2017 Data Breach Investigations Report

Kurzfassung

verizon

Überblick

Zum zehnten Mal beschäftigt sich Verizons Data Breach Investigations Report (DBIR) mit der düsteren Welt der Netzsicherheit. Er vereint die kollektive Erfahrung von 65 Unternehmen, um Ihnen ein vollständiges Bild über Cyberkriminalität zu vermitteln.

Wer steckt hinter den Angriffen?

75% von Außenstehenden verübt.

25% mit Beteiligung interner Akteure.

18% von staatsnahen Akteuren durchgeführt.

3% betrafen mehrere Parteien.

2% mit Beteiligung von Partnern.

51% mit Beteiligung von Gruppen der organisierten Kriminalität.

Wie erfolgen die Angriffe?

62% der Angriffe beruhten auf Hacking.

51% der Angriffe erfolgten mittels Malware.

81% der Hacker-Angriffe nutzten entweder gestohlene und/oder schwache Passwörter.

43% waren Angriffe auf soziale Netzwerke.

14% der Angriffe wurden durch Fehler ausgelöst. Der gleiche Anteil umfasste den Missbrauch von Nutzerdaten.

8% der Angriffe erfolgten durch direkten Zugriff auf die Hardware.

Wer sind die Opfer?

24% der Angriffe betrafen Finanzunternehmen.

15% der Angriffe zielten auf Unternehmen im Gesundheitswesen.

12% Einrichtungen des öffentlichen Sektors waren mit 12 % die dritthäufigsten Opfer von Angriffen.

15% der Angriffe entfielen auf den Einzelhandel und die Hotelbranche.

Was haben sie sonst noch gemeinsam?

66% der Malware wurde über schädliche E-Mail-Anhänge eingeschleust.

73% der Angriffe hatten finanzielle Beweggründe.

21% der Angriffe standen im Zusammenhang mit Spionage.

27% der Angriffe wurden durch Dritte entdeckt.

Setzen Sie Ihre Zukunft aufs Spiel?

Wenn Sie noch nicht angegriffen wurden und noch keine Daten verloren haben, waren Sie entweder unglaublich gut vorbereitet oder hatten äußerst viel Glück. Sind sie unglaublich gut vorbereitet?

Niemand glaubt, dass es ihn selbst einmal treffen werde. Bis es dann passiert ist.

Hollywood ist für viele Dinge verantwortlich. Im Film arbeiten Cyberkriminelle in schlecht beleuchteten, stillgelegten Lagerhallen, greifen sorgfältig ausgewählte Großkonzerne an und verwenden Dinge wie „Würmer“ und „Schlüssel“, um sich Zugang zu verschaffen. Dieses Zerrbild hat vielen ein falsches Gefühl der Sicherheit vermittelt, weil sie glauben, dass ein Angriff auf die eigenen Daten etwas ist, was nur anderen passieren könne.

Tatsächlich passen Cyberkriminelle selten in dieses Profil. Sie sind opportunistisch und gehen nach dem Gießkannenprinzip vor: Sie nutzen etwa Phishing, um Schwachstellen aufzuspüren, die sie als Ausgangspunkt für ihren Angriff verwenden können. Die Weltherrschaft ist dabei selten ihre Absicht, meist wollen sie nur Geld.

Egal ob es sich um Konstruktionspläne, Gesundheitsakten oder die guten alten Daten von Zahlungskarten handelt – irgendwo auf der Welt wird dies jemand als ihre perfekte Gelegenheit ansehen. Den meisten Cyberkriminellen ist es egal, wem sie etwas stehlen.

61%

der Opfer von Angriffen und Datenverlusten im diesjährigen Bericht sind Unternehmen mit weniger als 1.000 Mitarbeitern.

95%

der Phishing-Angriffe, die zu einem Datenverlust führten, installieren später auch noch eine Schadsoftware.

Unternehmen glauben, die Grundlagen abgedeckt zu haben.

Es fallen immer noch Menschen auf Phishing herein – ja, immer noch. Laut dem diesjährigen DBIR wurde etwa einer von 14 Nutzern dazu gebracht, einen Link anzuklicken oder einen Dateianhang zu öffnen – und ein Viertel von ihnen wurde in der Folge mehr als einmal getäuscht. Dort, wo Phishing erfolgreich Türen öffnete, kam es dann üblicherweise mittels Malware zum Abgreifen von Daten – oder es konnte sogar die Kontrolle über die Systeme erlangt werden.

Viele Nutzer verwenden noch immer keine sicheren Passwörter.

80 % der Hacker-Angriffe erfolgten entweder durch gestohlene und/oder unsichere oder leicht zu erratende Passwörter.

Auf den Seiten 6–7 erfahren Sie mehr über die neun Angriffsmuster, die 88 % der untersuchten Angriffe abdecken.

Die Menschen vertrauen auf ihre altbewährten Vorgehensweisen.

Viele Unternehmen verlassen sich noch immer auf veraltete Schutzmechanismen. Es ist verlockend, die gleichen Schutzmechanismen Jahr für Jahr beizubehalten, insbesondere wenn kein größerer Vorfall zu beklagen war. Aber sind diese Mechanismen tatsächlich an die Bedrohungen angepasst, denen Unternehmen wie Ihres heute gegenüberstehen?

Auf den Seiten 4–5 erfahren Sie mehr über die Bedrohungen, die nach unseren Erkenntnissen in Ihrer Branche am weitesten verbreitet sind.

Verteidigen Sie sich klug

Während Angreifer neue Methoden und Tricks anwenden, sind ihre Strategien insgesamt relativ unverändert geblieben. Das Verständnis dieser Strategien ist wichtig, um zu wissen, wie Sie Ihr Unternehmen vor Cyberangriffen schützen können.

88%

der Angriffe fallen in die neun Muster, die wir im Jahr 2014 zum ersten Mal identifiziert haben.

Das Verständnis dieser Angriffsmuster hilft Sicherheitsexperten, sich einen Überblick darüber zu verschaffen, wo und wie sie am besten ihre begrenzten Ressourcen einsetzen sollten. Für alle anderen bieten diese Muster eine schnelle und einfache Möglichkeit zu beurteilen, wo eine zukünftige Gefährdung am wahrscheinlichsten ist. Wenn Sie also eine neue App in Betrieb nehmen oder einen neuen Prozess aufbauen, können Sie von Anfang an Sicherheit einbauen.

Im Data Breach Digest 2017 finden Sie Beispiele, wie sich diese Angriffsmuster im wirklichen Leben abspielen können. Jedes der 16 Szenarien des DBD veranschaulicht jeweils eines dieser Angriffsmuster.

Crimeware

Alle Fälle unter Einsatz von Schadsoftware, die in kein bestimmtes Muster passten.

Ransomware ist das große Geschäft

Im DBIR 2014 war Ransomware die 22st-häufigste Form von Schadsoftware. In diesem Jahr steht sie an der fünften Stelle, und sie ist das am häufigsten vorkommende Crimeware-Muster. Aus Sicht der Angreifer ist der Diebstahl von Dateien gegen Lösegeld ein schnelles und einträgliches Geschäft mit einem geringen Risiko – insbesondere bei der Nutzung von Bitcoins, die anonyme Zahlungen erlauben.

Das können Sie tun

Achten Sie auf MS-Office-Dokumente mit aktiviertem Makromodus, und weisen Sie immer wieder auf die Wichtigkeit von Software-Updates hin.

Cyber-Spionage

Angriffe im Zusammenhang mit staatsnahen Akteuren und/oder mit Spionageabsichten.

Sie lassen es langsam angehen

Bösartige E-Mails sind für Cyber-Spione die erste Wahl. Aber hier geht es nicht um eine schnelle Aktion. Nach der ursprünglichen E-Mail folgen in der Regel Methoden, die darauf abzielen, Zugriff zu erhalten, damit der Angreifer die Zeit hat, die benötigten Daten abzugreifen.

Das können Sie tun

Führen Sie Schulungen durch, die die Sensibilität für das Thema Sicherheit erhöhen und ermutigen Sie Ihre Teams, verdächtige E-Mails zu melden Erschweren Sie es Ihrem Gegner, von einem manipulierten Rechner aus auf andere Geräte in Ihrem Netzwerk zuzugreifen.

Denial-of-Service-Angriffe

Jeder Angriff, der die Verfügbarkeit von Netzwerken und Systemen beeinträchtigen soll.

Getroffen werden, wo es weh tut

Die Ziele von DDoS-Angriffen sind fast immer (zu 98 %) große Unternehmen. Während manche vom Pech verfolgten Organisationen das ganze Jahr über Ziel von Angriffen sind, sind die meisten Angriffe innerhalb weniger Tage vorbei.

Das können Sie tun

Vergewissern Sie sich, dass Sie DDoS-Abwehrlösungen eingerichtet haben, dass diese regelmäßig überprüft werden und auch tatsächlich funktionieren.

Missbrauch von Insider-Informationen und Zugangsrechten

Jede unberechtigte oder missbräuchliche Verwendung von Ressourcen eines Unternehmens.

Der Feind im Inneren

In 60 % der Fälle tauchen Insider mit Daten unter, in der Hoffnung, diese in Geld verwandeln zu können. Manchmal jedoch handelt es sich um unerlaubtes Schnüffeln (17 %), oder die Daten werden mit zu einem neuen Arbeitgeber genommen, oder sie werden eingesetzt, um ein Konkurrenzunternehmen aufzubauen (15 %).

Das können Sie tun

Beschränken, protokollieren und überwachen Sie die Nutzung der Daten, und achten Sie auf große Datentransfers sowie die Verwendung von USB-Geräten.

Diverse Fehler

Unbeabsichtigte Aktionen, die unmittelbar die Sicherheit von Unternehmensdaten beeinträchtigen.

Es wurden Fehler gemacht

Sie können harmlos erscheinen, aber auch der Datenverlust durch Fehler kann Schaden anrichten. Vor allem, wenn es – wie in 76 % der Fälle – Ihr Kunde ist, der Sie auf die Panne aufmerksam macht.

Das können Sie tun

Legen Sie ein Verfahren zur Entsorgung sämtlicher vertraulicher Daten fest und setzen Sie es durch. Wenden Sie darüber hinaus das Vier-Augen-Prinzip bei der Veröffentlichung von Informationen an.

Physischer Diebstahl und Verlust von Daten

Jeder Vorfall, bei dem physische Ressourcen abhanden kommen –absichtlich oder versehentlich.

Menschen verlieren Dinge

Maßnahmen wie zum Beispiel Verschlüsselung können verhindern, dass gestohlene oder verlorene Daten missbräuchlich verwendet werden können. Verschlüsselung hilft jedoch nicht in jedem Fall. Bei der Mehrheit der bestätigten Vorfälle wurden gedruckte Dokumente entwendet.

Das können Sie tun

Verschlüsseln Sie, wo immer dies möglich ist, und fördern Sie eine Unternehmenskultur, die das Ausdrucken sensibler Daten missbilligt.

Auslesen von Zahlungskarten -

Alle Vorfälle, bei denen ein sogenanntes Aufsatzgerät auf einen Zahlungskartenleser platziert wurde.

Mit Vollgas

Während Geldautomaten weiterhin das Hauptziel von Auslese-Angriffen sind, hat sich die Anzahl der Angriffe auf Tankstellen-Endgeräte zum Abgreifen von Zahlungskartendaten im Vergleich zum DBIR des vergangenen Jahres mehr als verdreifacht. Skimming-Angriffe werden fast immer von Dritten entdeckt.

Das können Sie tun

Schulen Sie Ihre Mitarbeiter, damit sie Anzeichen einer Manipulation erkennen können. Kontrollieren Sie Zahlungsterminals per Videoüberwachung und stellen Sie sicher, dass die Aufnahmen regelmäßig angesehen werden.

Angriffe über Webanwendungen

Jeder Vorfall, bei dem eine Webanwendung als Angriffsmittel diente.

Machen Sie es Betrügern nicht zu leicht

Nicht alle Webseiten speichern die Daten von Zahlungskarten, aber häufig muss sich der Kunde anmelden, d. h. er muss seinen Namen, seine Anschrift und weitere Informationen angeben. Die Sicherheit ist hier oft schwächer als bei Seiten des Onlinehandels, sodass Angreifer hier leicht an personenbezogene Daten und Anmeldeinformationen gelangen, die sie dann anderswo nutzen können.

Das können Sie tun

Ermutigen Sie Ihre Kunden, verschiedene Passwörter zu verwenden und nutzen Sie die Zwei-Faktor-Authentifizierung. Begrenzen Sie die Menge an vertraulichen Informationen, die in webbasierten Anwendungen gespeichert werden.

Datendiebstahl am Point-of-Sale

Remote-Angriffe gegen POS-Terminals und -Controller.

Ertragreiche POS-Angriffe

Point-of-Sale (POS)-Umgebungen liefern Betrügern üppige Erträge. Fast 98 % aller erfassten POS-Angriffe führten zu einem bestätigten Abfluss von Daten. Der Fokus der Angriffe hat sich von Hotelketten hin zu Restaurants und kleineren Unternehmen verschoben.

Das können Sie tun

Fordern Sie von externen POS-Anbietern eine Überprüfung ihrer Sicherheitspraktiken – unter besonderer Berücksichtigung des Remote-Zugriffs.

Alle sonstigen Angriffe

Sämtliche Vorfälle, die nicht einem der neun Angriffsmuster entsprechen.

Vorsicht vor Betrügern

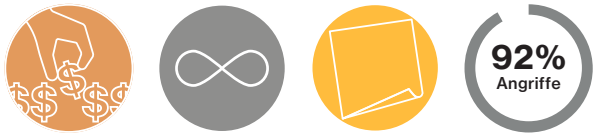
Dies ist vielleicht eine sehr allgemein gehaltene Kategorie, was aber nicht bedeuten soll, dass es keine interessanten und wichtigen Trends gäbe. Eine wichtige neue Taktik sind gefälschte E-Mails, bei denen „der Geschäftsführer“ Überweisungen anordnet und das mit einer glaubwürdigen Geschichte mit großer Dringlichkeit begründet.

Das können Sie tun

Verdeutlichen Sie Ihren Mitarbeitern – insbesondere jenen im Bereich Finanzen – dass niemand eine Zahlung außerhalb der autorisierten Prozesse verlangen wird. Weisen Sie außerdem die IT-Abteilung an, externe E-Mails mit einer unverwechselbaren Kennzeichnung zu versehen.

Erkennen Sie Ihre Bedrohungen

Hotelbranche



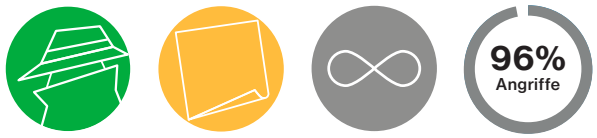
Bildungseinrichtungen

Finanzdienstleistungen

Gesundheitswesen

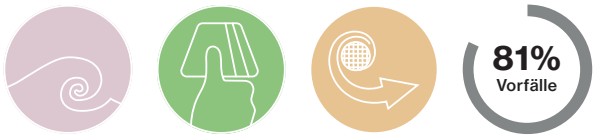
Informationsdienstleister

Fertigung



Öffentlicher Sektor

Einzelhandel



Richten Sie Ihre Abwehrmaßnahmen aus

Auf einer Expedition zum Nordpol würden Sie wahrscheinlich Ihre Shorts zu Hause lassen und stattdessen mehr Thermounterwäsche einpacken. Das Gleiche gilt für die Beurteilung, wofür Sie Ihr begrenztes Budget ausgeben möchten. Die oben abgebildeten Bewertungskarten helfen Ihnen, ein besseres Verständnis der Methoden zu erlangen, die gegen andere Unternehmen Ihrer Branche eingesetzt wurden. Wenn Sie wissen, wo die größten Gefährdungen bestehen, können Sie Ihre Abwehrmaßnahmen den Bedrohungen anpassen.

Sie müssen nicht groß oder berühmt sein

Die Gefährdung durch Innentäter ist im Gesundheitswesen nichts Neues. Es geht hier jedoch nicht darum, dass jemand einen kurzen Blick auf Patientendaten wirft, um den Namen oder das Geschlecht des Nachwuchses einer bekannten Persönlichkeit in Erfahrung zu bringen, bevor diese Informationen in der Presse erscheinen. Häufig geht es vielmehr um Identitätsdiebstahl und die missbräuchliche Verwendung der Daten ganz normaler Menschen.

Gleichermaßen sind es nicht nur bekannte Marken, die sich auf den Wunschlisten von Cyber-Spionen befinden. Start-ups sind z. B. werden aufgrund ihrer bahnbrechenden Technologien angegriffen. Etabliertere Unternehmen werden häufig aufgrund ihrer Umsätze zum Opfer. Und andere wiederum dienen als sogenannte „weiche Ziele“, als Ausgangspunkt, um in die Systeme ihrer Geschäftspartner einzudringen.

Nutzen Sie die neuesten Erkenntnisse – die Betrüger tun es auch!

Cyberkriminelle sind nicht mit dem Status Quo zufrieden. Wenn der Wert bestimmter Daten fällt, werfen sie ihre Netze weiter aus und verbessern ihre Methoden. Kein System ist zu 100 Prozent sicher, aber zu viele Unternehmen machen es ihnen leicht.

Täuschung der Mitarbeiter oder soziale Manipulation ist für Cyberkriminelle ein häufiges Mittel, um in ein System eindringen zu können. Mitarbeiter machen es ihnen einfach, indem sie leicht zu erratende Passwörter verwenden. Nutzer und sogar manche IT-Abteilungen machen sich mitschuldig, indem sie die werksseitigen Standard-Passwörter von Geräten unverändert weiternutzen. Diese lassen sich natürlich bequem im Internet herausfinden.

Das bedeutet, viele der von uns untersuchten Angriffe wären vermeidbar gewesen, wenn Unternehmen einige grundlegende Sicherheitsmaßnahmen eingeführt hätten. Unsere nachfolgenden sieben Tipps decken auf einfach abzustellende Fehler ab, die jedoch immer wieder gemacht werden.

Ihr IT-Team sollte dennoch über ein tiefgreifendes Verständnis der Bedrohungen verfügen, denen Ihr Unternehmen ausgesetzt ist. Cyberkriminelle verwenden alle Informationen, die sie bekommen können, um sich immer weiter zu verbessern. Sie sollten das ebenfalls tun. Der Data Breach Investigations Report (DBIR) 2017 ist ein Muss für jedes Unternehmen, dem ernsthaft etwas an Netzsicherheit gelegen ist.

Die wichtigsten Erkenntnisse

Seien Sie aufmerksam
Logdateien und Change-Management-Systeme können Sie frühzeitig vor einem Datendiebstahl warnen.

Ihre Mitarbeiter sind Ihr erster Schutz
Schulen Sie Ihre Mitarbeiter, damit diese die Warnsignale erkennen können.

Datenzugänge nach dem Notwendigkeitsprinzip
Nur Mitarbeiter, die zum Erledigen ihrer Arbeit Zugang zu Systemen benötigen, sollten einen Zugriff erhalten.

Schließen Sie Schwachstellen umgehend
Dies könnte vor vielen Angriffen schützen.

Verschlüsseln Sie vertrauliche Daten
Sorgen Sie dafür, dass Ihre Daten bei einem Diebstahl praktisch wertlos sind.

Verwenden Sie die Zwei-Faktor-Authentifizierung
Diese kann den Schaden durch verloren gegangene oder gestohlene Anmeldedaten begrenzen.

Denken Sie an die physische Sicherheit
Nicht jeder Datendiebstahl geschieht über das Internet.

Möchten Sie mehr erfahren?

DBIR 2017
Laden Sie den Data Breach Investigations Report (DBIR) 2017 herunter. Dieser Bericht ist unsere wichtigste Veröffentlichung zur IT-Sicherheit und eine der branchenweit angesehensten Informationsquellen.

DBD 2017
Lesen Sie im Data Breach Digest mehr über die faszinierendsten Untersuchungen von Verizon zur Cyberkriminalität . Erfahren Sie mehr über Angriffsmethoden, Fehler der Opfer und wie man den Schaden begrenzen kann.

VerizonEnterprise.com/de