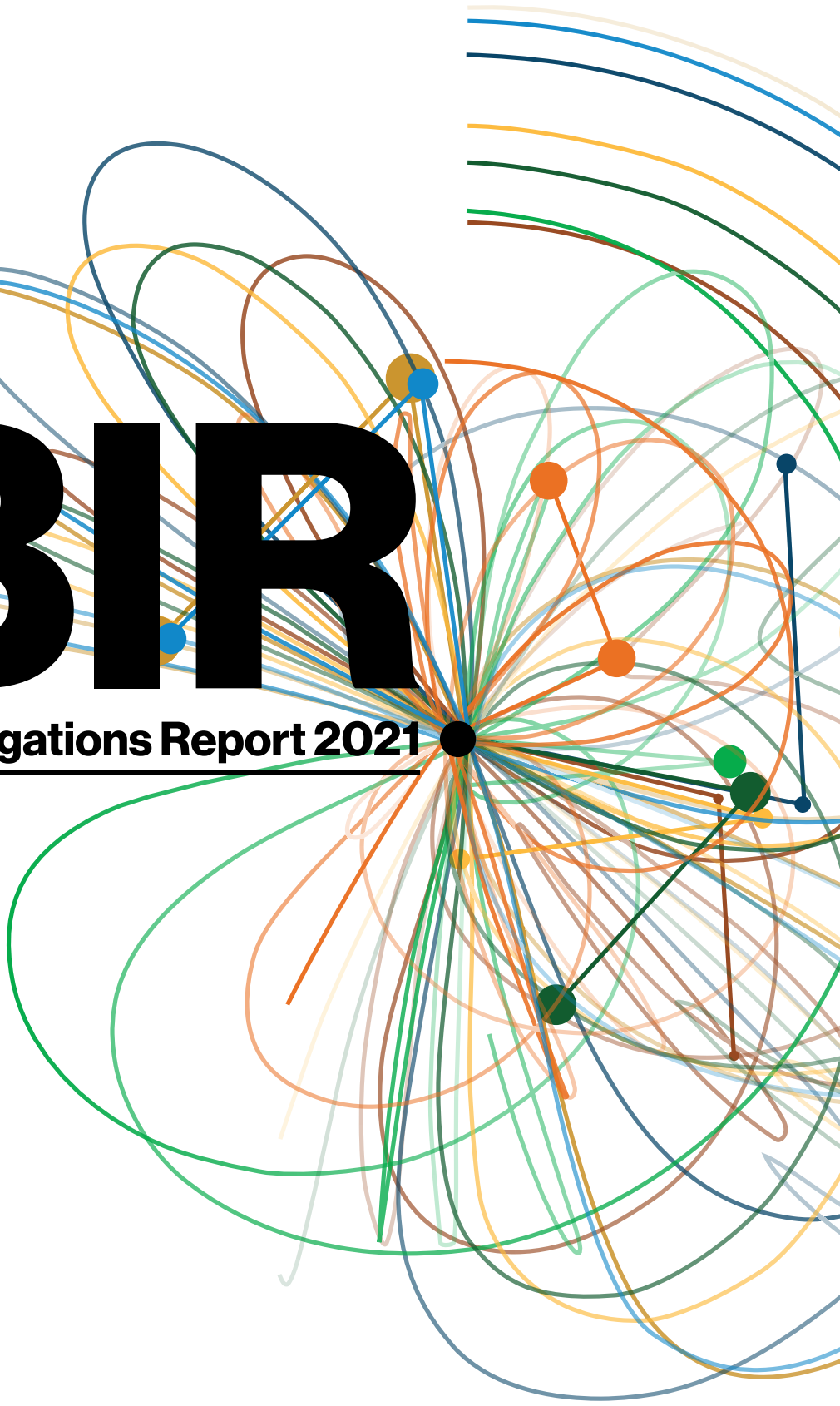
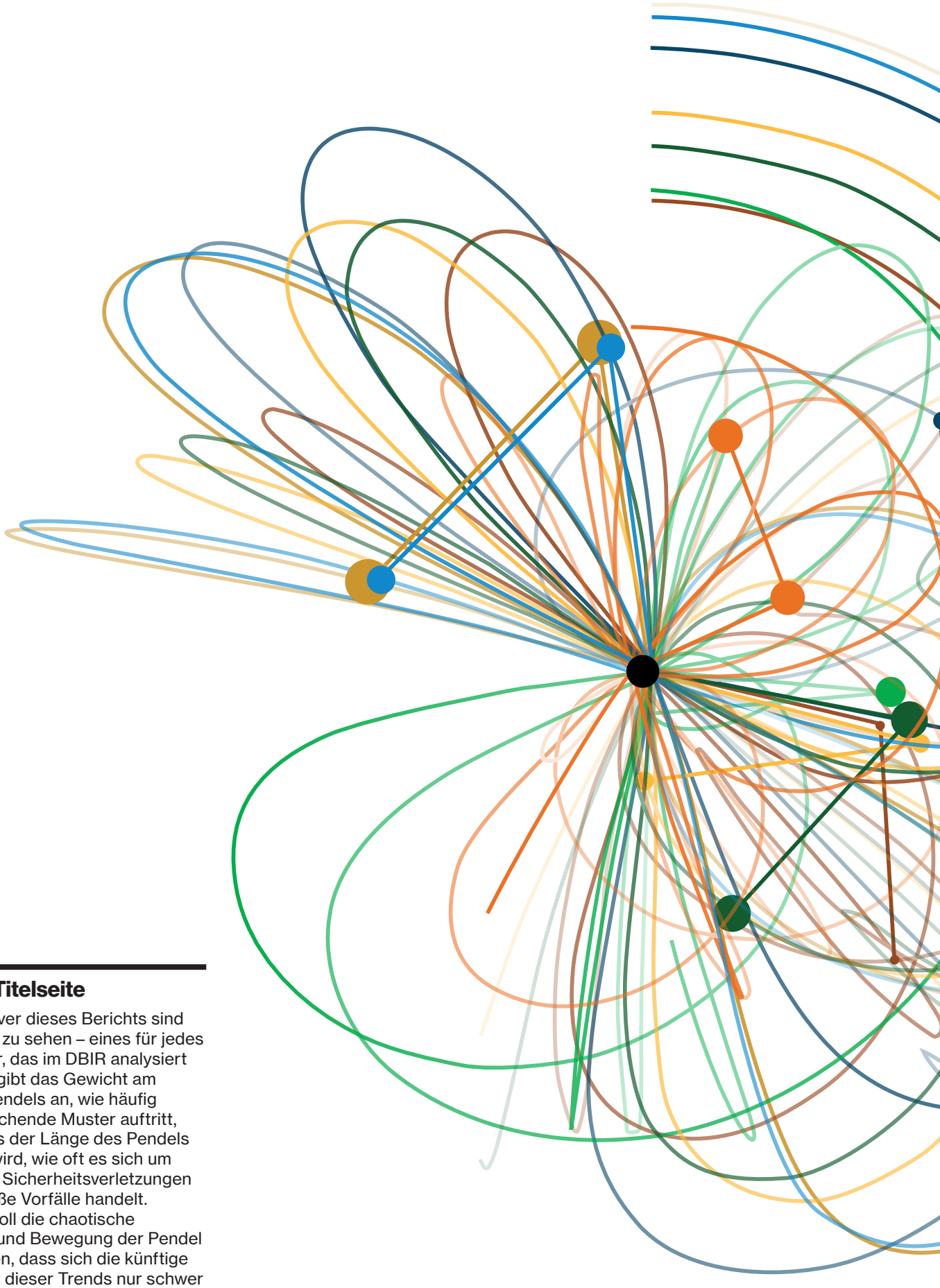
DBIR

Data Breach Investigations Report 2021

Kurzfassung



verizon



Über die Titelseite

Auf dem Cover dieses Berichts sind acht Pendel zu sehen – eines für jedes neue Muster, das im DBIR analysiert wird. Dabei gibt das Gewicht am Ende des Pendels an, wie häufig das entsprechende Muster auftritt, während aus der Länge des Pendels ersichtlich wird, wie oft es sich um gravierende Sicherheitsverletzungen statt um bloße Vorfälle handelt. Außerdem soll die chaotische Anordnung und Bewegung der Pendel verdeutlichen, dass sich die künftige Entwicklung dieser Trends nur schwer abschätzen lässt.

Inhaltsverzeichnis

Gut gewappnet für eine Welt im Wandel

Die Geschäftswelt wird immer wieder von tiefgreifenden Veränderungen erschüttert, die meist plötzlich und ohne vorherige Ankündigung eintreten. In diesen Fällen sind Unternehmen aufgefordert, schnell zu handeln und sich umgehend auf die neue Lage einzustellen. Dabei kommt es vor allem auf eine solide Entscheidungsgrundlage an, die den Verantwortlichen eine gezielte Vorbereitung auf die wahrscheinlichsten Eventualitäten ermöglicht. Deshalb veröffentlicht Verizon einmal jährlich den Data Breach Investigations Report (DBIR). An der Entstehung der jüngsten, 14. Ausgabe waren insgesamt 83 Institutionen und Unternehmen beteiligt – und damit mehr Mitwirkende als jemals zuvor. Insgesamt hat das mit der Erstellung beauftragte Team 29.207 Vorfälle untersucht, von denen 5.258 als schwerwiegende Sicherheitsverletzungen eingestuft wurden.

In diesem Datensatz haben wir mithilfe eines auf maschinellem Lernen basierenden Clustering-Verfahrens sieben typische Angriffs- und Vorfallsmuster identifiziert, die uns im diesjährigen DBIR als Darstellungsgrundlage und Kontrastfolie dienen. Infolgedessen gibt es in der neuen Ausgabe zwei komplett neue Muster – „Social Engineering" und „Systeminfiltration" – sowie überarbeitete bzw. rekalibrierte Versionen der Kategorien „Einfache Angriffe auf Web-Anwendungen", „Denial of Service", „Verlorene und gestohlene Ressourcen", „Verschiedene Fehler", „Missbrauch von Nutzerrechten" und dazu noch „Alles Andere". Darauf aufbauend untersuchen wir einmal mehr globale, regionale und branchenspezifische Trends (in 12 verschiedenen Sparten). Außerdem vergleichen wir die Bedrohungs- und Sicherheitslage von kleinen und mittleren Unternehmen (KMU) mit der von größeren Betrieben.

Im Folgenden finden Sie die wichtigsten Erkenntnisse aus dem diesjährigen Bericht in einer Kurzfassung, die Sie gern an Ihre Kollegen weiterleiten können. Zusätzlich ist der vollständige Bericht (auf Englisch) mit detaillierteren Angaben zu den aktuellen Bedrohungen zum Download verfügbar.

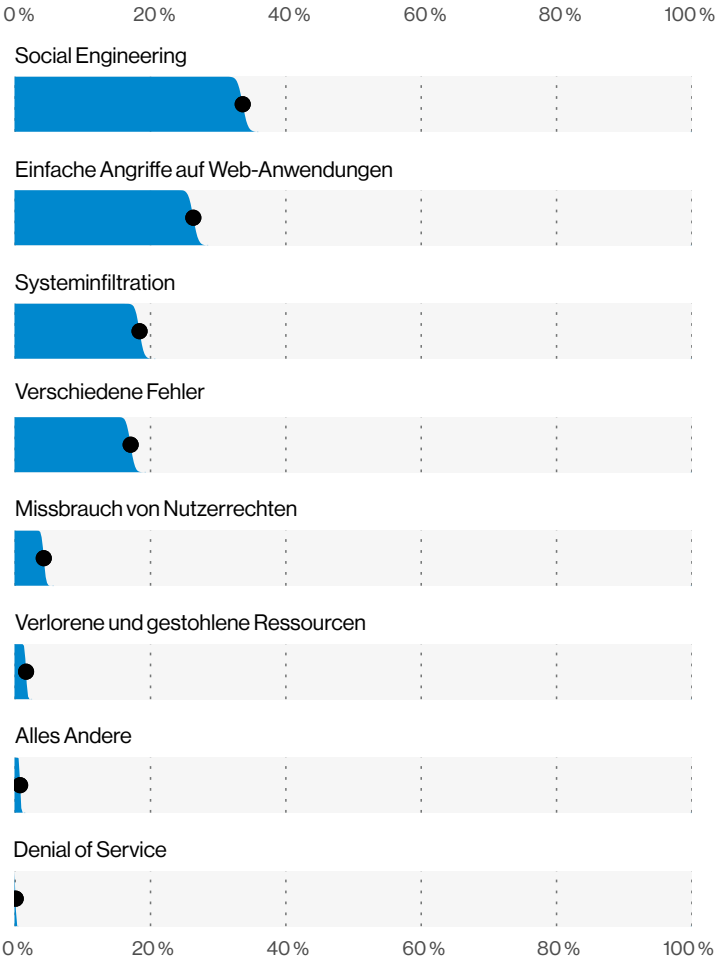
29.207

Das DBIR-Team hat 29.207 Vorfälle untersucht, von denen 5.258 als schwerwiegende Sicherheitsverletzungen eingestuft wurden.

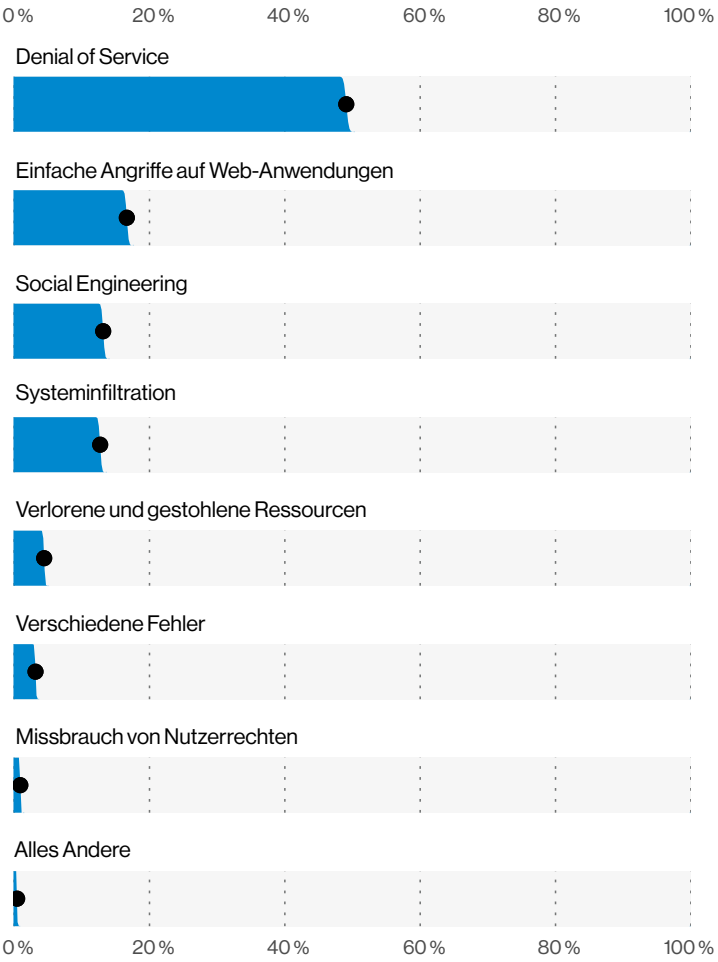
Jedes Jahr besser

Das DBIR-Team arbeitet ständig an der Erweiterung und Vereinfachung des zur Klassifizierung und Analyse von Sicherheitsvorfällen verwendeten VERIS-Frameworks (Vocabulary for Event Recording and Incident Sharing). Außerdem haben wir eine verbesserte Methode entwickelt, um unsere Forschungsergebnisse in Bezug zur kürzlich veröffentlichten neuesten Version der Center for Internet Security (CIS) Controls® zu setzen. Darauf aufbauend geben wir im Rahmen der branchenspezifischen Abschnitte an, welche CIS Controls aus der Implementierungsgruppe 1 (IG1) am besten zu den in der jeweiligen Sparte dominierenden Bedrohungen passen und von den Unternehmen prioritär umgesetzt werden sollten. Dadurch sind unsere Analysen praxisrelevanter und können von der Cyber-Sicherheits-Community nutzbringend eingesetzt werden.

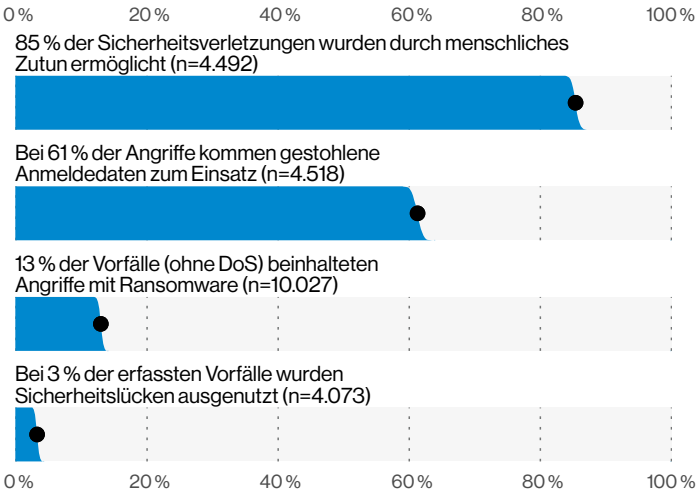
Die Ergebnisse im Überblick



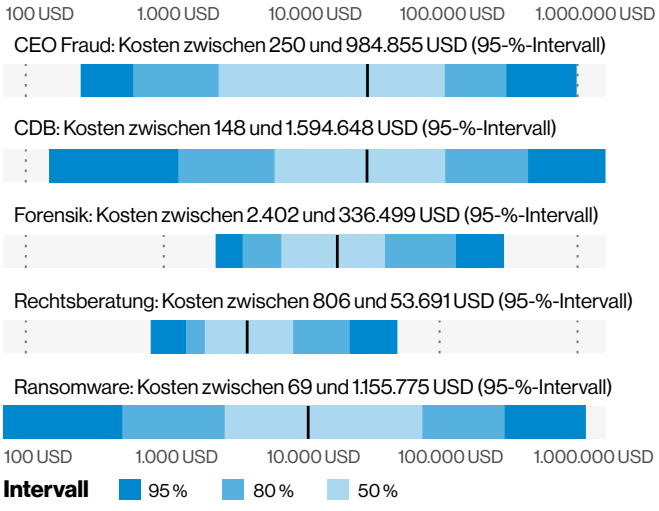
Relative Häufigkeit der identifizierten Muster bei Sicherheitsverletzungen (n=5.275)



Relative Häufigkeit ausgewählter Aktivitäten (n=29.207)



Relative Häufigkeit ausgewählter Varianten (n=4.073)



Direkte und indirekte Kosten von Sicherheitsvorfällen

Das Wichtigste in Kürze

Die Zahl der Ransomware-Angriffe nimmt weiter zu.

In 10 Prozent der erfassten Sicherheitsverletzungen wurde Ransomware eingesetzt. Damit hat sich dieser Anteil im Vergleich zum Vorjahr mehr als verdoppelt, befeuert durch neue Varianten, die die Daten vor der Verschlüsselung ausschleusen. Infolgedessen belegt Ransomware in der Rangliste der häufigsten Angriffsmethoden mittlerweile den dritten Platz.

Menschliche Schwächen sind ein wichtiger Faktor.

85 Prozent der Sicherheitsverletzungen wurden durch menschliches Zutun ermöglicht. So ist der Anteil der erfolgreichen Phishing-Angriffe an der Gesamtzahl der Vorfälle im Laufe der letzten zwölf Monate von 25 Prozent auf 36 Prozent gestiegen. Zugleich hat sich die Zahl der Fälle von Identitätsmissbrauch gegenüber dem Vorjahr verfünfzehnfacht, was unter anderem bedeutet, dass CEO Fraud (auch Business Email Compromise) zur zweihäufigsten Form des Social Engineering avanciert ist.

Fehler und Unterlassungen spielen eine (etwas) weniger prominente Rolle.

Im Vergleich zum Vorjahr ist die relative Häufigkeit von Sicherheitsverletzungen, die aus dem fahrlässigen oder unvorsichtigen Handeln wohlmeinender Mitarbeiter resultieren, von 22 Prozent auf 17 Prozent gesunken (obwohl die absolute Zahl derartiger Fälle von 883 auf 905 angestiegen ist). Das bedeutet das Ende einer dreijährigen Wachstums- bzw. Stagnationsphase.

Webanwendungen stehen weiterhin im Visier der Angreifer.

Webbasierte Apps wurden auch in diesem Jahr wieder häufig zum Ziel von Hackern und fungierten bei über 80 Prozent der erfassten Sicherheitsverletzungen als Einfallstor. Den zweiten Platz auf der Liste der wichtigsten Angriffsvektoren für Hackeroperationen belegten – mit einigem Abstand – Tools für die Bildschirmfreigabe.

Die Cloud im Fadenkreuz

Externe Cloud-Ressourcen waren häufiger als unternehmensinterne Bereitstellungsumgebungen von Vorfällen und Sicherheitslücken betroffen. Damit einhergehend sank die Zahl der von Angreifern infiltrierten Endgeräte (Desktop-PCs und Laptops). Bei genauerer Betrachtung erweist sich dieser Trend als direkte Konsequenz der Tatsache, dass die Kriminellen zunehmend soziale Medien und Web-Anwendungen für ihre böswilligen Zwecke nutzen – beispielsweise, um die zur Infiltration cloudbasierter E-Mail-Systeme nötigen Anmeldedaten zu erlangen.

Die Passwortdiebe bitten zur Kasse.

Manche Dinge ändern sich anscheinend nie: Die meisten Sicherheitsverletzungen gehen weiterhin auf das Konto externer, finanziell motivierter Angreifer. Und bei 61 Prozent der Angriffe kommen gestohlene Anmeldedaten zum Einsatz.

Es war ein außergewöhnliches Jahr.

Im August 2020 schätzten wir, dass im Zuge der COVID-19-Pandemie eine Zunahme der Zahl der Phishing-Angriffe, Ransomware-Infektionen, fahrlässigen Sicherheitsvorfälle und der Hackereinbrüche in Web-Anwendungen (mithilfe gestohlener Anmeldedaten) zu verzeichnen sein würde. Der DBIR 2021 bestätigt diese Voraussage allerdings nur zum Teil: Zwar ist die Häufigkeit der Vorfälle mit Phishing und Ransomware tatsächlich um 11 bzw. 6 Prozent gestiegen. Doch zugleich liegt die Zahl der Fälle, in denen gestohlene Kreditkarten missbraucht oder sensible Daten versehentlich offengelegt werden, in etwa auf dem Vorjahresniveau, während der Anteil der Fehlkonfigurationen und Fehlzustellungen (an der Gesamtheit der manuellen Fehler) um 2 bzw. 6 Prozent geschrumpft ist.

Sicherheitsverletzungen verursachen hohe Kosten.

Für die diesjährige DBIR-Ausgabe haben wir ermittelt, welche Kosten den Unternehmen durch Sicherheitsverletzungen entstehen können. Unsere diesbezüglichen Modelle basieren auf Angaben über Verluste, Versicherungskosten und Aktienkurse und bilden sämtliche finanziellen Aspekte eines Cyber-Angriffs ab.

Die Ergebnisse zeichnen ein zwiespältiges Bild: Einerseits hatten 14 Prozent der simulierten Sicherheitsverletzungen keine nennenswerten finanziellen Auswirkungen. Andererseits sollte sich die Sicherheitsstrategie Ihres Unternehmens nicht auf diese Hoffnung stützen, da der Kostenmedian der Vorfälle mit finanziellen Auswirkungen bei beachtlichen 21.659 US-Dollar liegt (und 95 Prozent der Vorfälle aus dieser Gruppe Verluste zwischen 826 und 653.587 US-Dollar verursachen).

Angriffs- und Vorfallsmuster

Die Angriffs- und Vorfallsmuster wurden im DBIR 2014 als nützliche Typologie häufig auftretender Szenarien eingeführt. Da sich die Bedrohungslandschaft seither ein wenig verändert hat, haben wir die DBIR-Muster für die diesjährige Ausgabe überarbeitet.

Unsere neuen Muster sind Resultat eines modernen, auf maschinellem Lernen basierenden Clustering-Prozesses und bilden komplexe Interaktionszusammenhänge sowie das Geschehen im Verlauf einer Sicherheitsverletzung besser ab. Dadurch eignen sie sich unter anderem als Grundlage für praktische Empfehlungen zur Prävention entsprechender Vorfälle.

Die aktualisierten Muster decken 95,8 % der analysierten Sicherheitsverletzungen und 99,7 % der untersuchten Vorfälle ab.

Im Folgenden finden Sie eine Aufstellung der wichtigsten Ergebnisse zu jedem identifizierten Muster.

Social Engineering	Psychologische Manipulation, die die Zielperson zu einer bestimmten Handlung unter Missachtung basaler Datenschutzregeln veranlassen soll	Die Zahl der Social-Engineering-Angriffe ist seit 2017 Jahr für Jahr gestiegen und die absolute Häufigkeit von CEO Fraud hat sich im Vergleich zum Vorjahr nochmals verdoppelt. Dabei stehen besonders webbasierte E-Mail-Dienste im Visier der Kriminellen. • Über 80 Prozent der Sicherheitsverletzungen aus dieser Kategorie werden durch externe Dritte aufgedeckt. • Vorlagen für Phishing-E-Mails unterscheiden sich hinsichtlich ihrer Effektivität und veranlassen in manchen Fällen keine, in anderen Fällen über 50 Prozent der Empfänger zum Klick auf schädliche Links. • Bei einer Stichprobenuntersuchung mit einer echten und einer simulierten Phishing-E-Mail stellten wir fest, dass keiner der 1.148 Teilnehmer auf den Link aus der simulierten Phishing-E-Mail klickte, während immerhin 2,5 Prozent der Empfänger auf die echte Phishing-E-Mail hereinfielen.
Einfache Angriffe auf Web-Anwendungen	Angriffe, bei denen auf die anfängliche Infiltration einer Web-Anwendung nur wenige weitere Schritte oder zusätzliche Aktionen der kriminellen Hacker folgen	Wir haben das Muster „Einfache Angriffe auf Web-Anwendungen“ neu definiert, sodass es nun einige Phänomene erfasst, die bisher in den Kategorien „Anwendungsbezogene Fehler in Online-Apps“, „Social Engineering“ und „Systeminfiltration“ versteckt waren. Es bezeichnet jetzt vor allem Angriffe auf cloudbasierte Server, die mit gestohlenen Anmeldedaten oder der Brute-Force-Methode gehackt werden. • 95 Prozent der von Credential-Stuffing-Aktivitäten betroffenen Unternehmen verzeichneten zwischen 637 und 3,3 Milliarden böswilliger Anmeldeversuche im Jahresverlauf. • Die Informationsbranche hat das Finanzwesen mittlerweile als häufigstes Ziel von Botnet-Angriffen auf Kunden abgelöst.

System-infiltration	Komplexe Angriffe, bei denen Malware und/oder Hackermethoden zur Einschleusung von Ransomware oder zur Realisierung anderer Zielsetzungen eingesetzt werden	Durch die Einführung dieses neuen Musters (das gemeinsam mit der Kategorie „Verschiedene Fehler“ den dritten Platz hinter „Social Engineering“ und „Einfache Angriffe auf Web-Anwendungen“ belegt) erhalten die Verantwortlichen in den Unternehmen Informationen über die Häufigkeit komplexer Angriffe. Das erleichtert ihnen die Entscheidung über Investitionen in entsprechende Abwehrmaßnahmen. • Über 70 Prozent der erfassten Instanzen dieses Musters beinhalteten den Einsatz von Malware. Der Einsatz von Hackermethoden wurde in 40 Prozent der Fälle beobachtet. • 99 Prozent der Vorfälle mit Ransomware fallen in diese Kategorie.
Verschiedene Fehler	Vorfälle, bei denen die Sicherheit von Datenbeständen durch unabsichtliche Handlungen beeinträchtigt wird – exklusive aller Geräteverluste (die bereits im Muster „Verlorene und gestohlene Ressourcen“ enthalten sind)	Der Anteil dieses Musters an der Gesamtheit der Sicherheitsverletzungen ist rückläufig. Allerdings liegt dies nicht an einem Rückgang der absoluten Häufigkeit der beobachteten Fehler, sondern an einem Anstieg der Zahl der in den anderen Kategorien enthaltenen Sicherheitsverletzungen. • Die mit Abstand gängigste Form dieses Musters waren Fehlkonfigurationen (mit einem Anteil von etwa 52 Prozent). • In der überwiegenden Mehrzahl der näher dokumentierten Fälle (80 Prozent) wurden die Fehler von Bedrohungsforschern und Sicherheitsexperten aufgedeckt. • Bei dieser Art von Vorfällen wurden vor allem personenbezogene Daten offengelegt.
Missbrauch von Nutzerrechten	Vorfälle rund um den ungenehmigten Einsatz oder böswilligen Missbrauch legitimer Zugriffsrechte	Der Missbrauch von Nutzerrechten macht einen zunehmend geringen Anteil an der Gesamtheit der erfassten Sicherheitsverletzungen aus. Das zeigt einmal mehr die sinkende Bedeutung von Insider-Bedrohungen im Vergleich mit anderen Mustern. • 70 Prozent der Sicherheitsverletzungen aus dieser Kategorie resultierten aus dem böswilligen Missbrauch legitimer Zugriffsrechte • Über 30 Prozent der hier subsummierten Vorfälle wurden erst nach Monaten oder Jahren entdeckt.
Verlorene und gestohlene Ressourcen	Vorfälle, bei denen Datenspeicher versehentlich oder durch schädliche Aktivitäten verlorengehen	Versehentliche Verluste von Ressourcen sind weitaus häufiger als der Diebstahl von Speichermedien und werden meist von den Mitarbeitern entdeckt. Es geht hier also vorwiegend um Fälle, in denen nicht einzelne Dokumente oder digitale Medien, sondern komplette Geräte verschwinden.
Denial of Service	Angriffe zur Störung der Verfügbarkeit von Netzwerken und Systemen – sowohl auf der Netzwerk- als auch auf der Anwendungsebene	DDoS-Angriffe (Distributed Denial of Service) verursachen plötzliche Lastspitzen mithilfe weit verteilter Systeme. Da sich diese Attacken nur mit großen Schwierigkeiten prognostizieren und proaktiv verhindern lassen, müssen die Verantwortlichen entscheiden, wie gut sie ihr jeweiliges Unternehmen gegen derartige Vorfälle absichern möchten (d. h. ob beispielsweise ein 50%iger, 80%iger, 95%iger oder noch stärkerer Schutz erforderlich ist).
Alles Andere	Residualkategorie für alle Vorfälle, die sich keinem der anderen Muster zuordnen lassen.	Hier sind unter anderem die Vorfälle enthalten, die früher der Kategorie „Skimming“ zugeschlagen worden wären. Diese Umverteilung war notwendig, weil die Gesamtheit der Sicherheitsverletzungen in diesem Jahr nur 20 Skimming-Angriffe beinhaltet. • Die Kategorie „Alles Andere“ umfasst in diesem Jahr drei seltene Fälle von Sicherheitsverletzungen, deren Ursprung im Partnernetzwerk der betroffenen Unternehmen liegt. • Durch das neue Clustering konnten wir zusätzliche 18 Prozent der Sicherheitsverletzungen anderen Kategorien zuschlagen und eine Einordnung in die Residualkategorie verhindern.

Branchenspezifische Erkenntnisse

Auch wenn grundsätzlich alle Unternehmen der Gefahr eines Cyber-Angriffs ausgesetzt sind, gibt es doch branchen- und größenspezifische Bedrohungsprofile. Das bedeutet: Um effektive und effiziente Sicherheitsmaßnahmen implementieren zu können, müssen Sie die speziellen Risiken Ihres Betriebs im Auge behalten. Aus diesem Grund enthält der diesjährige Bericht verschiedene Spartenanalysen, die auf der Brancheneinteilung des North American Industry Classification System (NAICS) basieren.

Hotel- und Gaststättengewerbe (NAICS 72)

Hackeroperationen, Social-Engineering-Angriffe und Malware-Infektionen treten im Hotel- und Gaststättengewerbe mit annähernd gleicher Häufigkeit auf.

Absolute Häufigkeit	69 Vorfälle, davon 40 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	85 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien „Systeminfiltration", „Social Engineering" und „Einfache Angriffe auf Web-Anwendungen".
Urheber der Bedrohungen	Extern (90 %), intern (10 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Motive der Angreifer	Habgier (86-100 %), Spionage (0-14 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Betroffene Daten	Personenbezogene Daten (51 %), Anmeldedaten (49 %), Zahlungsdaten (33 %), Sonstige (15 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Empfohlene Abwehrmaßnahmen (CIS Controls für IG1)	Schulungen zur Steigerung des Sicherheitsbewusstseins (14), Zugangskontrolle (6), Sichere Konfiguration der Unternehmensressourcen und -software (4)

Medien und Unterhaltung (NAICS 71)

Phishing- und Ransomware-Kampagnen sowie der Missbrauch gestohlener Anmeldedaten sind in dieser Branche weiterhin dominant. Darüber hinaus wurden unerwartet große Mengen an Gesundheitsdaten gestohlen, die im Rahmen von Fitnessprogrammen erhoben worden waren.

Absolute Häufigkeit	7.065 Vorfälle, davon 109 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	83 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien „Systeminfiltration", „Einfache Angriffe auf Web-Anwendungen" und „Verschiedene Fehler".
Urheber der Bedrohungen	Extern (70 %), intern (31 %), verschiedene (1 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Motive der Angreifer	Habgier (100 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Betroffene Daten	Personenbezogene Daten (83 %), Anmeldedaten (32 %), Gesundheitsdaten (26 %), Sonstige (18 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Empfohlene Abwehrmaßnahmen (CIS Controls für IG1)	Schulungen zur Steigerung des Sicherheitsbewusstseins (14), Sichere Konfiguration der Unternehmensressourcen und -software (4), Zugangskontrolle (6)

Bildungswesen (NAICS 61)

Das Bildungswesen verzeichnete einen ungewöhnlich hohen Anteil an Social-Engineering-Angriffen, bei denen die Kriminellen ihren Opfern unter Vorspiegelung falscher Tatsachen sensible Informationen entlocken und diese dann zur Realisierung eines betrügerischen Vermögensvorteils nutzen. Abgesehen davon wurden in der Branche viele Vorfälle aus den Kategorien „Verschiedene Fehler" und „Systeminfiltration" erfasst.

Absolute Häufigkeit	1.332 Vorfälle, davon 344 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	86 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien „Social Engineering", „Verschiedene Fehler" und „Systeminfiltration".
Urheber der Bedrohungen	Extern (80 %), intern (20 %), verschiedene (1 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Motive der Angreifer	Habgier (96 %), Spionage (3 %), Spaß (1 %), Mutwille (1 %), Groll (1 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Betroffene Daten	Personenbezogene Daten (61 %), Anmeldedaten (51 %), Sonstige (12 %), Gesundheitsdaten (7 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Empfohlene Abwehrmaßnahmen (CIS Controls für IG1)	Schulungen zur Steigerung des Sicherheitsbewusstseins (14), Zugangskontrolle (6), Sichere Konfiguration der Unternehmensressourcen und -software (4)

Finanz- und Versicherungsbranche (NAICS 52)

Bei den in der Finanzbranche beobachteten Fehlern und Unachtsamkeiten handelt es sich zu 55 Prozent um Falschzustellungen sensibler Daten. Zugleich werden Finanzunternehmen häufig Opfer externer Angreifer, die gestohlene Anmeldedaten missbrauchen oder Ransomware einschleusen.

Absolute Häufigkeit	721 Vorfälle, davon 467 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	81 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien „Verschiedene Fehler", „Einfache Angriffe auf Web-Anwendungen" und „Social Engineering".
Urheber der Bedrohungen	Extern (56 %), intern (44 %), verschiedene (1 %), Partner (1 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Motive der Angreifer	Habgier (96 %), Spionage (3 %), Groll (2 %), Spaß (1 %), Ideologie (1 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Betroffene Daten	Personenbezogene Daten (83 %), Bankdaten (33 %), Anmeldedaten (32 %), Sonstige (21 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Empfohlene Abwehrmaßnahmen (CIS Controls für IG1)	Schulungen zur Steigerung des Sicherheitsbewusstseins (14), Sichere Konfiguration der Unternehmensressourcen und -software (4), Zugangskontrolle (6)

Gesundheitswesen (NAICS 62)

Gesundheitsanbieter standen in der jüngeren Vergangenheit immer wieder wegen einfacher Fahrlässigkeiten ihrer Mitarbeiter in der Kritik. In diesem Jahr handelt es sich dabei am häufigsten (in 36 Prozent der Fälle) um Fehlzustellungen von Papierdokumenten oder elektronischen Akten. Dagegen ist die Zahl der böswilligen Insider in der Branche seit zwei Jahren rückläufig, sodass diese Art von Bedrohung nun nicht mehr zu den drei virulentesten Gefahren zählt. Stattdessen dominieren nun finanziell motivierte Hacker, die der organisierten Kriminalität zuzurechnen sind und mit Vorliebe Ransomware einsetzen.

Absolute Häufigkeit	655 Vorfälle, davon 472 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	86 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien „Verschiedene Fehler", „Einfache Angriffe auf Web-Anwendungen" und „Systeminfiltration".
Urheber der Bedrohungen	Extern (61 %), intern (39 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Motive der Angreifer	Habgier (91 %), Spaß (5 %), Spionage (4 %), Groll (1 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Betroffene Daten	Personenbezogene Daten (66 %), Gesundheitsdaten (55 %), Anmeldedaten (32 %), Sonstige (20 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Empfohlene Abwehrmaßnahmen (CIS Controls für IG1)	Schulungen zur Steigerung des Sicherheitsbewusstseins (14), Sichere Konfiguration der Unternehmensressourcen und -software (4), Zugangskontrolle (6)

IT und TK-Beratung (NAICS 51)

Unternehmen aus dieser Branche sind auffällig oft mit Problemen infolge von Fehlkonfigurationen und anderen Fehlern ihrer Mitarbeiter konfrontiert. Zugleich nehmen die meisten Vorfälle mit externen Ursachen die Form von DoS-Attacken an. Darüber hinaus hat die Informationsbranche mittlerweile das Finanzwesen als Hauptzielscheibe von Botnet-Angriffen abgelöst.

Absolute Häufigkeit	2.935 Vorfälle, davon 381 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	83 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien „Einfache Angriffe auf Web-Anwendungen", „Verschiedene Fehler" und „Systeminfiltration".
Urheber der Bedrohungen	Extern (66 %), intern (37 %), verschiedene (4 %), Partner (1 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Motive der Angreifer	Habgier (88 %), Spionage (9 %), Groll (2 %), Mutwille (1 %), Spaß (1 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Betroffene Daten	Personenbezogene Daten (70 %), Anmeldedaten (32 %), Sonstige (27 %), Interna (12 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Empfohlene Abwehrmaßnahmen (CIS Controls für IG1)	Schulungen zur Steigerung des Sicherheitsbewusstseins (14), Sichere Konfiguration der Unternehmensressourcen und -software (4), Zugangskontrolle (6)

Fertigungsindustrie (NAICS 31-33)

Genau wie zahlreiche andere Sparten wird auch die Fertigung immer wieder zum Ziel von Social-Engineering-Angriffen. Außerdem verzeichnete die Branche einen deutlichen Anstieg ransomwarebasierter Sicherheitsverletzungen.

Absolute Häufigkeit	585 Vorfälle, davon 270 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	82 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien „Systeminfiltration", „Social Engineering" und „Einfache Angriffe auf Web-Anwendungen".
Urheber der Bedrohungen	Extern (82 %), intern (19 %), verschiedene (1 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Motive der Angreifer	Habgier (92 %), Spionage (6 %), Mutwille (1 %), Groll (1 %), von untergeordneter Bedeutung (1 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Betroffene Daten	Personenbezogene Daten (66 %), Anmeldedaten (42 %), Sonstige (36 %), Zahlungsdaten (19 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Empfohlene Abwehrmaßnahmen (CIS Controls für IG1)	Schulungen zur Steigerung des Sicherheitsbewusstseins (14), Zugangskontrolle (6), Sichere Konfiguration der Unternehmensressourcen und -software (4)

Bergbau-, Öl- und Gasindustrie plus Versorgungsbetriebe (NAICS 21 u. 22)

Diese Branchen waren im Verlauf des Jahres immer wieder Ziel von Social-Engineering-Angriffen, bei denen die Hacker vor allem Anmeldedaten, personenbezogene Daten und Interna erbeuteten. Zugleich erwies sich Ransomware als eine virulente Bedrohung.

Absolute Häufigkeit	546 Vorfälle, davon 355 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	98 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien „Social Engineering", „Systeminfiltration" und „Einfache Angriffe auf Web-Anwendungen".
Urheber der Bedrohungen	Extern (98 %), intern (2 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Motive der Angreifer	Habgier (78-100 %), Spionage (0-33 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Betroffene Daten	Anmeldedaten (94 %), Personenbezogene Daten (7 %), Interna (3 %), Sonstige (3 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Empfohlene Abwehrmaßnahmen (CIS Controls für IG1)	Schulungen zur Steigerung des Sicherheitsbewusstseins (14), Zugangskontrolle (6), Management von Nutzerkonten (5)

Bildungswesen (NAICS 54)

In dieser Branche ist die überwiegende Mehrzahl der beobachteten Zwischenfälle auf eine Kombination der Muster „Systeminfiltration“ und „Social Engineering“ zurückzuführen. Die Angreifer missbrauchen gestohlene Anmeldedaten und machen sich die Tatsache zunutze, dass viele Mitarbeiter bereitwillig auf Phishing-E-Mails und ähnliche Taktiken ansprechen.

Absolute Häufigkeit	1.892 Vorfälle, davon 630 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	81 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien „Systeminfiltration“, „Social Engineering“ und „Einfache Angriffe auf Web-Anwendungen“.
Urheber der Bedrohungen	Extern (74 %), intern (26 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Motive der Angreifer	Habgier (97 %), Spionage (2 %), Groll (1 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Betroffene Daten	Anmeldedaten (63 %), Personenbezogene Daten (49 %), Sonstige (21 %), Bankdaten (9 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Empfohlene Abwehrmaßnahmen (CIS Controls für IG1)	Schulungen zur Steigerung des Sicherheitsbewusstseins (14), Zugangskontrolle (6), Sichere Konfiguration der Unternehmensressourcen und -software (4)

Öffentliche Verwaltung (NAICS 92)

In diesem Sektor geht die größte Bedrohung von Social-Engineering-Angriffen aus. Die Zahl der Fälle, in denen Kriminelle mithilfe aufwendig gefälschter Phishing-E-Mails Anmeldedaten erbeuten, hat ein besorgniserregendes Niveau erreicht.

Absolute Häufigkeit	3.236 Vorfälle, davon 885 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	92 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien „Social Engineering“, „Verschiedene Fehler“ und „Systeminfiltration“.
Urheber der Bedrohungen	Extern (83 %), intern (17 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Motive der Angreifer	Habgier (96 %), Spionage (4 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Betroffene Daten	Anmeldedaten (80 %), Personenbezogene Daten (18 %), Sonstige (6 %), Gesundheitsdaten (4 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Empfohlene Abwehrmaßnahmen (CIS Controls für IG1)	Schulungen zur Steigerung des Sicherheitsbewusstseins (14), Zugangskontrolle (6), Management von Nutzerkonten (5)

Einzelhandel (NAICS 44-45)

Der Einzelhandel steht seit jeher im Fokus finanziell motivierter Krimineller, die es auf Kreditkartendaten und andere sensible personenbezogene Informationen abgesehen haben. Dabei nutzen die Angreifer unter anderem Phishing-E-Mails sowie ausgeklügelte Täuschungsmanöver, die die Opfer unter Vorspiegelung falscher Tatsachen zu betrügerischen Überweisungen veranlassen sollen.

Absolute Häufigkeit	725 Vorfälle, davon 165 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	77 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien „Systeminfiltration“, „Social Engineering“ und „Einfache Angriffe auf Web-Anwendungen“.
Urheber der Bedrohungen	Extern (84 %), intern (17 %), verschiedene (2 %), Partner (1 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Motive der Angreifer	Habgier (99 %), Spionage (1 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Betroffene Daten	Zahlungsdaten (42 %), Personenbezogene Daten (41 %), Anmeldedaten (33 %), Sonstige (16 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Empfohlene Abwehrmaßnahmen (CIS Controls für IG1)	Schulungen zur Steigerung des Sicherheitsbewusstseins (14), Sichere Konfiguration der Unternehmensressourcen und -software (4), Zugangskontrolle (6)

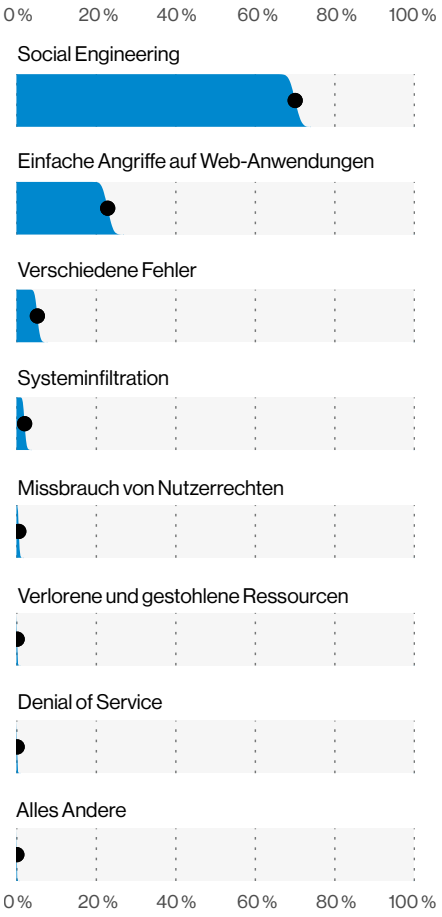
Die Situation der KMU

In Bezug auf die Zahl der erfassten Sicherheitsverletzungen ist die Kluft zwischen kleinen und großen Unternehmen in diesem Jahr weit weniger deutlich. Zugleich ist festzustellen, dass sich die dominanten Angriffs- und Vorfallsmuster der beiden Gruppen einander angenähert haben. Damit ist zum ersten Mal seit Beginn unserer Beobachtungen eine Situation eingetreten, in der die Verantwortlichen sämtlicher Betriebe mit ähnlichen Sicherheitsherausforderungen konfrontiert sind, weil beispielsweise kleine wie große Unternehmen im Visier finanziell motivierter Angreifer stehen.

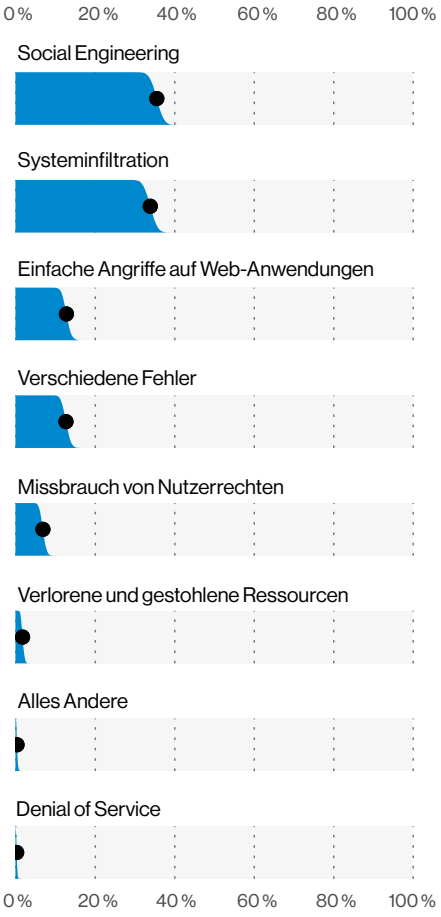
Einer der wenigen relevanten Unterschiede besteht im Hinblick auf die Fähigkeit zur Erkennung akuter Bedrohungen: Letztes Jahr stellte sich bei unserer Analyse heraus, dass kleinere Unternehmen hier augenscheinlich die Nase vorn hatten. Doch in diesem Jahr zeigen die von uns erhobenen Daten, dass die Aufdeckung von Sicherheitsverletzungen bei 55 Prozent der Großunternehmen nur wenige Tage dauert, während dies lediglich auf 47 Prozent der KMU zutrifft.

	KMU (weniger als 1.000 Angestellte)	Großunternehmen (mehr als 1.000 Angestellte)
Absolute Häufigkeit	1.037 Vorfälle, davon 263 mit bestätigten Datenlecks	819 Vorfälle, davon 307 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	80 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien „Systeminfiltration", „Verschiedene Fehler" und „Einfache Angriffe auf Web-Anwendungen".	74 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien „Systeminfiltration", „Verschiedene Fehler" und „Einfache Angriffe auf Web-Anwendungen".
Urheber der Bedrohungen	Extern (57 %), intern (44 %), verschiedene (1 %), Partner (0 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen	Extern (64 %), intern (36 %), Partner (1 %), verschiedene (1 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Motive der Angreifer	Habgier (93 %), Spionage (3 %), Spaß (2 %), Mutwille (1 %), Groll (1 %), Sonstige (1 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen	Habgier (87 %), Spaß (7 %), Spionage (5 %), Mutwille (2 %), Groll (2 %), von untergeordneter Bedeutung (1 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Betroffene Daten	Anmeldedaten (44 %), Personenbezogene Daten (39 %), Sonstige (34 %), Gesundheitsdaten (17 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen	Anmeldedaten (42 %), Personenbezogene Daten (38 %), Sonstige (34 %), Gesundheitsdaten (17 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen

Ergebnisse für spezifische Regionen



Relative Häufigkeit der Angriffsmuster in der Region APAC (n=1.495)

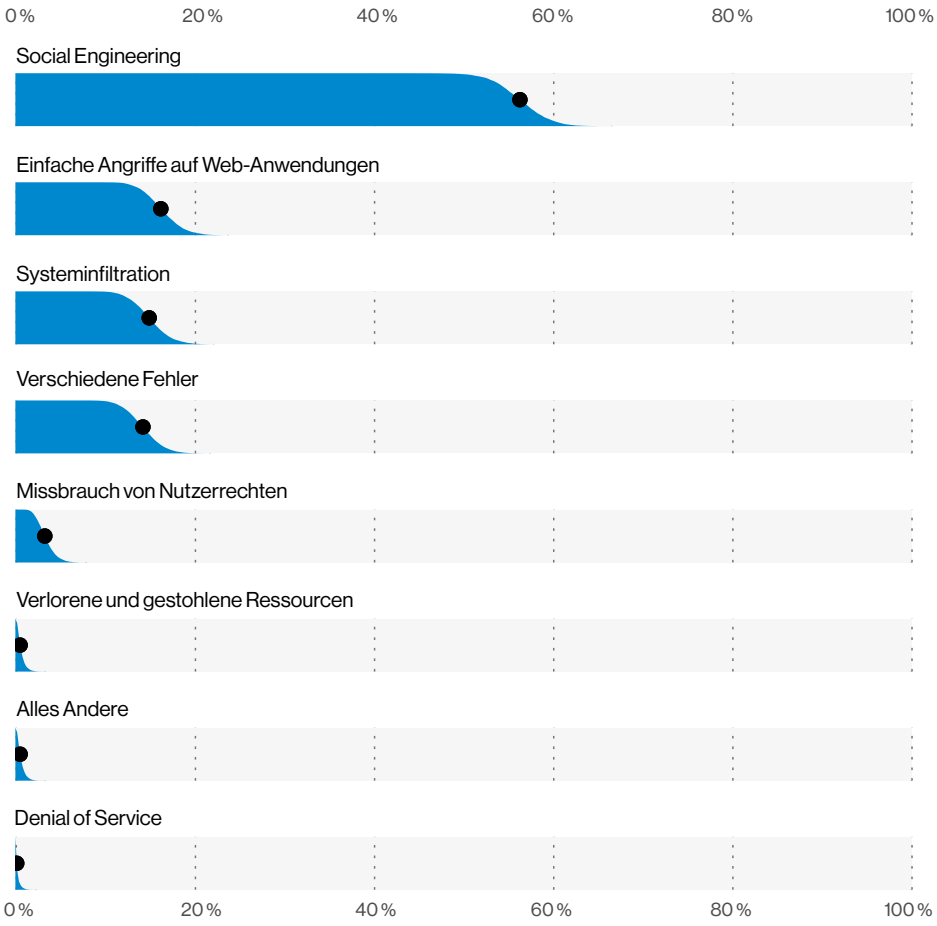


Relative Häufigkeit der Angriffsmuster in Nordamerika (n=11.080)

Finanziell motivierte Angriffe in den Regionen APAC und Nordamerika

Die Region Asien-Pazifik (APAC) verzeichnete viele finanziell motivierte Phishing-Angriffe, bei denen die Anmeldedaten von Mitarbeitern gestohlen wurden. Die erbeuteten Passwörter wurden dann für den unbefugten Zugriff auf geschäftliche E-Mail-Konten und unternehmenseigene Server für Webanwendungen missbraucht.

Parallel dazu gerieten auch in Nordamerika zahlreiche Unternehmen ins Visier von Kriminellen, die es auf Geldmittel oder wertvolle Daten abgesehen hatten. Dabei kamen vor allem Social Engineering, Hackermethoden und Malware zum Einsatz.



Relative Häufigkeit der Angriffsmuster in der Region EMEA (n=293)

Altbekannte Bedrohungen in der Region EMEA

In Europa, dem Mittleren Osten und Afrika dominieren weiterhin einfache Angriffe auf Web-Anwendungen, Systeminfiltrationen und Social-Engineering-Angriffe.

Best Practices

In diesem Jahr kombinieren wir unsere neue Muster-typologie mit den kürzlich aktualisierten CIS Controls, um jedem Unternehmen – unabhängig von seiner Größe und seinem Budget – effektive Präventionsmaßnahmen empfehlen zu können.

CIS Control 4: Sichere Konfiguration der Unternehmensressourcen und -software

Hinter diesem Wortungetüm verbergen sich vielfältige Maßnahmen, die sicherstellen sollen, dass neu eingerichtete Lösungen nicht im Nachhinein um aufgesetzte Schutzmaßnahmen erweitert werden müssen, weil sie von Anfang an über integrierte Sicherheitsmechanismen verfügen. Die Umsetzung dieses Prinzips hilft bei der Vermeidung von Fehlkonfigurationen und daraus resultierenden Sicherheitsverletzungen und ermöglicht beispielsweise die Prävention von Datenlecks durch den Einsatz von Remote-Löschfunktionen auf verlorengegangenen Mobilgeräten.

CIS Control 5: Management von Nutzerkonten

Obwohl es sich hier nominell um eine komplett neue Kategorie handelt, besteht sie schwerpunktmäßig aus altbekannten Best Practices, die bereits in früheren Versionen der CIS Controls enthalten waren. Diese Maßnahmen zielen vor allem auf eine effektivere Verwaltung des Zugriffs auf Nutzerkonten und die Vereitelung von Brute-Force- und Credential-Stuffing-Angriffen.

CIS Control 6: Zugangskontrolle

Die Implementierung dieser Best Practices steht in direktem Zusammenhang mit dem Management von Nutzerkonten (CIS Control 5). Allerdings geht es hier nicht nur um den Zugriff auf die Konten an sich, sondern auch um die Kontrolle der diesen zugewiesenen Rechten und Privilegien. So können Sie beispielsweise den Nutzen gestohlener Anmeldedaten minimieren, indem Sie wichtige Komponenten Ihrer IT-Infrastruktur mit Multi-Faktor-Authentifizierungsverfahren sichern.

CIS Control 14: Schulungen zur Steigerung des Sicherheitsbewusstseins

Sicherheitsschulungen haben eine lange Tradition und bedürfen daher keiner näheren Erklärung. In Anbetracht der auffallenden Häufigkeit fahrlässiger Verhaltensweisen und der hohen Virulenz von Social-Engineering-Angriffen kann kein Zweifel daran bestehen, dass eine Investition in entsprechende Trainingseinheiten entscheidend zum Schutz Ihres Unternehmens beiträgt.

Halten Sie sich und Ihr Team auf dem Laufenden

Um den aktuellen Bedrohungen in Ihrer Branche die Stirn bieten zu können, benötigen Sie zuverlässige Informationen, anhand derer Sie Ihre Sicherheitsmaßnahmen gezielt stärken und Ihre Mitarbeiter schulen können. Deshalb bietet Ihnen die vollständige Ausgabe des DBIR einen detaillierten, praxisrelevanten Überblick über die Ziele, Methoden und typischen Aktivitäten der Angreifer. Holen Sie sich alle Zahlen, Daten und Fakten, die für fundierte Sicherheitsmaßnahmen erforderlich sind.

Hier finden Sie zusätzliche Information und den vollständigen DBIR 2021.

Möchten Sie dazu beitragen, die Welt sicherer zu machen?

Der DBIR basiert auf Beiträgen von Dutzenden von Unternehmen und könnte mit Ihrer Beteiligung noch besser werden. Falls Sie interessiert sind oder uns Verbesserungsvorschläge für den nächsten DBIR unterbreiten möchten, können Sie uns unter der E-Mail-Adresse dbir@verizon.com oder per Tweet an @VZDBIR erreichen. Außerdem sollten Sie nicht versäumen, die GitHub-Seite zu unserem VERIS-Framework zu besuchen: https://github.com/vz-risk/veris (auf Englisch).

verizon