2016 Data Breach Investigations Report

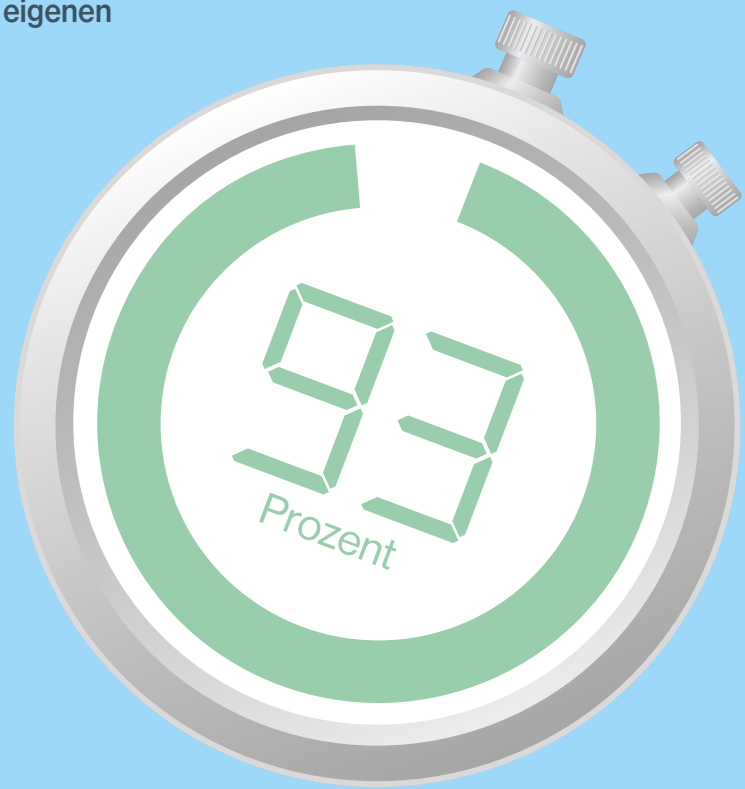
Executive Summary

Internetsicherheit betrifft nicht nur Sicherheitsexperten.
Der C-Level-Leitfaden für das, was man wissen muss.

verizon

Hatten Sie schon einmal eine Datenpanne?

In 93% der Fälle benötigten Angreifer Minuten oder noch weniger, um Systeme zu schädigen. Inzwischen benötigen Unternehmen Wochen oder noch länger, nur um zu entdecken, dass eine Sicherheitsverletzung stattgefunden hat – und in der Regel sind es Kunden oder Strafverfolgungsbehörden, die den Alarm auslösen, nicht die eigenen Sicherheitsmaßnahmen.



Mehr als 100.000 Vorfälle. Analyse von 2.260 Datenpannen. 82 Länder. 67 beitragende Unternehmen.

Der Verizon Data Breach Investigations Report (DBIR) wird von Sicherheitsexperten als einzigartige Quelle für Erkenntnisse akzeptiert – und unsere neunte Ausgabe ist die bisher umfassendste. Aber wenn Sie Leiter der Informationstechnologie, Vertriebsleiter oder Geschäftsführer sind, müssen Sie die Risiken ebenfalls verstehen, daher gibt es diesen Leitfaden für Sie.

Sicherheit muss eine treibende Kraft sein, keine nachträgliche Überlegung.

Daten sind die treibende Kraft für Innovationen. Durch sie werden Lieferketten beschleunigt und Kundenerfahrungen neu definiert. Aber Unternehmen und Verbraucher sind über die Sicherheit besorgt. Es ist wichtig, Gefahren zu begegnen, um Ihre Kunden zu beruhigen und um Ihnen das Vertrauen zu geben, die digitale Beschleunigung umfassend anzunehmen.

Jedes Unternehmen ist in irgendeiner Weise auf die digitale Welt angewiesen – zur Kommunikation, für Transaktionen oder aufgrund des Wettbewerbs. Heute geht es bei Wettbewerbsvorteilen darum, etwas digital durchführen zu können – und zwar besser. Aber dazu brauchen Sie zuverlässige und sichere Systeme. Und das bedeutet, dass Datensicherheit etwas ist, um das wir uns alle kümmern müssen.

Datenpannen sind teuer. Es geht nicht nur um Entschädigung und Bußgelder, die Gebühren für Rechtsdienste und Mängelbeseitigung können ebenfalls erheblich sein. Auch der Ruf der Marke leidet unter Sicherheitsverletzungen. Das ist besonders wichtig, da das Vertrauen Ihrer Kunden und Partner noch nie so entscheidend war.

Eine Datenpanne wird Sie wahrscheinlich nicht sofort aus dem Geschäft drängen, aber sie kann Ihrer Zukunft ernsthaft gefährlich werden.

Nehmen wir einmal an, Sie betreiben einen Baumarkt. Vielleicht kaufen Kunden noch in Ihrem Markt – auch wenn sie dann wahrscheinlich noch eher mit Bargeld zahlen – aber werden sie Ihre neue App herunterladen oder Ihre neue Lösung für ein Heimnetzwerk kaufen?

Bei den meisten Sicherheitsverletzungen geht es um Geld

Vergessen Sie diesen Hollywood-Film. Die meisten Cyberangriffe erfolgen willkürlich und sind durch Gier motiviert – nicht durch Rache oder als Dienst an der Öffentlichkeit. Die meisten Angreifer möchten Ihre Daten stehlen, weil diese etwas wert sind, nicht weil Sie es sind. Hauptsache, man kann es zu Geld machen. Da der Wert von Kreditkartendaten fällt – durch die bessere Betrugserkennung der Banken – könnten sich die Angreifer vermehrt auf Dinge wie geistiges Eigentum und geschützte Gesundheitsinformationen konzentrieren.

Angreifer wählen den einfachsten Weg

Es wäre ein Fehler zu glauben, dass Ihre größte Gefahr in den brandneuen Schwachstellen liegt. Die meisten Angriffe nutzen bekannte Schwachstellen aus – bei denen bereits seit Monaten, wenn nicht sogar Jahren, ein Patch zur Verfügung steht.

63% der bestätigten Datenschutzverletzungen beinhalten die Nutzung schwacher, standardmäßiger oder gestohlener Passwörter.

Der Grund, weshalb die Verbrecher so schnell in das System kamen, war häufig der, dass sie bereits den Schlüssel hatten. Social Engineering bleibt besorgniserregend wirksam – "hier klicken, um Ihr Bankkennwort zurückzusetzen". Wir haben herausgefunden, dass fast ein Drittel (30%) der Phishing-Nachrichten geöffnet wurden – mehr als die 23% im Jahr 2014. Und 12% der Zielpersonen öffneten auch den bösartigen Anhang oder klickten auf den Link – in etwa der gleiche Anteil wie 2014 (11%).

Machen Sie den Angreifern das Leben schwer

Es gibt kein System, in das man gar nicht eindringen kann, aber Internet-Kriminelle werden oft schon durch eine halbwegs annehmbare Verteidigung abgehalten – sie ziehen weiter und suchen sich ein einfacheres Ziel. Leider erreichen viele Unternehmen nicht einmal dieses bescheidene Ziel.

95% der Datenschutzverletzungen lassen sich neun Mustern zuordnen.

Dieses Jahr konzentriert sich der DBIR wieder auf die neun Vorfallsmuster, die wir im Jahr 2014 erkannt haben. Wenn Sie diese Muster verstehen, hilft es Ihnen dabei, Ihre Sicherheitsbemühungen auf die richtigen Bereiche zu konzentrieren.

95% der Datenschutzverletzungen und 86% der Datenpannen werden von nur neun Mustern abgedeckt.

Intelligenter investieren.

Die Bösewichte werden ständig besser. Andererseits entwickelt sich Ihre Infrastruktur schneller als je zuvor. Wie können Sie aktuell bleiben, ohne Ihr Budget zu sprengen?

Der Druck auf Unternehmen, digitaler zu werden, wächst von Tag zu Tag. Es müssen mehr Geräte geschützt werden, es gibt mehr Menschen mit Zugang zu Daten und immer mehr Partner, die integriert werden müssen.

Neue Technologien — beispielsweise Mobiltelefone und das Internet der Dinge (Internet of Things/IoT) — drohen Angreifern neue Möglichkeiten zu geben.

Bisher haben wir keine wesentliche Anzahl von Vorfällen gesehen, an denen Mobiltelefone oder IoT-Geräte beteiligt waren. Aber die Bedrohung ist sicherlich real. Dass Schwachstellen ausgenutzt werden können, wurde aufgezeigt, und es ist nur eine Frage der Zeit, bis wir eine groß angelegte Sicherheitsverletzung erleben.

Neun Muster beschreiben über 80%

[redacted] **Vorfälle**
Sicherheitsverletzungen

Ansicht wechseln

Und die Bösewichter erhöhen ihre Einsätze. Das müssen sie, weil der Marktwert einiger Arten von Daten, insbesondere Kreditkarteninformationen, fällt. Um ihr Einkommen zu halten, müssen die Angreifer mehr Daten stehlen oder neue, lukrativere Informationsformen zum Verkauf finden – beispielsweise geschützte Gesundheitsinformationen und geistiges Eigentum.

Sie müssen die Angreifer dort treffen, wo es weh tut – in ihrer Brieftasche. Aber Sie haben kein unbegrenztes Budget. Das bedeutet, Sie müssen das Geld intelligenter einsetzen. Die neun Klassifikationsmuster für Pannen wurden 2014 zum ersten Mal veröffentlicht. Sie decken den größten Teil von Pannen und bestätigten Sicherheitsverletzungen ab, wie in Abbildung 1 gezeigt. Betrachtet man die einzelnen Branchen, fallen die meisten Bedrohungen jeweils nur unter drei Muster – siehe Abbildung 2. Die Analyse dieser Muster hilft Ihnen dabei, zu verstehen, wie Sie Ihre begrenzte Mitarbeiterzahl und Ihr begrenztes Budget am besten einsetzen, um die besten Ergebnisse zu erzielen.

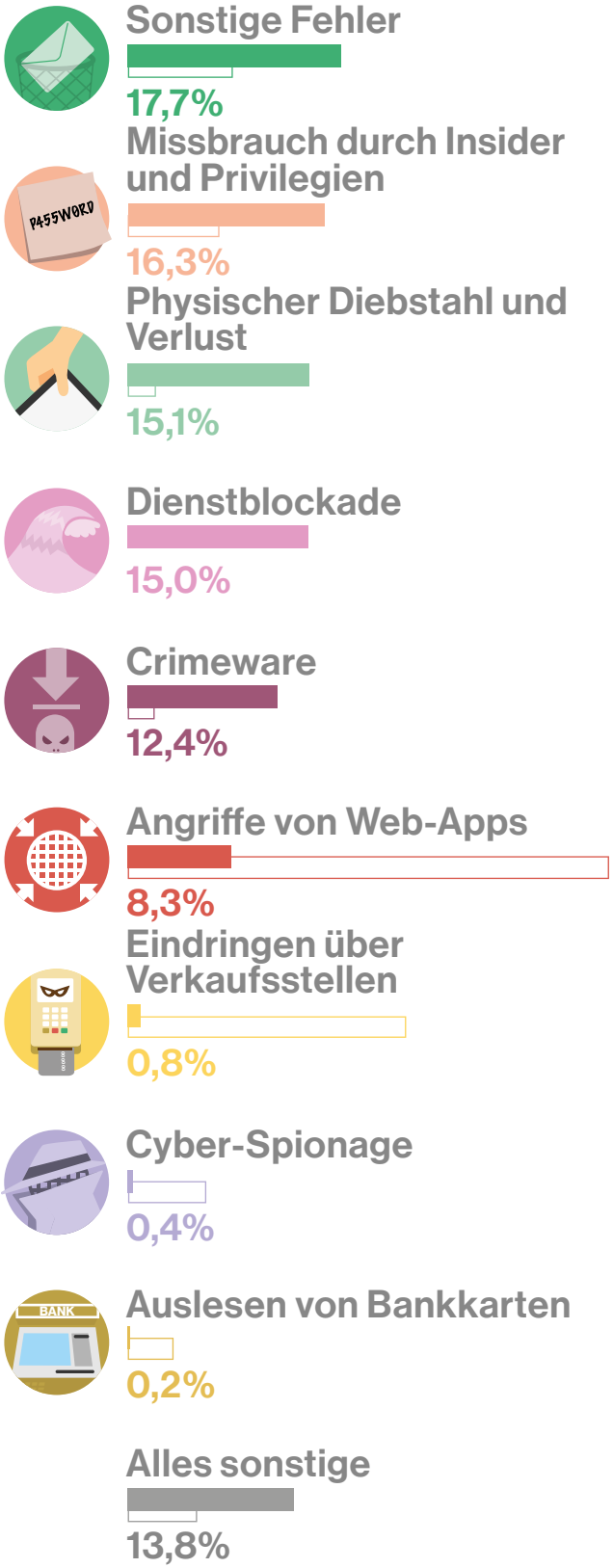


Abbildung 1: Pannen/Sicherheitsverletzungen nach Klassifikationsmuster, alle Branchen

In den meisten Branchen werden die Datenschutzverletzungen und Datenpannen von nur drei Mustern abgedeckt.

Unterkünfte (3 Muster = 96% der Vorfälle)

Unterhaltung (3 Muster = 100% der Vorfälle)

Finanzdienstleistungen (3 Muster = 88% der Vorfälle)

Gesundheitswesen (3 Muster = 73% der Vorfälle)

Produktion (3 Muster = 55% der Vorfälle)

Freiberufler (3 Muster = 94% der Vorfälle)

Öffentlicher Sektor (3 Muster = 66% der Vorfälle)

Einzelhandel (3 Muster = 90% der Vorfälle)

Transport (3 Muster = 77% der Vorfälle)

Versorger (3 Muster = 69% der Vorfälle)

Abbildung 2: Die drei wichtigsten Pannen/Sicherheitsverletzungen nach Branche

Sonstige Fehler

Alle unbeabsichtigten Aktionen oder Fehler, die die Sicherheit beeinträchtigen, ohne den Verlust von Vermögenswerten.

Am meisten betroffene Branchen:
Öffentlicher Sektor, Gesundheitswesen, Information

40% der Vorfälle nach diesem Muster wurden durch mangelnde Serverkapazität verursacht, bei der nicht-bösartige Spitzen im Internetverkehr Systeme überlasten und zum Absturz wichtiger Anwendungen führten. Aber häufig ist es nur ein einfacher Fehler eines Mitarbeiters, der einen Vorfall auslöst.

Bei 26% der sonstigen Fehler wurden unter anderem sensible Informationen an die falsche Person gesendet.

Was können Sie tun?

- **Lernen Sie aus Ihren Fehlern:** Führen Sie Aufzeichnungen über häufige Fehler, die in der Vergangenheit aufgetreten sind. Diese können Sie für Schulungen zum Sicherheitsbewusstsein und die Messung der Wirksamkeit Ihrer Kontrollen verwenden.
- **Kontrollen verstärken:** Ziehen Sie die Verwendung von Software gegen Datenverlust (Data Loss Prevention/DLP) in Erwägung, dadurch kann die Verbreitung von sensiblen Daten außerhalb des Unternehmens eingeschränkt werden.
- **Gründliche Löschverfahren einführen:** Stellen Sie sicher, dass sensible Daten vor dem Verkauf Ihrer Datenträger gelöscht wurden. Das klingt einleuchtend, aber wir haben viele Beispiele gesehen, wo dies nicht geschehen ist.

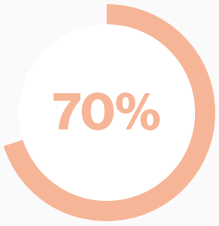
Missbrauch durch Insider und Privilegien

Besteht vor allem aus Vorfällen, bei denen Missbrauch durch Insider vorliegt. Aber es sind auch Außenstehende (durch betrügerische Absprachen) und Partner vertreten, die privilegierten Zugang zu Systemen haben.

Am meisten betroffene Branchen:
Gesundheitswesen, öffentlicher Sektor, Verwaltung

Im Gegensatz zur Meinung einiger Menschen sind es selten Systemadministratoren oder Entwickler mit höheren Rechten, die zum Opfer werden. Bei einem Drittel des Missbrauchs durch Insider sind Endnutzer betroffen. Die Angriffe sind in der Regel durch Geld motiviert: Bei 34% der Verstöße mit Missbrauch war Geld die Motivation – obwohl ein Viertel (25%) auch mit Spionage verknüpft werden kann, beispielsweise dem Diebstahl geistigen Eigentums.

70% der Verstöße mit Missbrauch von Insidern werden erst nach Monaten oder Jahren entdeckt.



Was können Sie tun?

- **Ihre Daten kennen:** Sie müssen wissen, welche sensiblen Daten Sie haben, wo sie sind und wer darauf Zugriff hat. Die Unternehmensorganisation muss sicherstellen, dass der Zugriff auf diejenigen beschränkt ist, die die Daten tatsächlich benötigen und dass der tatsächliche Zugriff anhand dieser Liste überprüft wird.
- **Nutzerverhalten überwachen:** Die Systemnutzung nachverfolgen – insbesondere den Zugang zu Daten, die für finanzielle Vorteile verwendet werden können – und den Zugriff sofort sperren, wenn ein Mitarbeiter das Unternehmen verlässt.
- **USB-Nutzung nachverfolgen:** Bringen Sie sich nicht in eine Position, in der Sie erst dann merken, dass ein Mitarbeiter Daten übernommen hat, wenn er das Unternehmen verlassen hat.

Physischer Diebstahl und Verlust

Verlust oder Diebstahl von Laptops, USB-Sticks, Ausdrucken und anderen Informationsträgern.

Am meisten betroffene Branchen:
Gesundheitswesen, öffentlicher Sektor

Ein sicherheitsrelevantes Ereignis wird normalerweise dann ausgelöst, wenn ein Mitarbeiter ein Laptop oder Mobiltelefon verloren hat. Aber die größte Gefahr von Datenmissbrauch droht durch verlorene oder gestohlene Dokumente, die nicht verschlüsselt werden können.

39% der Diebstähle erfolgen vom eigenen Arbeitsbereich des Opfers und 34% aus persönlichen Fahrzeugen der Mitarbeiter.

Was können Sie tun?

- **Verschlüsseln Sie Ihre Daten:** Wenn gestohlene Geräte verschlüsselt sind, ist es für den Angreifer viel schwieriger, auf die Daten zuzugreifen.
- **Schulen Sie Ihre Mitarbeiter:** Die Entwicklung des Sicherheitsbewusstseins ist für Ihr Unternehmen von entscheidender Bedeutung. Arbeiten Sie mit der Personalabteilung zusammen, um die physische Sicherheit von Unternehmensbeständen als Teil der einführenden und laufenden Mitarbeiterschulungen aufzunehmen.
- **Verwendung von Papier reduzieren:** Ausdrucke verringern. Erstellen Sie Regeln zur Datenklassifizierung und schaffen Sie Unternehmensleitlinien für den Ausdruck und den Transport von sensiblen Daten.

Dienstblockade (Denial of Service/DoS)

Die Verwendung von Bot-Netzen – eine "Zombie"-Armee von Computern, die in der Regel ohne Zustimmung des Besitzers übernommen wurden – um ein Unternehmen durch schädlichen Datenverkehr zu überwältigen. DoS-Angriffe können den normalen Geschäftsbetrieb zum Stillstand bringen und Chaos verursachen.

Am meisten betroffene Branchen:
Unterhaltung, freie Berufe, Bildung

Unterschätzten Sie nicht die Auswirkungen, die ein DoS-Angriff auf Ihr Unternehmen haben kann. Er ist in unseren Daten das vierthäufigste Muster für alle Sicherheitsvorfälle. Und ein groß angelegter Angriff könnte Ihre Website oder Ihre unternehmenskritischen Systeme für Wochen vom Internet trennen.

Der durchschnittliche Datenverkehr eines DoS-Angriffs liegt bei 1,89 Millionen Paketen pro Sekunde — als würden in jeder Minute über 113 Millionen Menschen versuchen, auf Ihren Server zuzugreifen.

1,89 Mpps

Was können Sie tun?

- **Wichtige Server trennen:** Primärsysteme trennen, um sie vor Angriffen zu schützen.
- **Wählen Sie Ihren Anbieter sorgfältig aus:** Stellen Sie sicher, dass die Anbieter für Ihren Cloud-Dienst Lösungen umgesetzt haben, um die Verfügbarkeit Ihrer Dienste und Infrastruktur zu schützen.
- **Prüfen Sie Ihren Dienst gegen DoS:** Er sollte nicht installiert und dann vergessen werden. Stellen Sie sicher, dass sie Ihre Dienstgütevereinbarungen (Service Level Agreements/SLAs) für den DoS-Schutz genau verstehen.

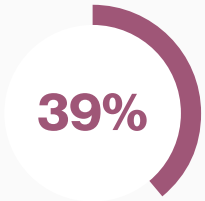
Crimeware

Dies umfasst jede Verwendung von Malware, die nicht in ein bestimmtes Muster passt. Crimeware wirkt sich häufig auf die Verbraucher aus.

Am meisten betroffene Branchen:
Öffentlicher Sektor, Produktion, Information

Die Angriffe sind in der Regel opportunistisch und durch finanziellen Gewinn motiviert. Die Malware gelangt auf Ihr System, wenn jemand auf einen schädlichen E-Mail-Link klickt oder eine infizierte Website besucht. Erpressungssoftware ist auf dem Vormarsch. Dabei verschlüsseln Angreifer den Inhalt eines Geräts und machen es dadurch nutzlos. Dann verlangen sie ein Lösegeld, um die Daten zu entsperren.

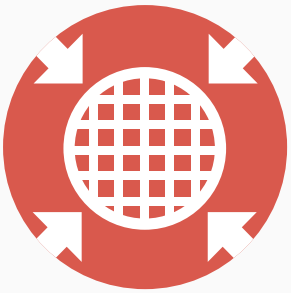
An 39% der Crimeware-Vorfälle im Jahr 2015 war Erpressungssoftware beteiligt.



Was können Sie tun?

- **Patches sofort einspielen:** Internetkriminelle nutzen erfolgreich bekannte Schwachstellen aus, eine rechtzeitige Aktualisierung könnte viele Angriffe blockieren.
- **Einführung einer Überwachung von Konfigurationsänderungen:** Viele Angriffsmethoden können leicht durch die Beobachtung von Kennzahlen überwacht werden.
- **Sicheren Sie Ihre Systeme regelmäßig:** Dadurch wird Ihr Betrieb am Laufen gehalten, sollte eines der Systeme durch Erpressungssoftware gesperrt sein.
- **Daten über Angriffe erfassen:** Untersuchen Sie die verschiedenen Arten von Malware, die bei Ihnen aufgetreten sind – und, falls möglich, den Eintrittspunkt. Dadurch erhalten Sie Kenntnis darüber, wo Sie Ihre Bemühungen verstärken müssen.

Angriffe von Web-Apps

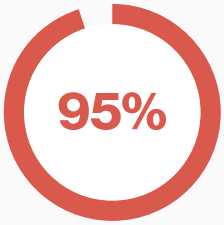


Wenn eine Web-App – beispielsweise ein Content Management System (CMS) oder eine E-Commerce-Plattform – als Mittel zum Eindringen verwendet wurde.

Am meisten betroffene Branchen:
Finanzdienstleistungen, Einzelhandel, Information

Viele Web-App-Angriffe erfolgen willkürlich – die Angreifer finden ein schwaches Ziel mit einer Verwundbarkeit, die sie ausnutzen können, oder sie erhalten Zugriff über eine Phishing-Kampagne. Internetkriminelle waren sehr erfolgreich bei der Verwendung von CMS-Plugins zum Einschleusen bösartiger Software. Ist sie einmal im System, wird die Website des Ziels durch viele Angriffe unkenntlich gemacht. Aber wir haben fast 20.000 Vorfälle erlebt, bei denen die betroffenen Websites für Angriffe durch verteilte Dienstblockaden (Distributed Denial of Service/DDoS) genutzt oder zu Phishing-Seiten umfunktioniert wurden.

95% der Web-App-Angriffe, bei denen von Kriminellen Daten gestohlen wurden, waren finanziell motiviert.



Was können Sie tun?

- **Verwenden Sie eine Zwei-Faktor-Authentifizierung:** Und sperren Sie nach wiederholten Fehlversuchen das Konto. Sie sollten auch über die Verwendung biometrischer Daten nachdenken.
- **Patches sofort einspielen:** Führen Sie ein robustes Verfahren für die Patches von CMS-Plattformen ein, einschließlich der Plugins von Drittanbietern und der E-Commerce-Systeme. Siehe “Effektive Aktualisierung kann sie stoppen” auf Seite 10.
- **Alle Eingaben überwachen:** Überprüfen Sie alle Ihre Protokolle, um bösartige Aktivitäten besser zu erkennen.

Eindringen über Verkaufsstellen (Point-of-Sale/POS)

Wenn Angreifer die Computer und Server, auf denen POS-Anwendungen laufen, beeinträchtigen, mit dem Ziel, die Zahlungsdaten abzufangen.

Am meisten betroffene Branchen:
Unterkünfte, Einzelhandel

Im Jahr 2015 schafften es Hotelketten aufgrund von Sicherheitsverletzungen bei Internet-Zahlungen mit Bankkarte in die Schlagzeilen. Im Jahr 2014 waren es große Einzelhändler. Ein erfolgreiches Eindringen erfolgt häufig über einen POS-Hersteller und weniger als Ergebnis von schlecht konfigurierten, mit dem Internet verbundenen POS-Geräten.

An 95% der bestätigten Sicherheitsverletzungen bei Bewirtungsunternehmen war das Eindringen in POS beteiligt.

Was können Sie tun?

- **Patches für Server sofort einspielen:** Und nur den Personen
  Zugang gewähren, die ihn unbedingt benötigen.
- **Wählen Sie Ihren Anbieter sorgfältig aus:** Stellen Sie sicher, dass die Anbieter für Ihren Cloud-Dienst Lösungen umgesetzt haben, um Ihre Systeme zu schützen.
- **Reservieren Sie POS-Systeme für POS-Aktivitäten:** Erlauben Sie den Mitarbeitern nicht, diese für das Internet, zum Abrufen von E-Mails oder zum Spielen zu verwenden.
- **Verwenden Sie eine Zwei-Faktor-Authentifizierung:** Ihr POS-Anbieter sollte eine Zwei-Faktor-Authentifizierung verwenden.

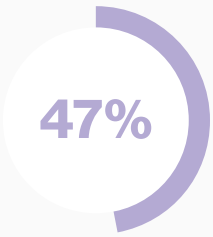
Cyber-Spionage

Von Spionage motivierte Angriffe, die durch mit einem Staat verbundene Akteure ausgeführt werden, die häufig nach geistigem Eigentum suchen.

Am meisten betroffene Branchen:
Produktion, Information, freie Berufe

Diese Angriffe beginnen in der Regel mit den gleichen Werkzeugen und Techniken, die an anderer Stelle erfolgreich verwendet werden, bevor sie zu ausgereifteren Methoden übergehen. Das bedeutet, dass die grundlegenden Sicherheitsmaßnahmen beim Schutz gegen Cyber-Spionage überraschend wirksam sind und nicht zugunsten eines speziellen Schutzes vergessen werden dürfen.

47% aller bestätigten Sicherheitsverletzungen in Produktionsbetrieben können als Cyber-Spionage klassifiziert werden.



Was können Sie tun?

- **Patches sofort einspielen:** Internetkriminelle nutzen erfolgreich bekannte Schwachstellen aus, eine rechtzeitige Aktualisierung könnte viele Angriffe blockieren.
- **Einführung einer Überwachung von Konfigurationsänderungen:** Viele Angriffsmethoden können leicht durch die Beobachtung von Kennzahlen überwacht werden.
- **Getrennte Systeme:** Stellen Sie sicher, dass ein betroffener Desktop keinen Zugang zu kritischeren Systemen und Daten bietet.

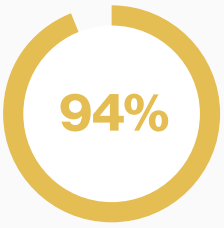
Auslesen von Bankkarten

Zwischenfälle mit physisch installierten Geräten an einem Geldautomaten, einer Zapfsäule oder einem POS-Terminal, die Kartendaten auslesen.

Am meisten betroffene Branchen:
Finanzdienstleistungen, Einzelhandel, Unterkünfte

Die meisten dieser Angriffe gibt es an Geldautomaten, es tauchen aber auch Zapfsäulen und andere Geräte auf. Auslesevorrichtungen können auch für das geübte Auge fast unmöglich zu erkennen sein.

94% der Sicherheitsverletzungen durch Auslesen von Karten fanden an Geldautomaten statt.



Was können Sie tun?

- **Nutzen Sie manipulationssichere Terminals:** Einige Terminals sind anfälliger für Manipulationen als andere. Wählen Sie eines, das entwickelt wurde, um Verbrecher abzuschrecken.
- **Achten Sie auf Manipulationen:** Führen Sie ein Verfahren zur regelmäßigen Integritätsprüfung von Kartenlesern an Geldautomaten und Zapfsäulen ein. Schulen Sie Ihre Mitarbeiter darauf, Auslesevorrichtungen zu erkennen und machen Sie es den Mitarbeitern leicht, alles Verdächtige zu melden.
- **Verwenden Sie manipulationssichere Kontrollen:** Das kann etwas so Einfaches wie ein Siegel über der Tür einer Zapfsäule sein.

Die Bösewichter sind schneller

Internet-Kriminelle können innerhalb von Minuten eindringen und Daten stehlen (herausfiltern). In 93% der Fälle, in denen Daten gestohlen wurden, wurde innerhalb von Minuten oder noch schneller in die Systeme eingedrungen. In 28% der Fälle fand das Herausfiltern innerhalb von Minuten statt. Aber selbst dann, wenn das Herausfiltern Tage dauerte, hatten die Kriminellen nichts zu befürchten. In 83% der Fälle fanden die Opfer über Wochen oder noch länger nicht heraus, dass es einen Datendiebstahl gab.

Je länger Sie benötigen, um eine Sicherheitsverletzung zu entdecken, desto mehr Zeit haben die Kriminellen, um die wertvollen Daten zu finden, nach denen sie suchen und um Ihre Geschäftstätigkeit zu stören. Aus diesem Grund ist Schutz nicht genug – Sie benötigen wirksame Systeme und Verfahren zur Erkennung und Beseitigung, um Angriffe zu vereiteln und den möglichen Schaden zu verringern.

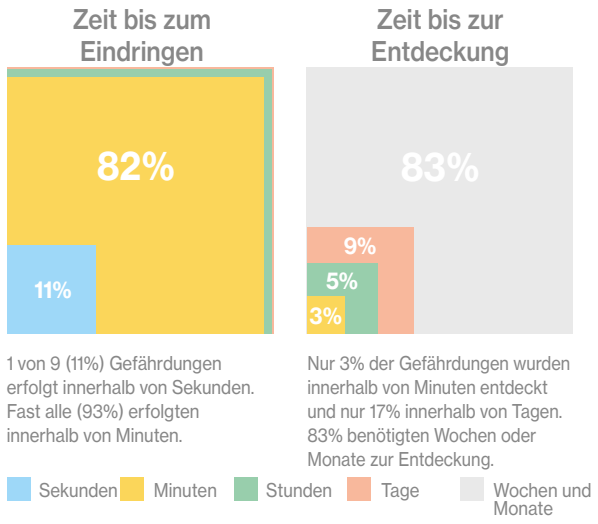


Abbildung 3: Zeitachse Sicherheitsverletzung

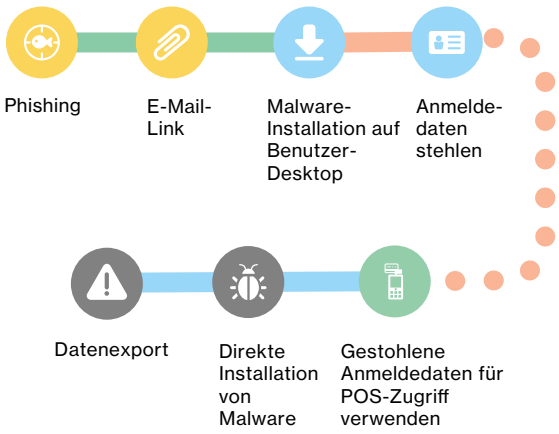


Abbildung 4: Geburt und Wiedergeburt eines Datenlecks

Wie sie zuschlagen

Die Bausteine eines Angriffs zu verstehen, kann Ihnen dabei helfen, eine solide Abwehr zu schaffen und eine Sicherheitsverletzung schnell zu erkennen, wenn sie auftritt.

Selbst ausgereifte Angriffe teilen sich DNA mit den einfachsten Angriffen. Die einzelnen Teile eines Angriffs erfolgen jedoch nicht immer in der gleichen Reihenfolge. Und Sie stehen nicht nur jeweils einem Angriff gegenüber. Grafische Darstellungen von Angriffen können dabei helfen, die gesamte Angriffsfläche hervorzuheben, nicht nur die Wege, die Sie gesehen haben.

Effektive Aktualisierung kann sie stoppen

Die 10 wichtigsten Schwachstellen [Häufige Schwachstellen und Expositionen (Common Vulnerabilities and Exposures/CVEs)] auf die 85% des erfolgreichen illegalen Datenverkehrs entfielen. Die anderen 15% umfassen mehr als 900 CVEs.

Schnelles Patchen ist wichtig, bei so vielen neuen Schwachstellen, die entdeckt werden, ist es schwer festzustellen, wo man anfangen soll. Der diesjährige DBIR liefert wertvolle Informationen, die Ihnen dabei helfen, dieses Problem zu lösen.

Die von Kenna Security bereitgestellten Daten legen nahe, dass die Schwachstellen in Adobe-Produkten am schnellsten ausgenutzt wurden, die in Mozilla-Produkten am langsamsten – siehe Abbildung 5. Die Analyse dieser Informationen wird Ihnen helfen, von der Durchführung von "Notfallübungen" wegzukommen und sich auf Patches zu konzentrieren.

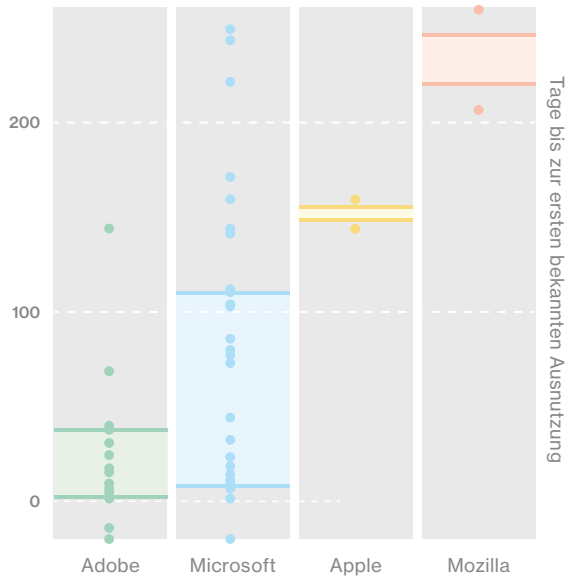


Abbildung 5: Tage bis zur ersten bekannten Ausnutzung

Nutzen Sie Informationen, die Gauner tun es auch!

Die Internetkriminellen sind mit der derzeitigen Situation nicht zufrieden. Da der Wert einiger Datenformen fällt, werfen sie ihre Netze weiter aus und verbessern ihre Taktik.

Kein System ist zu 100% sicher, aber viele Unternehmen machen es den Kriminellen einfach. Sie schließen bekannte Schwachstellen nicht und lassen ihre Mitarbeiter einfach zu erratende Passwörter verwenden – häufig bleiben sogar die Standardeinstellungen erhalten, mit denen das Gerät geliefert wird.

Das bedeutet, dass viele Sicherheitsverletzungen, die wir gesehen haben, vermeidbar gewesen wären, wenn die Unternehmen grundlegende Sicherheitsmaßnahmen umgesetzt hätten. Unsere sieben Tipps auf der rechten Seite decken die einfachen Fehler ab, die wir immer und immer wieder sehen.

Aber Ihr IT-Team sollte ein umfassendes Verständnis für die Bedrohungen haben, denen Ihr Unternehmen ausgesetzt ist. Internet-Kriminelle nutzen alle Informationen, die sie bekommen können, für Ihr böses Spiel. Das sollten Sie auch. Der Data Breach Investigations Report 2016 ist ein Muss für jedes Unternehmen, das Internetsicherheit ernst nimmt.

Schnellüberblick

- **Seien Sie wachsam:** Protokolldateien und Änderungsmanagement-Systeme können Ihnen bei einer Sicherheitsverletzung eine frühzeitige Warnung geben.
- **Machen Sie Menschen zu Ihrer ersten Verteidigungslinie:** Schulen Sie Ihre Mitarbeiter darauf, die Warnzeichen zu erkennen.
- **Halten Sie Daten nur nach dem Prinzip "Kenntnis nur nach Bedarf":** Es erhalten nur Mitarbeiter den Zugang zu den Systemen, die diesen zur Erledigung ihrer Aufgaben benötigen.
- **Patches sofort einspielen:** Das kann vor vielen Angriffen schützen.
- **Verschlüsseln Sie sensible Daten:** Machen Sie Ihre Daten bei Diebstahl so gut wie nutzlos.
- **Verwenden Sie eine Zwei-Faktor-Authentifizierung:** Damit kann der Schaden bei verlorenen oder gestohlenen Anmeldeinformationen begrenzt werden.
- **Vergessen Sie nicht die physische Sicherheit:** Nicht alle Datendiebstähle geschehen online.

Holen Sie sich den Data Breach Investigations Report 2016

Der DBIR ist unsere wichtigste jährliche Veröffentlichung zur Sicherheit und eine der branchenweit angesehensten Informationsquellen. Neben dem vollständigen Bericht und dieser Zusammenfassung veröffentlichen wir auch eine Anzahl weiterer Ressourcen, um Sie beim Verständnis der Bedrohungen und der Verbesserung Ihrer Abwehrmaßnahmen zu unterstützen. Sehen Sie es sich an.

Erhalten Sie unseren vollständigen DBIR 2016 und andere nützliche Ressourcen.

Weiterlesen ›

Machen Sie bei der Internetsicherheit etwas falsch? Sehen Sie sich SlideShare an.

SlideShare ›

VerizonEnterprise.com