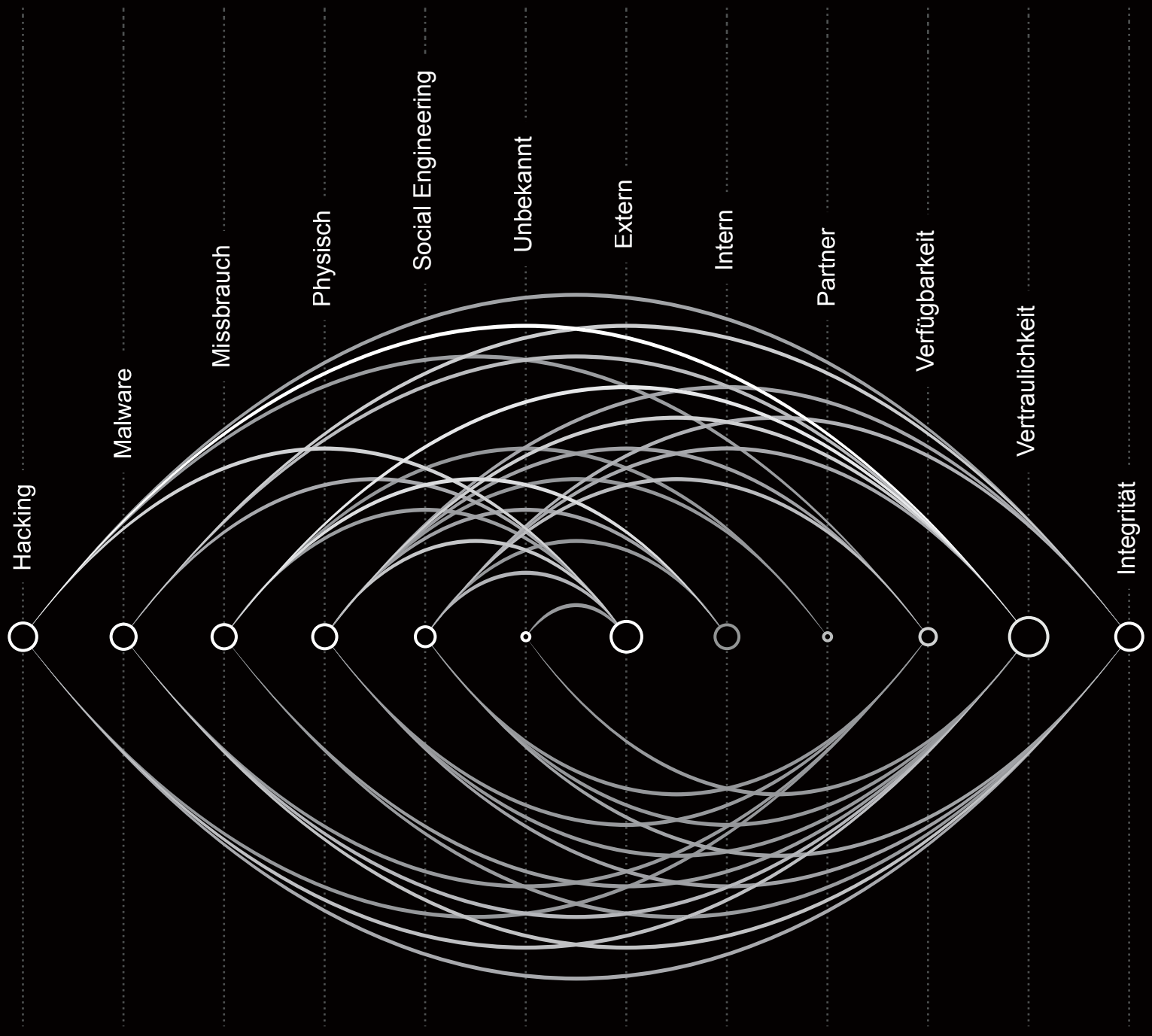
Kurzfassung

Data Breach Investigations Report 2018



verizon

verizon

Die Sicherheit Ihres Unternehmens hängt von Ihnen ab

Sicherheitsverstöße gehen nicht nur Sicherheitsfachleute etwas an. Ihre Auswirkungen machen sich im ganzen Unternehmen bemerkbar – von der Rechtsabteilung, die Klagen bearbeiten muss, bis zu den Mitarbeitern mit Kundenkontakt, die keinen Zugriff auf die benötigten Tools haben. Deshalb muss jeder seinen Teil zum Risikomanagement beitragen. Aber zunächst müssen Sie verstehen, womit Sie konfrontiert sind.

Um digitale Innovationen voll nutzen zu können, müssen Sie auf Ihre Sicherheit vertrauen können. Deshalb veröffentlichen wir jährlich den „Data Breach Investigations Report“ (DBIR); dieses Jahr bereits zum 11. Mal. Jeder Bericht basiert auf Tausenden von Vorfällen aus der Praxis. Dieses Jahr waren es über 53.000, einschließlich 2.216 bestätigter Datenverluste.

53.308 Sicherheitsvorfälle, 2.216 Datenverluste, 65 Länder, 67 Teilnehmer.

Auch dieses Jahr mussten wir wieder feststellen, dass Cyber-Kriminelle immer noch mit altbewährten Methoden Erfolg haben und ihre Opfer immer noch dieselben Fehler machen.

Als ersten Schritt zur Stärkung der Sicherheit sollten Sie recherchieren, wer Sie „im Visier“ hat, worauf diese Angreifer es abgesehen haben und wie sie vermutlich vorgehen werden, um es sich zu beschaffen.

Eines Tages trifft es auch Sie

Die meisten Cyber-Kriminellen wollen sich einfach nur bereichern. Wenn Ihr Unternehmen etwas besitzt, das sich zu Geld machen lässt, haben Sie ihr Interesse bereits geweckt. Das können beispielsweise Zahlungsdaten, personenbezogene Daten oder auch geistiges Eigentum sein.

Dabei ist es Datendieben egal, wen sie bestehlen. Der gängigen Vorstellung zum Trotz sind sie keineswegs nur an milliardenschweren Konzernen interessiert. Im Gegenteil: Sie sind Opportunisten. Sie greifen nicht die wohlhabensten oder bekanntesten Unternehmen an, sondern diejenigen, die am wenigsten auf einen Angriff vorbereitet sind.

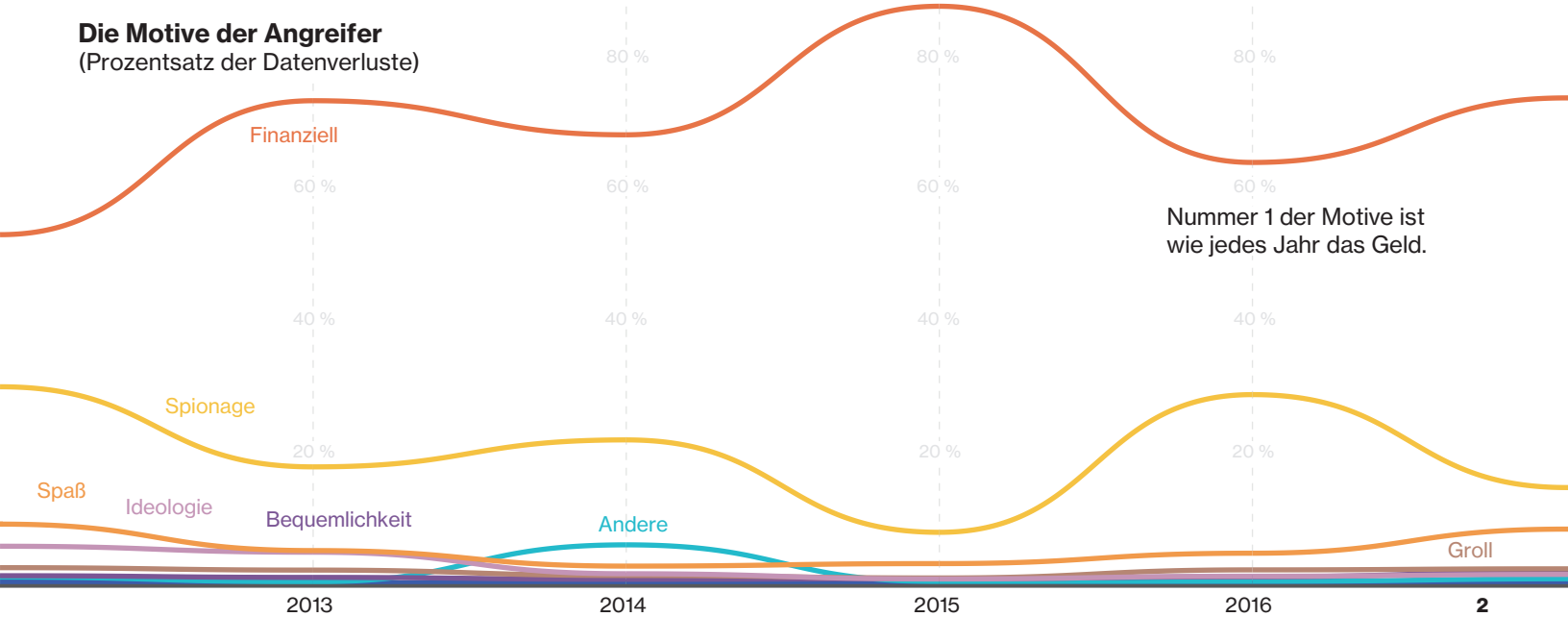
76 % der Sicherheitsverletzungen hatten ein finanzielles Motiv.

Wer sind die Angreifer?

Fast drei Viertel (73 %) der Cyber-Angriffe wurden von außen verübt. Die Hälfte der Angriffe gingen von organisierten Verbrechergruppen und 12 % von staatlichen Behörden oder staatlich gesponserten Akteuren aus.

Doch nicht alle Angriffe kommen von außen. An über einem Viertel (28 %) waren Insider beteiligt. Der Schutz gegen diese Bedrohung ist besonders schwierig, denn Anzeichen dafür, dass jemand seinen legitimen Zugang zu Ihren Daten für kriminelle Aktivitäten nutzt, sind nur schwer zu erkennen.

Die Motive der Angreifer
(Prozentsatz der Datenverluste)



verizon

Menschen machen Fehler

Die Bedrohung von innen ist nicht immer ein bösartiger Bereicherungsversuch eines Mitarbeiters. Fast jede fünfte Sicherheitslücke (17 %) entstand durch Versehen oder Unterlassungen. Beispiele hierfür sind, dass jemand ein vertrauliches Dokument nicht schreddert, eine E-Mail an die falsche Person sendet oder einen Web-Server falsch konfiguriert. Dahinter steckt keine böse Absicht, aber alle drei Beispiele können großen Schaden anrichten.

Phishing-Kampagnen sind bei 4 % aller Empfänger erfolgreich.

Wie wir bereits in den letzten drei Jahren festgestellt haben, fallen leider immer noch Menschen auf Phishing herein. Die gute Nachricht ist, dass 78 % aller Mitarbeiter das ganze Jahr über auf keine einzige Phishing-Nachricht klicken. Dennoch funktioniert jede einzelne Phishing-Kampagne bei durchschnittlich 4 % der Zielpersonen. Und, so unglaublich es klingt: Je mehr Phishing-E-Mails jemand bereits angeklickt hat, desto wahrscheinlicher ist, dass er es wieder tut.

Nach Beginn einer Phishing-Kampagne haben Sie im Schnitt 16 Minuten Zeit, bis jemand anbeisst und auf den Link klickt. Nach 28 Minuten wird der erste besser informierte Empfänger Sie auf die Kampagne aufmerksam machen.

Machen Sie sich nicht erpressbar

Cyber-Kriminelle müssen Ihre Daten nicht stehlen, um sie zu Geld zu machen. Es reicht, wenn Sie selbst sie nicht mehr nutzen können. Im DBIR 2013 kam zum ersten Mal Ransomware zur Sprache. In diesem Jahr wurde sie bei 39 % der Angriffe mit Malware gefunden und ist damit die häufigste Malware-Variante.

Ransomware wurde bei 39 % der Angriffe mit Malware gefunden und ist damit die häufigste Malware-Variante.

Warum ist Ransomware so weit verbreitet? Weil sie einfach zu verbreiten und sehr wirksam ist. Mit fertigen Toolkits kann jeder Amateurkriminelle in wenigen Minuten Ransomware erstellen und verbreiten. Die Masche ist billig und risikolos, und es müssen keine gestohlenen Daten zu Geld gemacht werden.

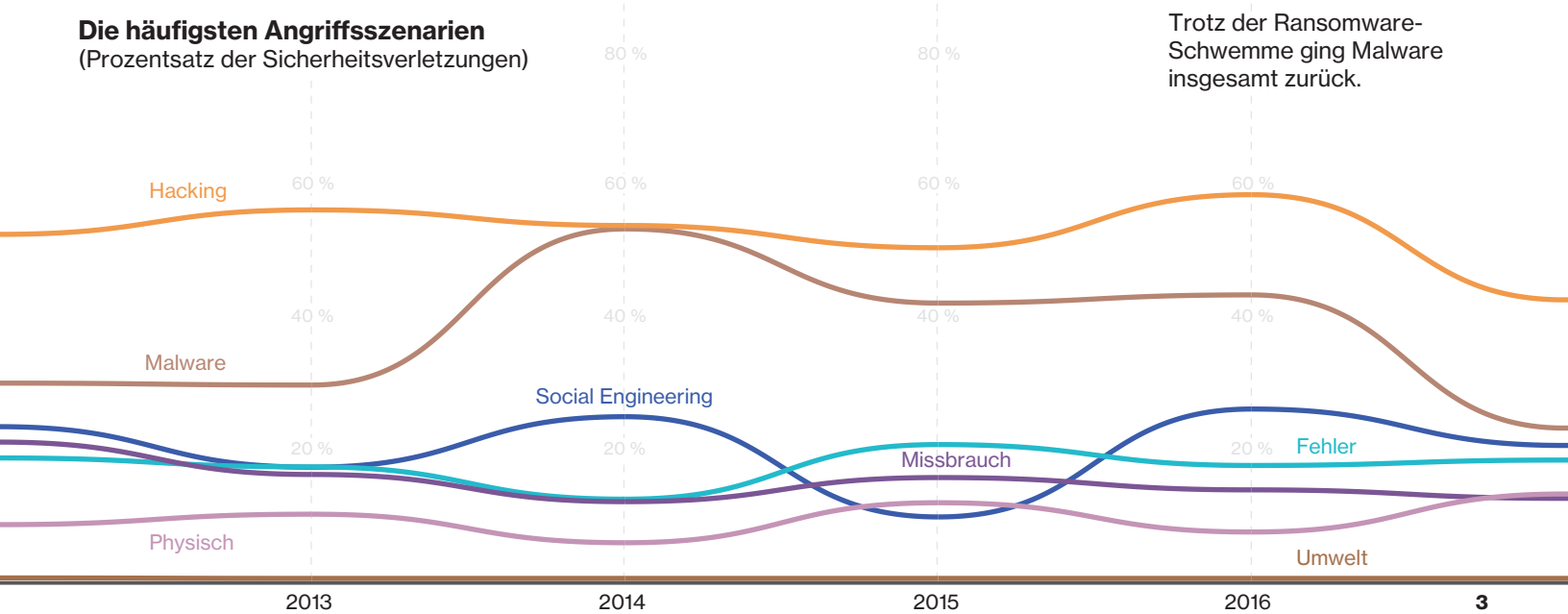
Cyber-Kriminelle verschlüsseln zunehmend nicht nur einzelne Endgeräte. Wenn es ihnen gelingt, einen Fileserver oder eine Datenbank zu verschlüsseln, sind der Schaden und das potenzielle Lösegeld viel höher. Wenn Sie keine Backups haben, können Cyber-Kriminelle mit dieser Masche Ihr gesamtes Unternehmen lahmlegen.

So können Sie sich schützen

Im Folgenden gehen wir auf die größten Bedrohungen in Ihrer Branche ein.

Die häufigsten Angriffsszenarien
(Prozentsatz der Sicherheitsverletzungen)

Trotz der Ransomware-Schwemme ging Malware insgesamt zurück.



verizon

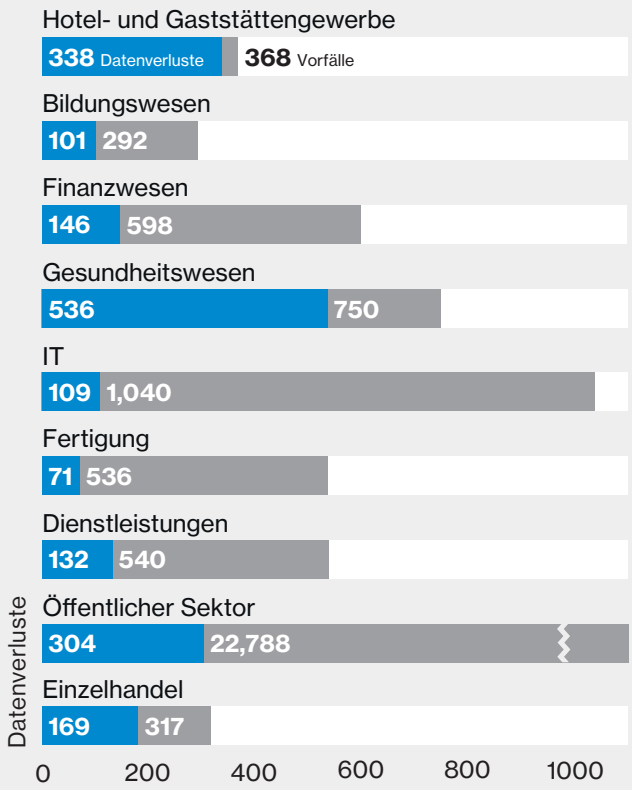
Welches ist das größte Risiko für Ihr Unternehmen?

Die genaue Zusammensetzung der verschiedenen Bedrohungen ist von Branche zu Branche verschieden. Wenn Sie die größten Bedrohungen in Ihrer Branche kennen, können Sie Ihr Sicherheitsbudget optimal nutzen und die Risiken senken.

Im diesjährigen DBIR klassifizieren wir die Bedrohungen in neun Branchen – im Folgenden sehen Sie eine Zusammenfassung der Ergebnisse. Wenn Ihr Industriezweig nicht dabei ist, heißt das nicht, dass es dort keine Bedrohungen gibt, sondern nur, dass uns nicht genug Ausgangsdaten für eine fundierte statistische Analyse vorliegen.

Der DBIR 2018 umfasst mehr Details zu den Bedrohungen in jeder Branche sowie Empfehlungen für Maßnahmen, mit denen Sie Ihr Unternehmen schützen können.

Anzahl der Vorfälle und Sicherheitsverletzungen nach Branche



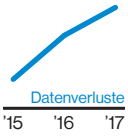
Hotel- und Gaststättengewerbe

Wer	99 % extern, 1 % intern
Was	93 % Zahlungsdaten, 5 % personenbezogen, 2% Anmeldedaten
Wie	93 % Hacking, 91 % Malware

Die größte Gefahr droht ganz klar den Zahlungssystemen, mit 90 % aller Angriffe. Ihr Risiko eines Angriffs auf einen POS-Controller ist 100-mal so hoch wie der Durchschnitt aller Branchen in unserem Datensatz.

Bildungswesen

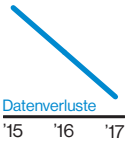
Wer	81 % extern, 19 % intern
Was	72 % personenbezogen, 14 % Geschäftsgeheimnisse, 11 % medizinisch
Wie	46 % Hacking, 41 % Social Engineering



Vertrauliche Daten Ihrer Mitarbeiter werden mit Social-Engineering-Methoden gestohlen und für Identitätsbetrug missbraucht. Spione sind an Ihren Forschungsergebnissen interessiert und für 20 % der Angriffe verantwortlich. Doch nicht immer geht es um finanzielle Bereicherung: 11 % der Angriffe geschahen „zum Spaß“.

Finanzwesen

Wer	79 % extern, 19 % intern
Was	36 % personenbezogen, 34 % Zahlungsdaten, 13 % Bankdaten
Wie	34 % Hacking, 34 % physisch

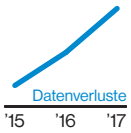


Organisierte Banden betreiben noch immer Skimming an Geldautomaten. Beim etwas neueren „Jackpotting“ wird Software oder Hardware installiert, die Automaten zur Geldausgabe veranlasst. Auch Denial-of-Service-Angriffe zur Störung Ihres Geschäftsbetriebs sind nach wie vor eine sehr reale Gefahr.

verizon

Gesundheitswesen

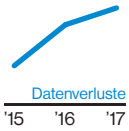
Wer	43 % extern, 56 % intern
Was	79 % medizinisch, 37 % personenbezogen, 4 % Zahlungsdaten
Wie	35 % Fehler, 24 % Missbrauch



Das Gesundheitswesen ist die einzige Branche, in der die Gefahr von innen größer ist als die von außen. Die Hauptursache sind menschliche Fehler. Mitunter missbrauchen Mitarbeiter auch ihren Zugang zu Systemen oder Daten, wobei in 13 % der Fälle Spaß oder Neugier die Motive waren, beispielsweise wenn kürzlich eine prominente Person Patient war.

Dienstleistungen

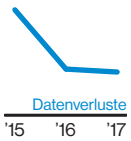
Wer	70 % extern, 31 % intern
Was	56 % personenbezogen, 28 % Anmeldedaten, 16 % Interna
Wie	50 % Hacking, 21 % Social Engineering



Die Angreifer haben meist finanzielle Motive und nutzen oft Phishing oder gestohlene Anmeldedaten. Auch Fehler durch Mitarbeiter stellen eine Gefahr dar. Die Angreifer brauchen meist höchstens ein paar Stunden, um an die anvisierten Daten zu kommen. Es kann jedoch Tage dauern, bevor der Angriff aufgedeckt wird – oftmals durch Dritte.

IT

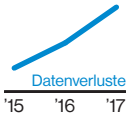
Wer	74 % extern, 23 % intern
Was	56 % personenbezogen, 41 % Anmeldedaten, 9 % Interna
Wie	57 % Hacking, 26 % Fehler



Angriffe auf Web-Anwendungen, oft mit gestohlenen Anmeldedaten, sind ein großes Problem. Auch Mitarbeiterfehler wie falsch konfigurierte Datenbanken und Fehler bei der Veröffentlichung verursachen erhebliche Schäden. Die vermutlich größte Bedrohung (mit 56 % der gemeldeten Vorfälle im Jahr 2017) sind jedoch Denial-of-Service-Angriffe.

Öffentlicher Sektor

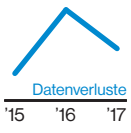
Wer	67 % extern, 34 % intern
Was	41 % personenbezogen, 24 % Geheimnisse, 14 % medizinisch
Wie	52 % Hacking, 32 % Social Engineering



Cyber-Spionage bleibt ein wichtiges Thema – 44 % der Vorfälle fielen in diese Kategorie. Dabei spielen Phishing sowie die Installation und Nutzung von Hintertüren oder Command-and-Control-Kanälen eine wichtige Rolle. Gefährdet sind nicht nur Staatsgeheimnisse, sondern auch personenbezogene Daten von Bürgern und Mitarbeitern.

Fertigung

Wer	89 % extern, 13 % intern
Was	32 % personenbezogen, 30 % Geschäftsgeheimnisse, 24 % Anmeldedaten
Wie	66 % Hacking, 34 % Malware



Insgesamt betrachtet sind die meisten Cyber-Angriffe opportunistisch: Sie erfolgen dort, wo sich eine Gelegenheit bietet. Doch in der Fertigung gelten 86 % der Angriffe einem bestimmten Ziel. Das ist oft die Planung, Forschung und Entwicklung eines neuen Produkts. Fast die Hälfte (47 %) der Sicherheitsverstöße waren mit Industriespionage verbunden.

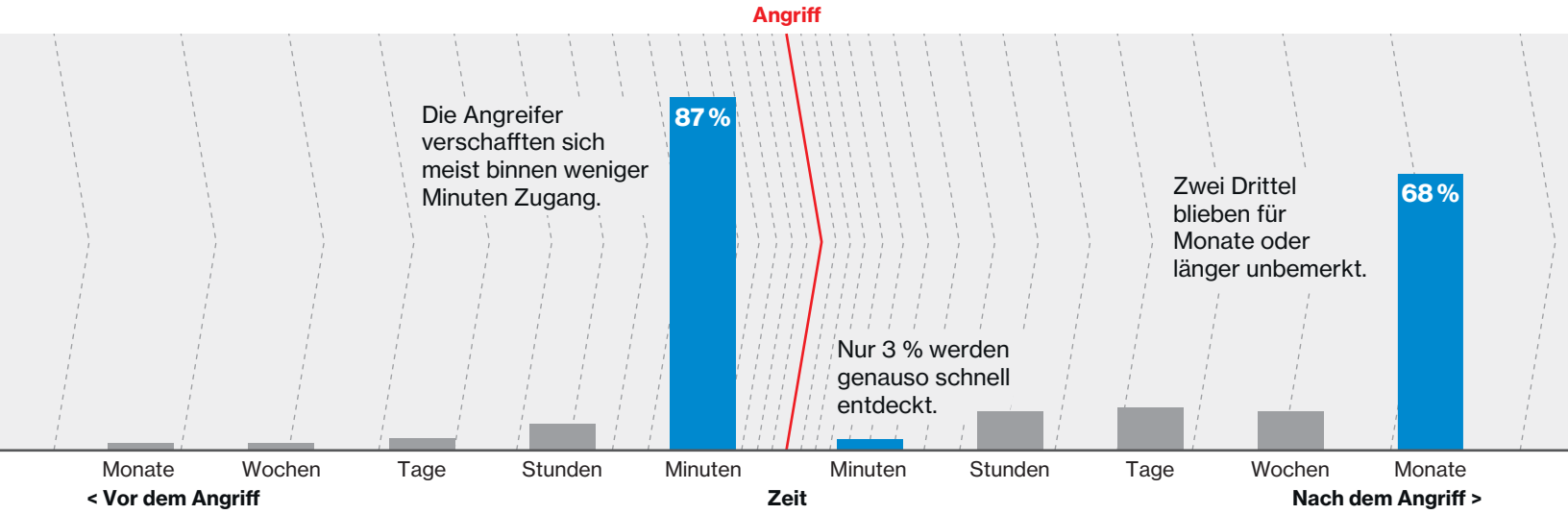
Einzelhandel

Wer	91 % extern, 10 % intern
Was	73 % Zahlungsdaten, 16 % personenbezogen, 8 % Anmeldedaten
Wie	46 % Hacking, 40 % physisch

Beim Datendiebstahl standen Angriffe auf Web-Anwendungen, die laxe Validierungen oder gestohlene Anmeldedaten ausnutzten, an der Spitze. Datendiebstahl ist aber nicht Ihre einzige Sorge. Denial-of-Service-Angriffe können das Durchführen von Transaktionen verhindern, Ihre Website und die in Ladengeschäften genutzten Systeme verlangsamen und andere schwerwiegende Auswirkungen haben.

verizon

Es ist höchste Zeit



Cyber-Kriminelle brauchen oft nur Minuten oder gar Sekunden, um in ein System einzudringen. Auch das Finden und Ausschleusen wertvoller Daten dauert nicht lange. Da die meisten Unternehmen einen Angriff erst nach Wochen oder Monaten bemerken, haben die Angreifer gewöhnlich mehr als genug Zeit.

68 % der Angriffe wurden erst nach Monaten oder noch später entdeckt.

Viele Angriffe werden nicht einmal vom betroffenen Unternehmen selbst aufgedeckt, sondern von Dritten wie Ermittlungsbehörden oder Geschäftspartnern. Noch schlimmer: Viele Fälle werden von Kunden entdeckt. Sie wissen selbst am besten, was das für Ihr Marken-Image bedeuten würde.

Zum Schutz Ihrer Reputation sollten Sie zwei Ziele verfolgen: die Prävention und die Abwehr von Angriffen. Ihre Präventionsmaßnahmen sollten stark genug sein, um Opportunisten abzuschrecken. Aber es gibt keinen 100 %igen Schutz. Sie müssen darauf vorbereitet sein, schnell und wirksam auf erfolgreiche Angriffe zu reagieren.

So können Sie sich schützen

Seien Sie wachsam
Warten Sie nicht, bis eine Behörde oder ein Kunde Sie auf einen Sicherheitsverstoß aufmerksam macht. Logdateien und Änderungsmanagement-Systeme enthalten oft erste Hinweise auf eine Sicherheitsverletzung.

Mobilisieren Sie Ihre Mitarbeiter
Wissen Ihre Mitarbeiter, wie wichtig die Cyber-Sicherheit für Ihre Marke und Ihre Geschäftsergebnisse ist? Holen Sie sie ins Boot und sensibilisieren Sie sie für die Anzeichen eines Angriffs und die notwendigen Gegenmaßnahmen.

Gewähren Sie nur die unbedingt erforderlichen Zugriffsrechte
Wissen Sie, wer Zugriff auf Ihre sensiblen Daten und Systeme hat? Beschränken Sie den Zugriff auf Mitarbeiter, die ihn für ihre Arbeit benötigen. Richten Sie Prozesse zum Widerrufen von Zugriffsrechten ein und nutzen Sie diese konsequent, wenn Mitarbeiter den Arbeitsplatz wechseln.

Spielen Sie Patches zeitnah ein
Cyber-Kriminelle nutzen längst bekannte Schwachstellen noch immer erfolgreich aus. Sie können viele Bedrohungen vermeiden, indem Sie einfach nur Ihre Antiviren-Software aktuell halten.

Verschlüsseln Sie sensible Daten
Trotz aller Anstrengungen Ihrerseits wird vermutlich früher oder später ein Hacker in eines Ihrer Systeme eindringen. Doch wenn Sie Ihre Daten verschlüsseln, sind sie für Datendiebe wertlos.

Nutzen Sie Zwei-Faktor-Authentifizierung
Phishing-Kampagnen sind immer noch sehr wirksam. Und Mitarbeiter machen Fehler. Mit einer Zwei-Faktor-Authentifizierung begrenzen Sie den Schaden, den Angreifer mit gestohlenen Anmeldedaten anrichten können.

Vernachlässigen Sie physische Zugangsbeschränkungen nicht
Nicht alle Datendiebstähle passieren online. Überwachungskameras und Systeme, die den Zugang zu bestimmten Unternehmensbereichen kontrollieren, machen es Kriminellen schwerer, Systeme zu manipulieren oder sensible Ressourcen zu stehlen.

verizon

Nutzen Sie unsere Informationen

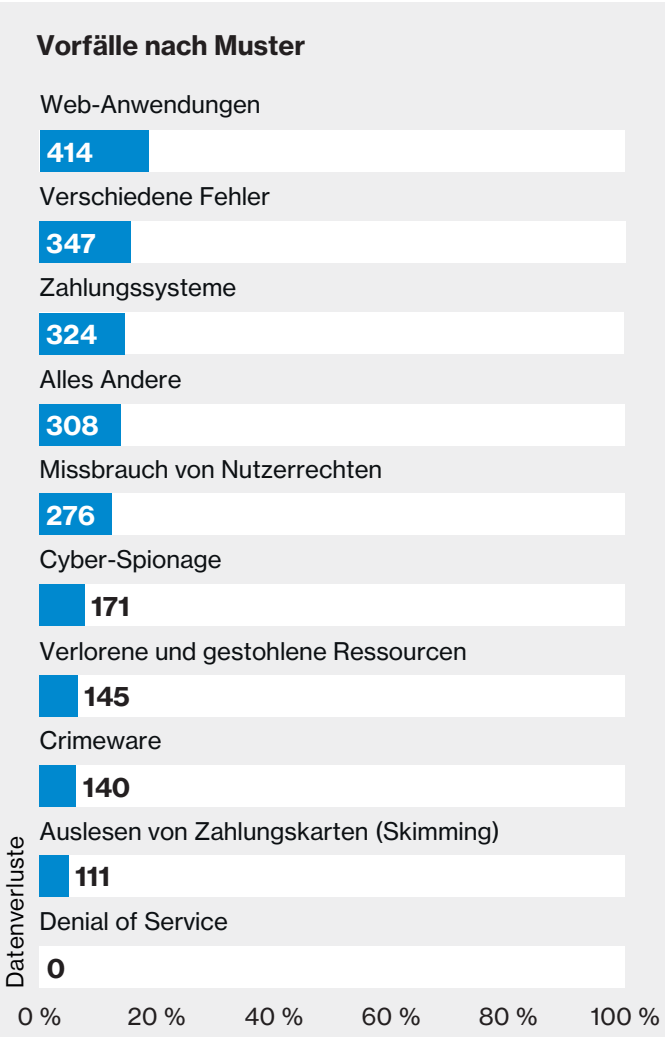
Angreifer entwickeln ständig neue Techniken, um an Ihre Systeme und Daten zu gelangen. Wir mussten jedoch im Zuge unserer Forschung feststellen, dass zu viele Unternehmen es ihnen immer noch zu einfach machen. Mancherorts werden selbst die einfachsten Sicherheitsmaßnahmen nicht konsequent durchgeführt, zum Beispiel die Aktualisierung der Antivirensoftware oder die Schulung der Mitarbeiter im Erkennen der Anzeichen eines Angriffs.

Sie können sich besser schützen, wenn Sie wissen, welchen Bedrohungen Ihr Unternehmen ausgesetzt ist. Deshalb veröffentlichen wir den DBIR. Im Bericht von 2014 identifizierten wir die neun gängigsten Angriffsmuster. Diese haben sich seitdem nicht geändert.

94 % der Sicherheitsvorfälle und 90 % der bestätigten Datenverluste seit 2014 entsprechen einem dieser neun Muster.

Anhand dieser Muster können Sie die größten Risiken für Ihr Unternehmen schnell und einfach beurteilen. Das bedeutet, dass Sie von Anfang an wirksame Sicherheitsmaßnahmen einbauen können, wenn Sie eine neue Anwendung in Auftrag geben oder ein System aktualisieren. Und es bedeutet auch, dass Ihre Sicherheitsexperten gezielt in die Maßnahmen investieren können, die für Ihr Unternehmen am wichtigsten sind.

Nähere Informationen über die einzelnen Muster und ihre Bedeutung für Ihre Branche finden Sie im DBIR 2018.

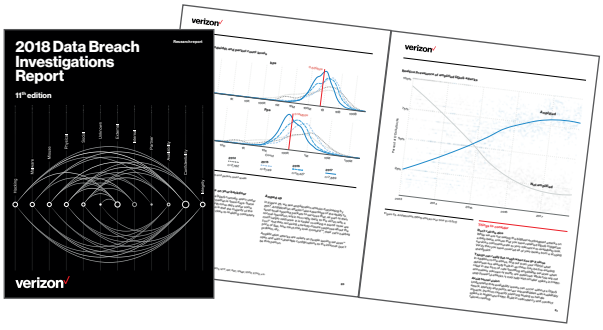


Der „Data Breach Investigations Report“ von Verizon vermittelt Ihnen einen Überblick über die Bedrohungen, denen Ihr Unternehmen ausgesetzt ist, und empfiehlt Maßnahmen zur Risikominderung.

Der Bericht von 2018 beruht auf der detaillierten Analyse von über 53.000 Sicherheitsvorfällen, einschließlich 2.216 bestätigter Sicherheitsverletzungen. Der DBIR erscheint bereits seit 11 Jahren und ist eine der renommiertesten Informationsquellen der Sicherheitsbranche.

Laden Sie den vollständigen Bericht herunter:

verizonenterprise.com/DBIR2018



Über die Titelseite

Das Liniendiagramm auf der Titelseite basiert auf den Daten in Anhang C, „Beaten paths“ (Typische Angriffsverläufe), des ausführlichen Berichts. Es veranschaulicht die Akteure, Aktivitäten und Attribute als Knoten und ihre zeitliche Abfolge bei einem Angriff als Kanten. Wir haben ermittelt, wie oft jeder Knoten in jedem Angriffsszenario vorkommt und das Ergebnis in der Größe abgebildet: Je größer der Knoten, desto größer die Häufigkeit. Die Kanten zwischen den Knoten sind als bogenförmige Linien dargestellt. Die Farbe jedes Bogens zeigt, bei wie vielen Angriffen diese Abfolge auftritt.

verizonenterprise.com/de