Die Befragung wurde von einem unabhängigen Marktforschungsinstitut (Valid Research, Bielefeld) im Mai/Juni 2015 durchgeführt.

Umsatzverteilung der befragten Unternehmen:



Datenklau und Spionage – im toten Winkel der Gefahren-wahrnehmung?

Wie hoch schätzen die Unternehmen die eigene Gefährdung ein?

Wie entwickeln sich Risiken in Zukunft?

Welche Unternehmen sind besonders betroffen und warum?

Gefahrenbewusstsein nur leicht gestiegen

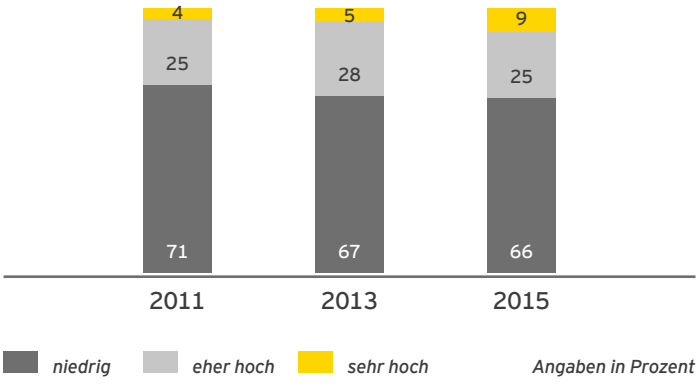
Aktuellen Enthüllungen und der veränderten Informationslage zum Trotz: Weiterhin macht sich nur eine Minderheit der deutschen Manager Sorgen um die Gefahren durch Datenklau und Cyberangriffe.

So bewertet nur jeder dritte Befragte das Risiko für das eigene Unternehmen, Opfer von Spionage und Cyberangriffen zu werden, als hoch.

Gegenüber 2013 ist das Gefahrenbewusstsein damit nur geringfügig gestiegen.

Dabei wäre ein stärkeres Gefahrenbewusstsein absolut nachvollziehbar. Öffentlichkeitswirksame Warnsignale gab es bereits reichlich – spätestens seit eine groß angelegte und erfolgreiche Attacke auf das IT-Netz des Deutschen Bundestags bekannt geworden ist.

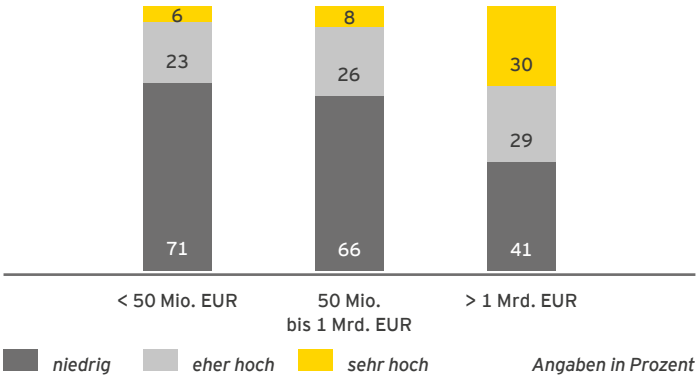
Wie hoch schätzen Sie das Risiko für Ihr Unternehmen ein, Opfer von Cyberangriffen/Datenklau zu werden?



Großunternehmen und Finanzbranche besonders risikobewusst

Mehr als jedes zweite Großunternehmen (59 Prozent) mit Jahresumsätzen von mehr als 1 Mrd. Euro schätzt das Risiko, Opfer von Cyberangriffen zu werden, als eher sehr hoch ein. Deutlich weniger risikobewusst zeigen sich kleine und mittlere Unternehmen: Hier liegt der Anteil bei nur 29 bzw. 34 Prozent.

Wie hoch schätzen Sie das Risiko für Ihr Unternehmen ein, Opfer von Cyberangriffen/Datenklau zu werden?



Besonders gefahrenbewusst ist die Finanzbranche, wo fast jedes zweite Institut das Risiko eines Angriffs als hoch bewertet, gefolgt von Energieunternehmen und produzierende Industrie.

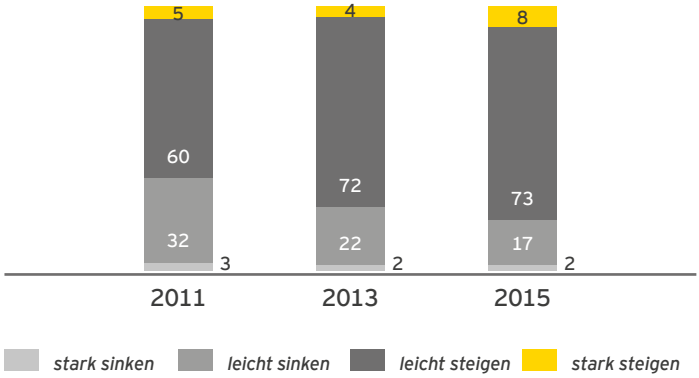
Anteil „hoch" 2015	
Finanzbranche	48
Energie	39
Industrie	37
Handel und Konsumgüter	28
Sonstige Dienstleistungen	24
Sonstige	36

Unternehmen erwarten eine Verschärfung des Problems

Bei aller Gelassenheit: Für die Zukunft erwarten die Manager, dass die Bedeutung des Risikofeldes rund um Datenklau und Cyberangriffe zunehmen wird.

So gehen etwa acht von zehn Managern (81 Prozent) von einer wachsenden Bedrohung aus dem Netz aus – das sind etwas mehr als noch vor zwei Jahren. Zum Vergleich: Damals waren es 76 Prozent.

Was meinen Sie, wie wird sich die Bedeutung des Problems Cyberangriffe/Datenklau für Ihr Unternehmen künftig entwickeln?



Risikoprognose branchenübergreifend und unabhängig von Größe

Die große Mehrheit der Unternehmen rechnet mit einer sich zukünftig verschärfenden Gefahrenlage durch Cyberangriffe – unabhängig von Unternehmensgröße und Branche.

Besonders risikobewusst zeigen sich allerdings erneut Großunternehmen: Hier liegt der Anteil derer, die mit einer Verschärfung des Problems rechnen, mit 14 Prozent doppelt so hoch, wie bei kleinen und mittleren Unternehmen.

Besonders sensibel ist hierbei die Handels- und Konsumgüterindustrie. Hier rechnen 85 Prozent der Führungskräfte mit steigenden Risiken. Gefolgt von der Finanzbranche (84 Prozent) und Industrieunternehmen (83 Prozent).

Anteil „steigen" 2015	
Handel und Konsumgüter	85
Finanzbranche	84
Industrie	83
Sonstige Dienstleistungen	75
Energie	74
Sonstige	69

Spionagegefahr aus dem In- und Ausland

Welche Tätergruppen halten die deutschen Unternehmen für besonders relevant?

Wer führt Cyber-Angriffe durch und warum?

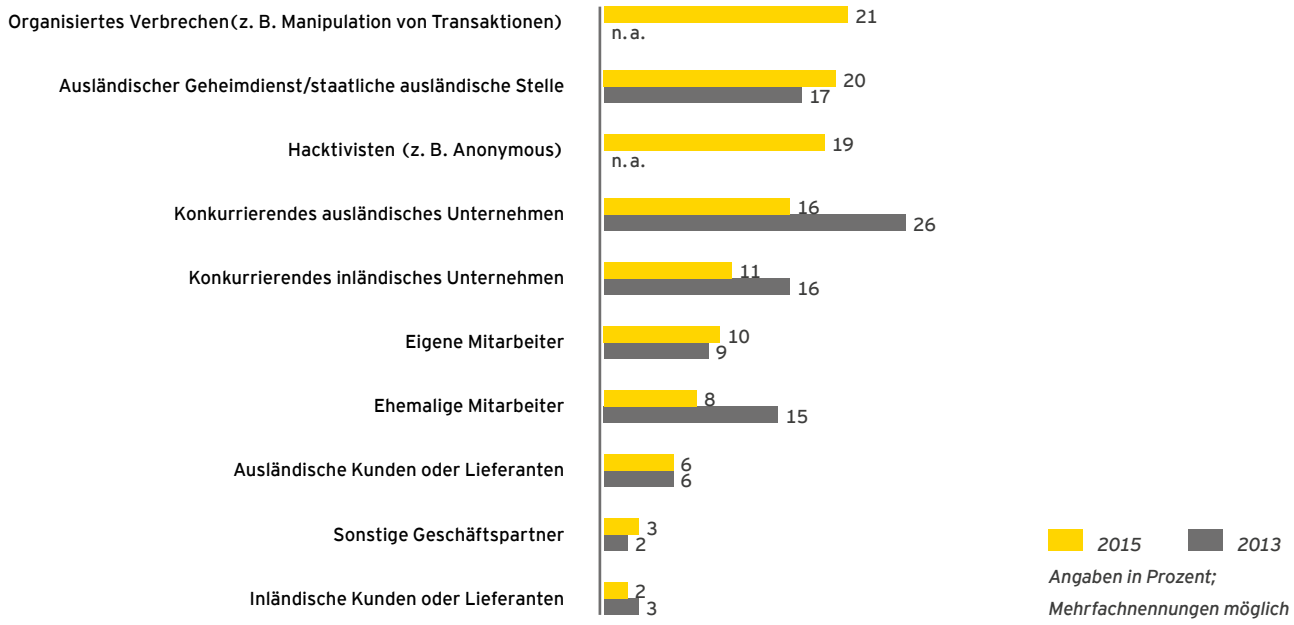
Wo kommen die Angreifer her?

Besonders gefürchtet: Organisiertes Verbrechen, ausländische Geheimdienste und Hacktivisten

Unternehmen in Deutschland befürchten vor allem, Opfer von organisiertem Verbrechen, ausländischen Geheimdiensten/ staatlichen ausländischen Stellen oder Hacktivisten zu werden.

Nur noch jedes sechste Unternehmen sieht hingegen das Risiko eines Angriffs vonseiten ausländischer Unternehmen; vor zwei Jahren war es noch jedes vierte.

Wie bewerten Sie das Risiko, von folgenden Tätergruppen geschädigt zu werden? (Nennungen „großes Risiko" und „sehr großes Risko")



Attacken werden vor allem aus China und Russland erwartet

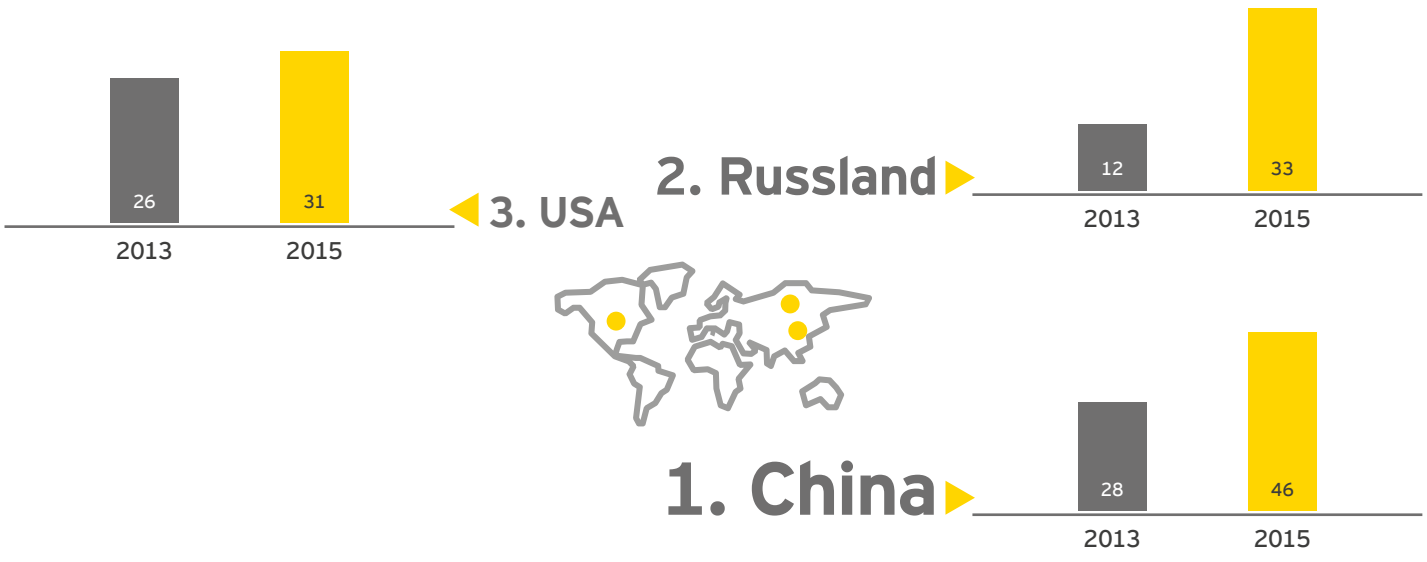
Von einigen Weltregionen aus wird besonders viel Industriespionage betrieben; davon ist heute nur noch knapp jedes zweite Unternehmen überzeugt, deutlich weniger als noch vor zwei Jahren (61 Prozent).

Dabei geht die größte Gefahr aus Sicht der Manager von China aus: 46 Prozent nennen das Land als Region mit dem höchsten Risikopotenzial, dahinter folgen Russland (33 Prozent) und die USA (31 Prozent).

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. Nicht einmal jedes dritte Unternehmen nennt die USA als besonderen Risikoherd.

Regionen mit besonders hohem Gefährdungspotenzial im Vergleich 2013 – 2015



Basis: Unternehmen, die eine Region nennen

Datenklau-Attacken und Aufdeckung im Fokus

Wer sind die Täter? Wer die Opfer?
Wer muss vor Spionage und Datenklau am meisten Angst haben?
Welche Unternehmensbereiche sind besonders gefährdet?
Wie sehen konkrete Erfahrungen aus?

Zahl der entdeckten Attacken gestiegen

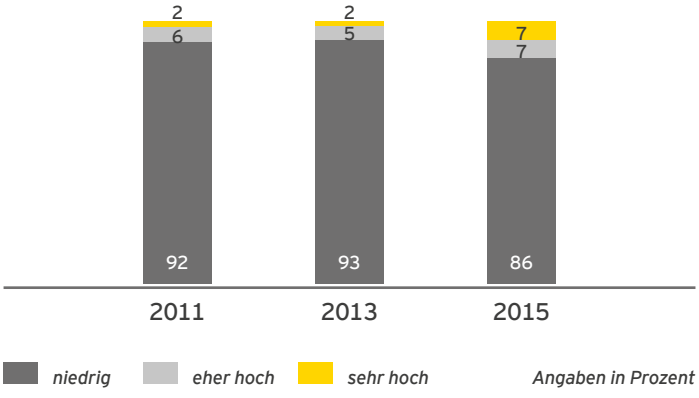
14 Prozent der Unternehmen haben in den vergangenen drei Jahren konkrete Hinweise auf Spionageattacken und/oder Datenklau entdeckt, das sind immerhin doppelt so viele wie noch vor zwei Jahren.

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.

Gab es in Ihrem Unternehmen bereits konkrete Hinweise auf Spionage bzw. einen Datenklauinnerhalb der vergangenen drei Jahre?

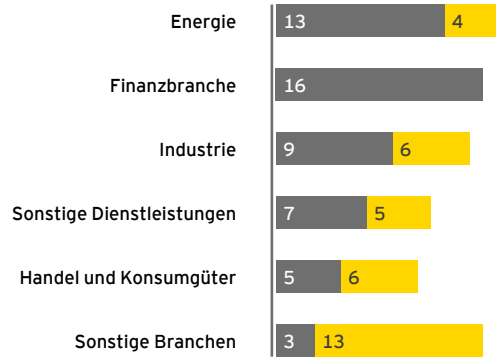


Großunternehmen sowie Finanzbranche und Energiesektor sind besonders betroffen

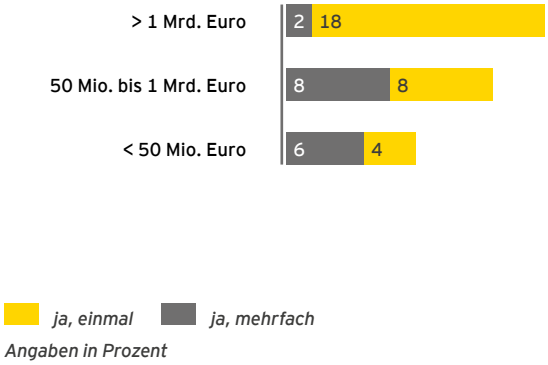
Die Unternehmen sind unterschiedlich stark vom Datenklau betroffen – je nach Größe und Branche. So werden Unternehmen der Energie- und der Finanzbranche am häufigsten Opfer von Spionage und Datenklau: In der Energiebranche geben 17 Prozent an, es habe in den vergangenen drei Jahren konkrete Hinweise auf eine Attacke gegeben, bei vier Prozent sogar mehrfach. In der Finanzbranche geben 16 Prozent an, in den vergangenen drei Jahren mit Spionage und Datenklau zu tun gehabt zu haben – hier waren sogar alle mehrfach betroffen. In der Industrie wurden 15 Prozent der Unternehmen bereits zum Opfer, sechs Prozent mehrfach.

Gab es in Ihrem Unternehmen bereits konkrete Hinweise auf Spionage bzw. einen Datenklauinnerhalb der vergangenen drei Jahre?

Branche



Umsatzklasse



Angaben in Prozent

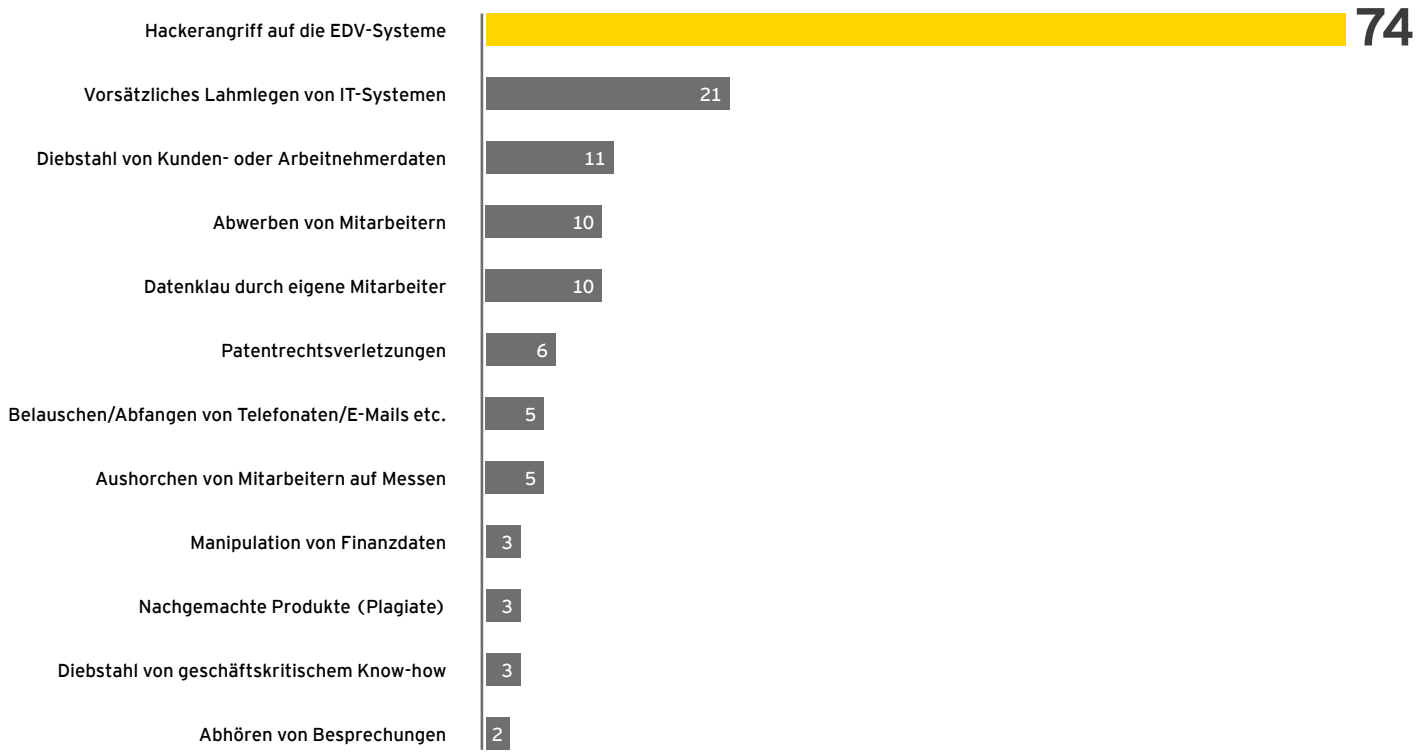
21 % *der Attacken hatten zur Folge, dass das IT-System lahmgelegt wurde*

48 % *der Attacken wurden durchgeführt, ohne dass die Täter identifiziert werden konnten*

Drei von vier Attacken sind Hackerangriffe

In drei von vier Fällen (74 Prozent) handelte es sich bei den Attacken um Hackerangriffe auf die EDV-Systeme, in 21 Prozent wurden IT-Systeme vorsätzlich lahmgelegt. Deutlich seltener wurden Kunden- oder Arbeitnehmerdaten ausgespäht (11 Prozent), Mitarbeiter abgeworben oder Datenklau durch eigene Mitarbeiter begangen (jeweils zehn Prozent). In den meisten Fällen (48 Prozent) ließ sich der Täter nicht zuordnen, er blieb unerkannt. In 18 Prozent der Fälle konnten sogenannte Hacktivisten – also Hackergruppen wie Anonymous – als Täter identifiziert werden. In 15 Prozent der Fälle wurde ein konkurrierendes ausländisches Unternehmen identifiziert, was sich etwa mit den durch die Unternehmen erwarteten 16 Prozent deckt.

Welche konkreten Handlungen fanden statt?



Angaben in Prozent; Basis: Unternehmen, die bereits geschädigt wurden; Mehrfachnennungen möglich

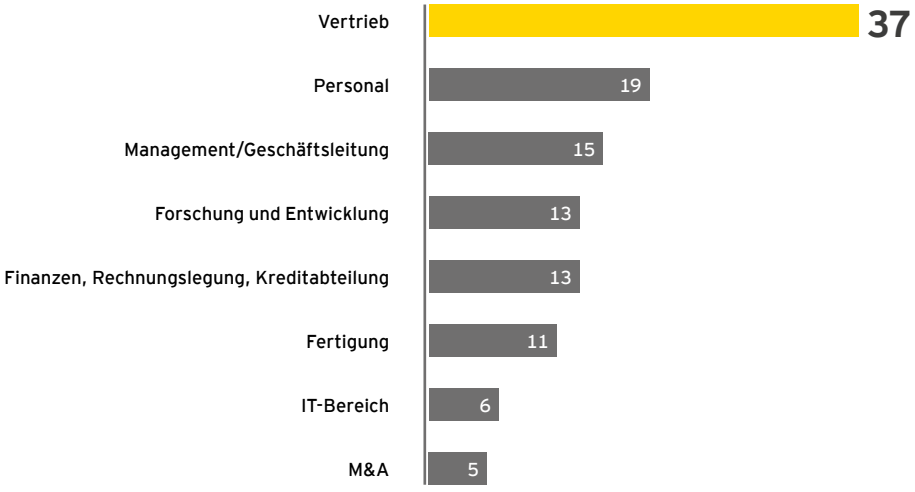
Tatort Vertrieb

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.

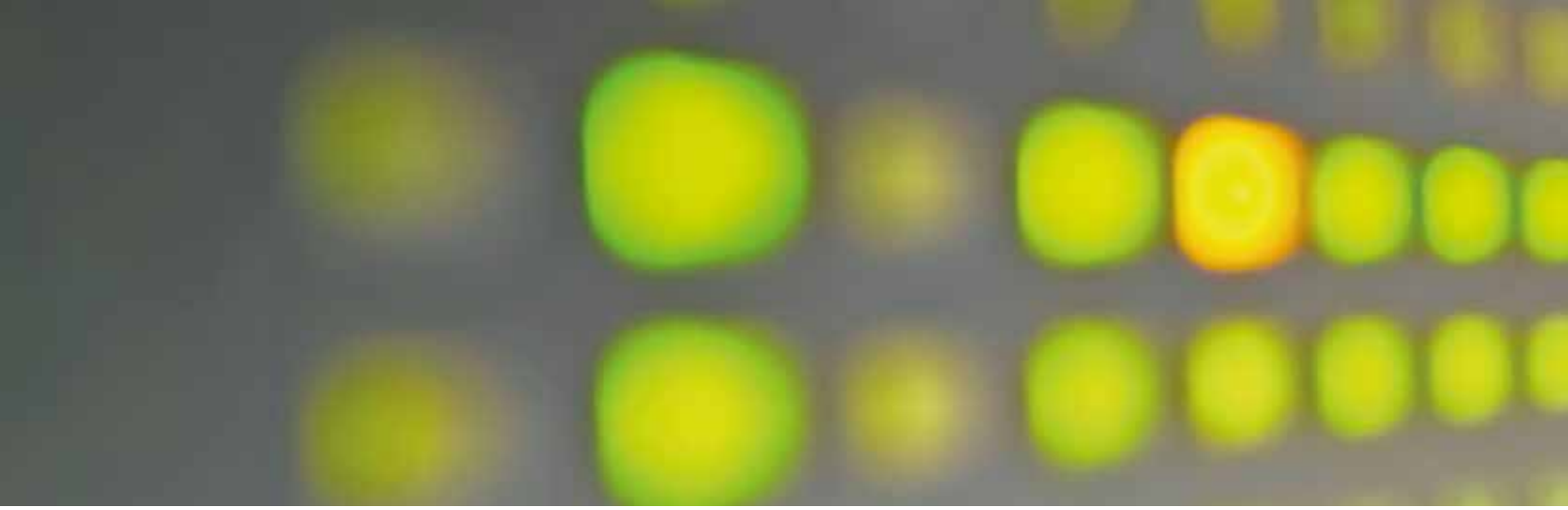
Auch die Personalabteilung ist in den Unternehmen eine besonders heikle Stelle, gefolgt von Management und Geschäftsleitung.

Diese Befunde überraschen nicht: Liegen doch in Vertrieb, Personalabteilung und der Führungsetage die sensibelsten und damit für Angreifer die wertvollsten Unternehmens- und Mitarbeiterdaten.

Welcher Bereich war vom Datenklau betroffen bzw. wo ergab sich dieser Verdacht?



Angaben in Prozent; Basis: Unternehmen, die bereits geschädigt wurden; Mehrfachnennungen möglich



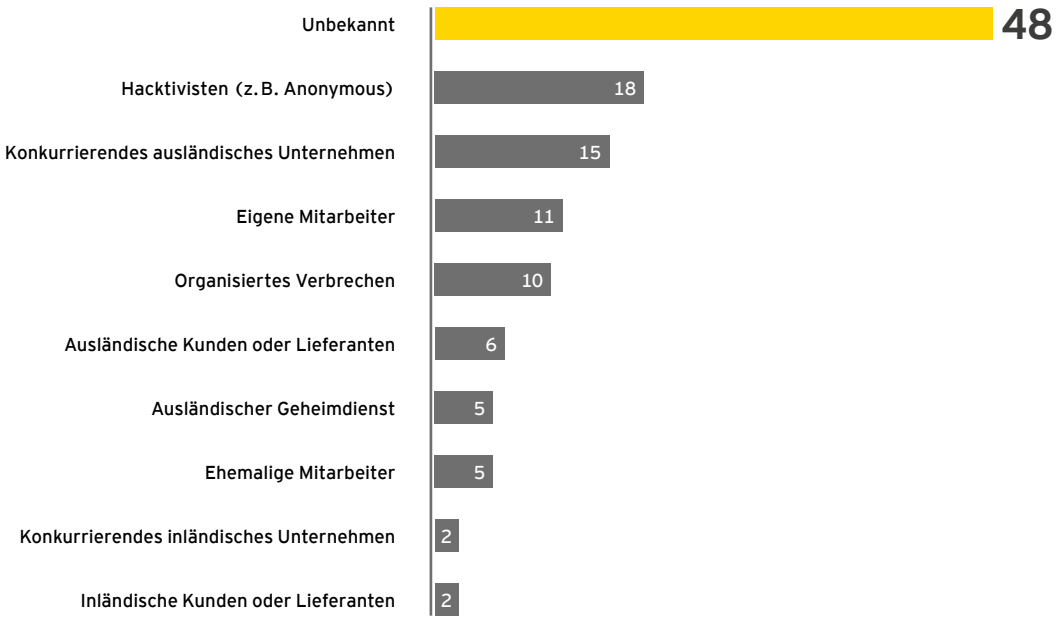
Spione bleiben oft unbekannt

Fast jeder zweite Spionagefall bleibt unaufgeklärt: In 48 Prozent der Fälle ließen sich die Täter nicht ermitteln.

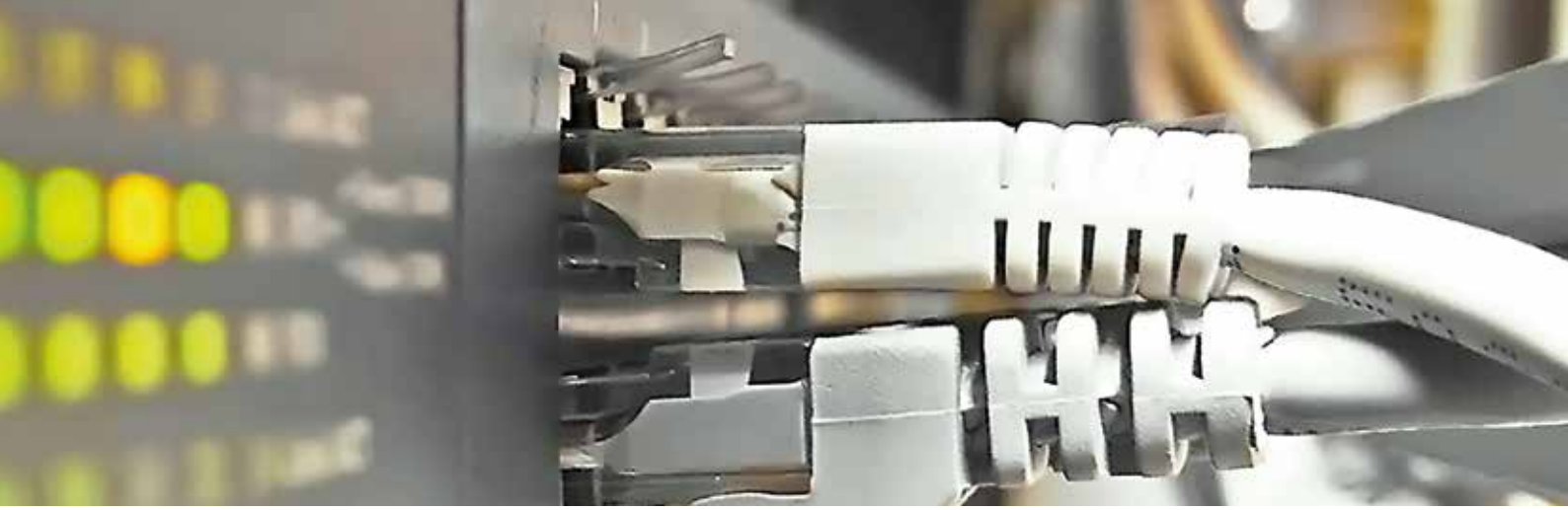
Gut jede sechste Spähattacke geht von Hacktivisten aus, etwas weniger – 15 Prozent – von der ausländischen Konkurrenz.

Eigene Mitarbeiter sind nur in jedem neunten Spionagefall als Täter beteiligt, ehemalige Mitarbeiter in jedem 20. Vorfall.

Von welchem Täterkreis ging die Gefährdung aus?



Angaben in Prozent; Basis: Unternehmen, die bereits geschädigt wurden; Mehrfachnennungen möglich



Jeder zweite Angriff kommt durch das interne Kontrollsystem ans Licht

In gut der Hälfte der Fälle half ein Kontrollsystem des Unternehmens 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. Dort, wo das Kontrollsystem nicht ausreichte oder der Zufall nicht mithalf, blieben demnach viele Angriffe unentdeckt.

Die Dunkelziffer dürfte aber deutlich höher liegen. Gerade kleinere Unternehmen verfügen oft nicht über die entsprechenden Mittel oder das Know-how, um solche Attacken überhaupt aufzuspüren.

IT-Abteilung soll sich um entdeckte Angriffe kümmern

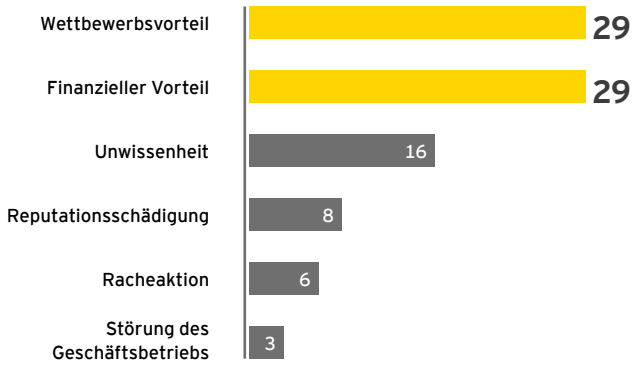
Wird eine Cyberattacke bekannt, dann ist die IT-Abteilung meist die erste Anlaufstelle (69 Prozent). Nur jedes achte Unternehmen wendet sich an externe Dienstleister.

Ein Computer-Emergency-Response-Team wird nur sehr selten bei Fällen von Ausspähung herangezogen.

Wettbewerbs- und finanzielle Vorteile sind die wichtigsten Motive der Ausspähung

Hinter drei von zehn Angriffen steckt der Wunsch, sich einen Wettbewerbsvorteil zu verschaffen. Genauso viele Angriffe zielen auf die Schaffung eines finanziellen Vorteils ab. Immerhin: jeder sechste Angriff geschieht aus Unwissenheit. Racheaktionen und die Störung des Geschäftsbetriebs sind nur von untergeordneter Bedeutung.

Was war die vermutete Motivation des Angriffs?



Angaben in Prozent; Basis: Unternehmen, die bereits geschädigt wurden; Mehrfachnennungen möglich

Prävention und Vorsorge

Schützen sich die Unternehmen ausreichend?

Welche Maßnahmen ergreifen sie bereits heute? Welche sind geplant?

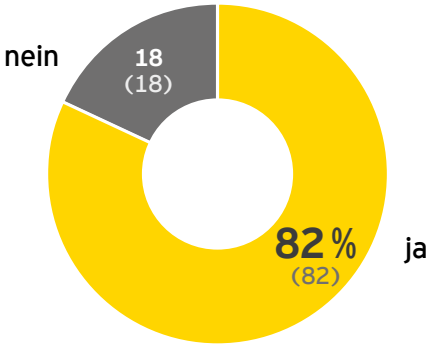
Wie werden Datenklau-Attacken entdeckt und welche Rolle spielt dabei der Zufall?

Acht von zehn Unternehmen fühlen sich vor der Gefahr der Ausspähung sicher

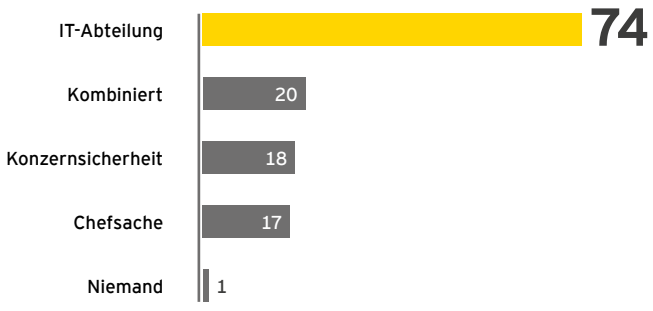
Im Vergleich zur Untersuchung aus dem Jahr 2013 hat sich am Sicherheitsgefühl der Unternehmen nur sehr wenig geändert. Nach wie vor halten 82 Prozent der Manager die präventiven Maßnahmen gegen Datenklau in ihrem Unternehmen für ausreichend.

In den allermeisten Fällen ist die interne IT-Abteilung mit dem Schutz von Unternehmenswerten vor Spionage und Datenklau betreut. Nur 17 Prozent geben an, diese Belange seien reine Chefsache.

Sind aus Ihrer Sicht die präventiven Vorkehrungen im Unternehmen ausreichend,um sich wirkungsvoll gegen Informationsabfluss zu schützen?



Wer kümmert sich im Unternehmen um die zentralen Belange des Schutzes wichtiger Unternehmensassets?



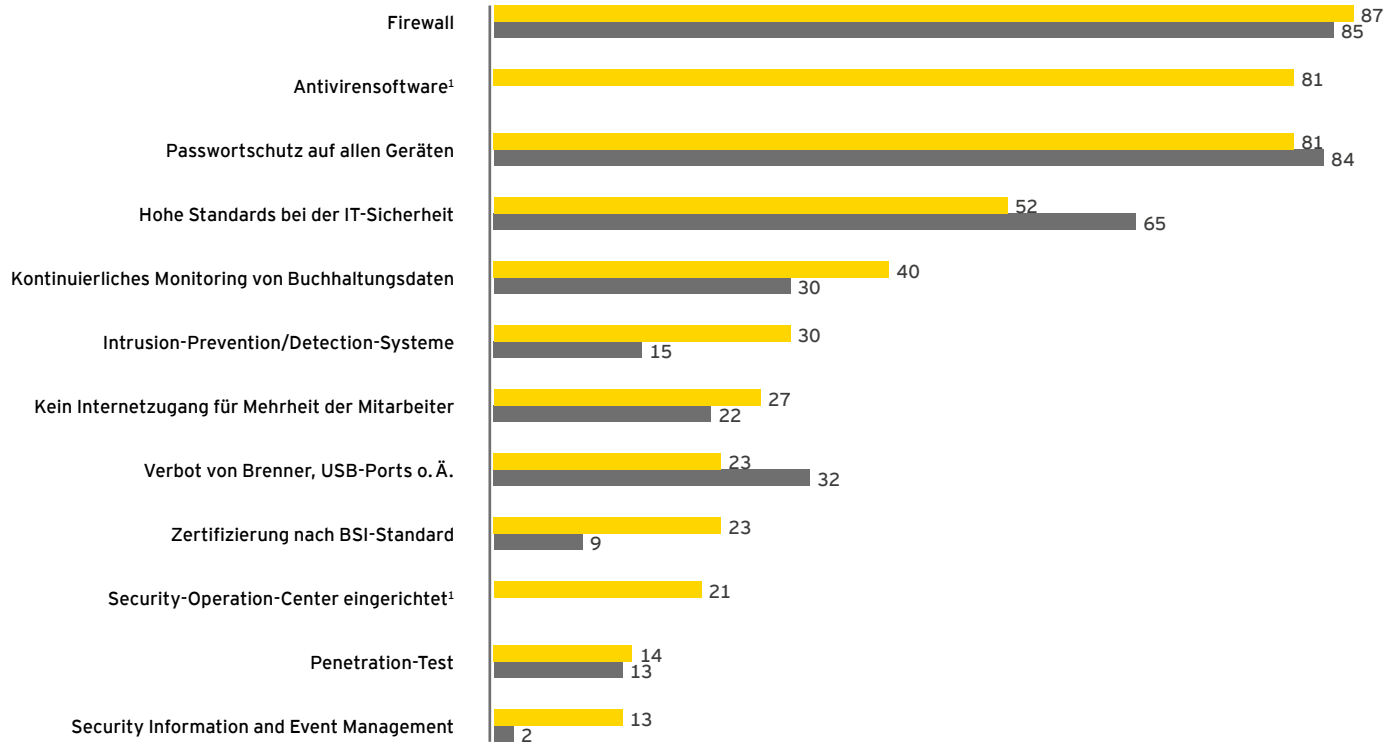
Angaben in Prozent; Werte 2013 in Klammern

Firewall, Antivirenschutz und Passwörter sind Standard

Unternehmen setzen vor allem auf einfache Sicherheitsvorkehrungen. Jeweils mehr als 80 Prozent der befragten Unternehmen setzen zur Vorbeugung von Ausspähungsattacken weiter nur auf Firewalls, Antivirensoftware und gute Passwörter. Allerdings sollen diese Vorkehrungen auch noch andere Aufgaben erfüllen, sie fungieren nicht ausschließlich zur Abwehr von Angriffen.

Umfassendere Schutzvorkehrungen sind in den Unternehmen hingegen 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, damit aber immerhin doppelt so viele wie noch 2013.

Welche Sicherheitsvorkehrungen haben Sie im IT-Bereich getroffen, um sich gegen Spionage/Informationsabfluss zu schützen?



Angaben in Prozent; Mehrfachnennungen möglich

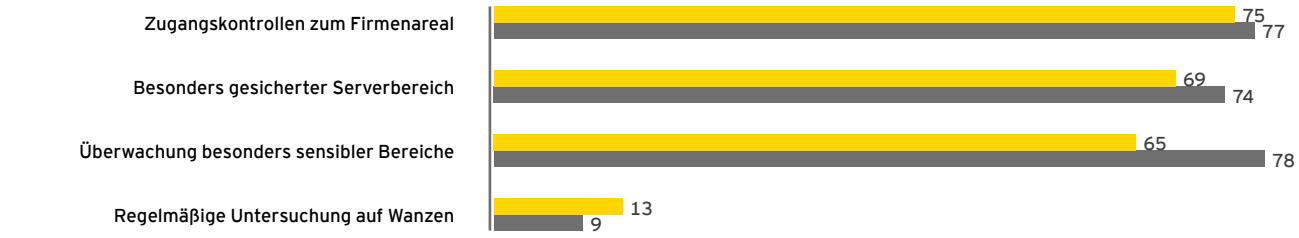
[1] keine Vorjahreswerte

Objektschutzvorkehrungen wurden in den vergangenen zwei Jahren eher abgebaut

Seit der letzten Befragung im Jahr 2013 wurden die Sicherheitsvorkehrungen der Unternehmen im Bereich Objektsicherheit eher zurückgefahren.

Immerhin: Der Anteil der Unternehmen, die regelmäßige Untersuchungen auf Abhöreinrichtungen durchführen, ist leicht gestiegen.

Welche Sicherheitsvorkehrungen haben Sie im Bereich Objektsicherheit getroffen?



Angaben in Prozent; Mehrfachnennungen möglich

84 % *der Unternehmen setzen auf Geheimhaltungsverpflichtungen in Arbeitsverträgen*

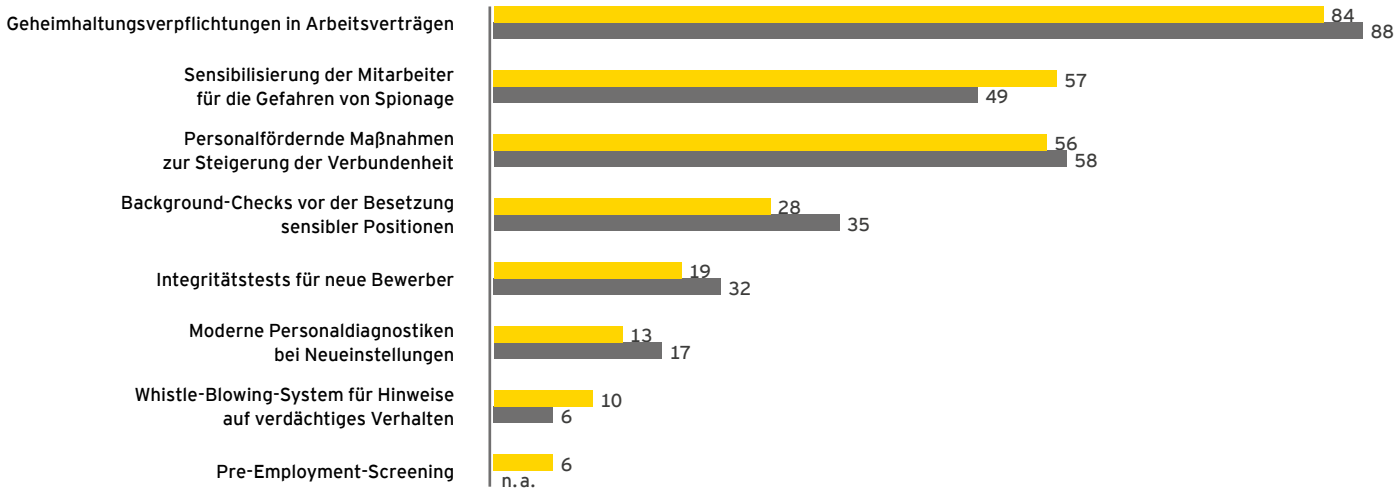
57 % *der Unternehmen sensibilisieren ihre Mitarbeiter für die Gefahren von Spionage*

Geheimhaltungsverpflichtungen an der Tagesordnung

Um sich vor Datenklau durch Mitarbeiter zu schützen, setzen die meisten Unternehmen auf Geheimhaltungsvereinbarungen, Sensibilisierung für die Gefahren der Spionage und pflegen die Verbindung zu den Mitarbeitern.

Whistle-Blowing-Systeme sowie Pre-Employment-Screenings hingegen sind – wie vor zwei Jahren – nur bei den wenigsten Unternehmen zu finden.

Welche Sicherheitsvorkehrungen haben Sie im Bereich Personal getroffen?



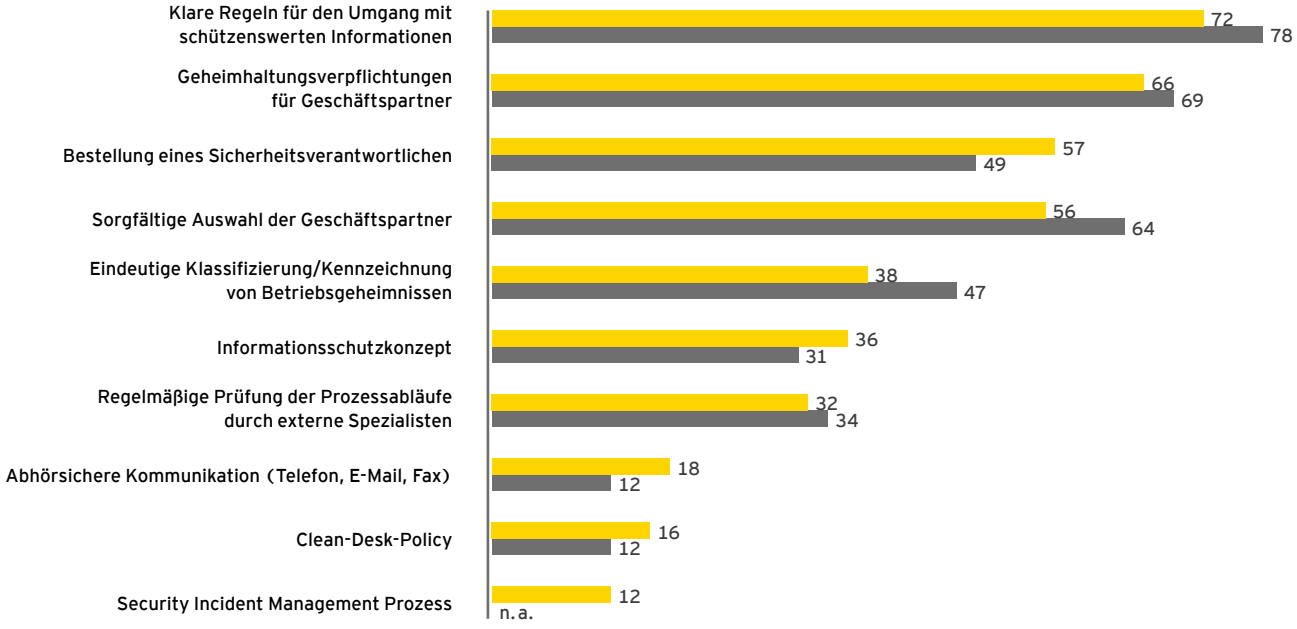
Angaben in Prozent; Mehrfachnennungen möglich

Abhörsichere Kommunikation in weniger als jedem fünften Unternehmen

Ein großer Teil der deutschen Unternehmen gibt klare Regeln für den Umgang mit sensiblen Informationen vor und verpflichtet seine Geschäftspartner zur Geheimhaltung.

Eine abhörsichere Kommunikation ist allerdings nur in seltenen Fällen anzutreffen.

Welche prozesstechnischen Vorkehrungen haben Sie getroffen, um sich vor Industriespionage zu schützen?



Angaben in Prozent; Mehrfachnennungen möglich

„Wer sensible Firmen- oder Kundendaten auf seinen Servern hat, sollte strenge Sicherheitsvorkehrungen einführen."

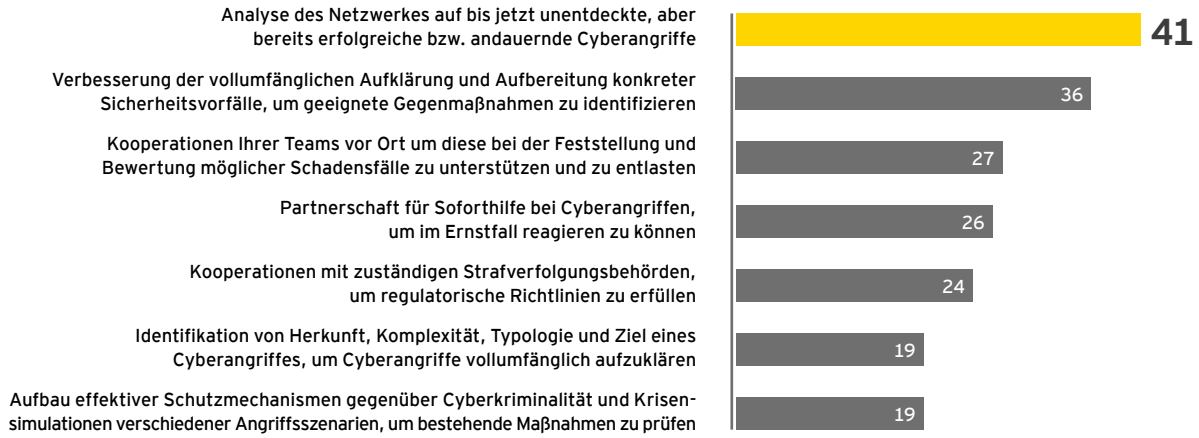
Bodo Meseke

Geplante Abwehrmaßnahmen: Unternehmen priorisieren Netzwerkdatenanalyse und Aufklärung

Zur Abwehr von Cyberangriffen setzen die Unternehmen vor allem auf eine verstärkte Netzwerkdatenanalyse sowie eine verbesserte Aufklärung und Aufbereitung konkreter Sicherheitsvorfälle.

Umfassendere Maßnahmen wie die vollumfängliche Aufklärung von Cybervorfällen und Krisensimulationen von Angriffsszenarien sind nur von jedem fünften Unternehmen beabsichtigt.

Welche Maßnahmen zur Abwehr von Cyberangriffen planen Sie für die Zukunft?



Angaben in Prozent; Mehrfachnennungen möglich

Fazit und Ausblick

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.

Der bisherige Umgang mit den Bedrohungen grenzt an Fahrlässigkeit. Passwörter und Antivirensoftware können von Hackern heute mitunter minutenschnell umgangen werden. Ein Sicherheitssystem, das lediglich auf diese herkömmlichen Schutzmaßnahmen setzt, öffnet Hackern bereitwillig die Tore. Wer sensible Firmen- oder Kundendaten auf seinen Servern hat, sollte unbedingt strengere Sicherheitsvorkehrungen einführen.

Technische Infrastruktur effektiv vor Angriffen aus dem Netz zu schützen, erfordert viel Erfahrung und ein umfassendes, technisches Know-how. Wichtige Hinweise auf die richtigen Maßnahmen stammt auch aus Insiderwissen über die Typologie der Angreifer, ihre Methoden und ihre Motive.

Dabei zeichnet sich ein wirksamer Schutzmechanismus gegen Cyberkriminalität nicht nur dadurch aus, dass er Angriffe erkennt, zurückverfolgt und Gefahren beseitigt. Vielmehr muss das eigene Schutzsystem sukzessive verbessert werden, um es Angreifern immer schwerer zu machen.

Ihr Ansprechpartner

Bodo Meseke
Partner
Leader Forensic Technology & Discovery Services/
EMEIA Central Zone
Business Integrity & Corporate Compliance

Ernst & Young GmbH
Wirtschaftsprüfungsgesellschaft
Mergenthalerallee 3-5
65760 Eschborn

Telefon: +49 6169 22174
Mobil: +49 160 939 22174
E-Mail: bodo.meseke@de.ey.com

EY | Assurance | Tax | Transactions | Advisory

Die globale EY-Organisation im Überblick
Die globale EY-Organisation ist einer der Marktführer in der Wirtschaftsprüfung, Steuerberatung, Transaktionsberatung und Managementberatung. Mit unserer Erfahrung, unserem Wissen und unseren Leistungen stärken wir weltweit das Vertrauen in die Wirtschaft und die Finanzmärkte. Dafür sind wir bestens gerüstet: mit hervorragend ausgebildeten Mitarbeitern, starken Teams, exzellenten Leistungen und einem sprichwörtlichen Kundenservice. Unser Ziel ist es, Dinge voranzubringen und entscheidend besser zu machen – für unsere Mitarbeiter, unsere Mandanten und die Gesellschaft, in der wir leben. Dafür steht unser weltweiter Anspruch „Building a better working world".

Die globale EY-Organisation besteht aus den Mitgliedsunternehmen von Ernst & Young Global Limited (EYG). Jedes EYG-Mitgliedsunternehmen ist rechtlich selbstständig und unabhängig und haftet nicht für das Handeln und Unterlassen der jeweils anderen Mitgliedsunternehmen. Ernst & Young Global Limited ist eine Gesellschaft mit beschränkter Haftung nach englischem Recht und erbringt keine Leistungen für Mandanten. Weitere Informationen finden Sie unter www.ey.com.

In Deutschland ist EY an 22 Standorten präsent. „EY" und „wir" beziehen sich in dieser Publikation auf alle deutschen Mitgliedsunternehmen von Ernst & Young Global Limited.

KKL 1511-207
ED None

EY ist bestrebt, die Umwelt so wenig wie möglich zu belasten. Diese Publikation wurde CO_2-neutral und auf FSC®-zertifiziertem Papier gedruckt, das zu 60 % aus Recycling-Fasern besteht.

www.de.ey.com