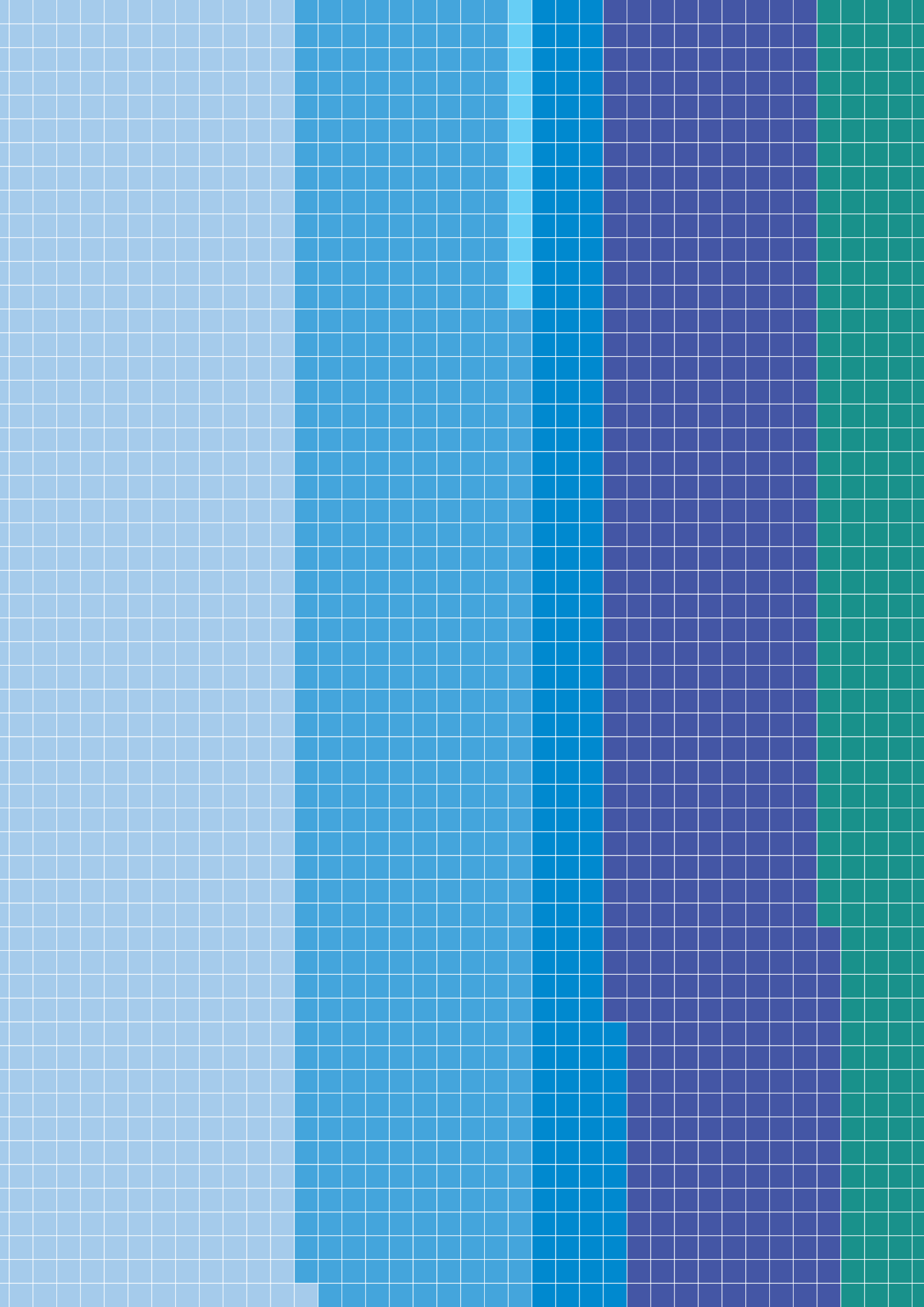
DBIR

2020 Data Breach Investigations Report

Kurzfassung

verizon



3.950 Angriffe

Das sehen Sie hier: Die Quadrate repräsentieren Angriffe in den 16 Branchen und vier Weltregionen, die wir für den vorliegenden Bericht analysiert haben. Jedes Quadrat steht für einen Angriff (oder, um ganz exakt zu sein, 1,04 Angriffe). Insgesamt sehen Sie hier 4.675 Quadrate, weil jeder Angriff in seiner Branche und seiner Region gezeigt wird.

Darüber hinaus haben wir insgesamt 157.525 Vorfälle analysiert (und damit einen neuen Rekord aufgestellt), von denen 32.002 unsere Qualitätsanforderungen erfüllten. Unsere diesjährige Datenbasis ist so umfassend, dass sie durch das schwarz-weiße Deckblatt durchscheint und damit verdeutlicht, dass der DBIR ein auf soliden Daten basierendes Dokument ist. Blättern Sie um und lesen Sie selbst!

Inhalt

Zahlen und Fakten zu aktuellen Bedrohungen

Je mehr Sie über die aktuelle Bedrohungslage wissen, desto besser können Sie Ihre Daten vor unbefugtem Zugriff schützen und schlagzeilenträchtige Sicherheitsverletzungen vermeiden. Deshalb veröffentlicht Verizon einmal jährlich den *Data Breach Investigations Report* (DBIR). An der Entstehung der jüngsten, 13. Ausgabe waren insgesamt 81 Institutionen und Unternehmen beteiligt – und damit mehr Mitwirkende als je zuvor. Das mit der Erstellung beauftragte Team hat insgesamt 32.002 Vorfälle untersucht, von denen 3.950 als schwerwiegende Sicherheitsverletzungen eingestuft wurden. Außerdem enthält der DBIR 2020 mehr branchenspezifische Informationen und wurde um nach Regionen aufgeschlüsselte Statistiken erweitert.

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

32.002

Das mit der Erstellung beauftragte Team hat insgesamt 32.002 Vorfälle untersucht, von denen 3.950 als schwerwiegende Sicherheitsverletzungen eingestuft wurden.

Jedes Jahr besser

Das DBIR-Team arbeitet ständig an der Erweiterung und Verbesserung des zur Klassifizierung und Analyse von Sicherheitsvorfällen verwendeten VERIS-Frameworks (Vocabulary for Event Recording and Incident Sharing). Für den diesjährigen Bericht haben wir eine Darstellungsweise entwickelt, die auf der MITRE ATT&CK®-Matrix und den Empfehlungen des Center for Internet Security (Center for Internet Security's Critical Security Controls, CIS CSC) basiert. Dadurch sind unsere Analysen aussagekräftiger und können von der Cybersicherheits-Community nutzbringend eingesetzt werden.

Die Ergebnisse im Überblick

Abbildung 1: Wer sind die Opfer?

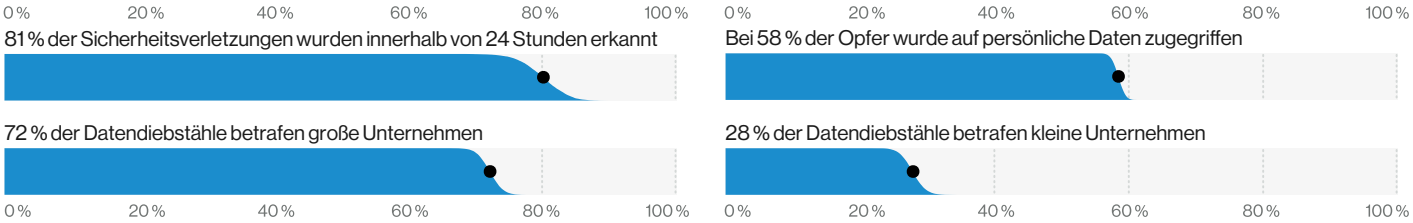


Abbildung 2: Wer sind die Angreifer?

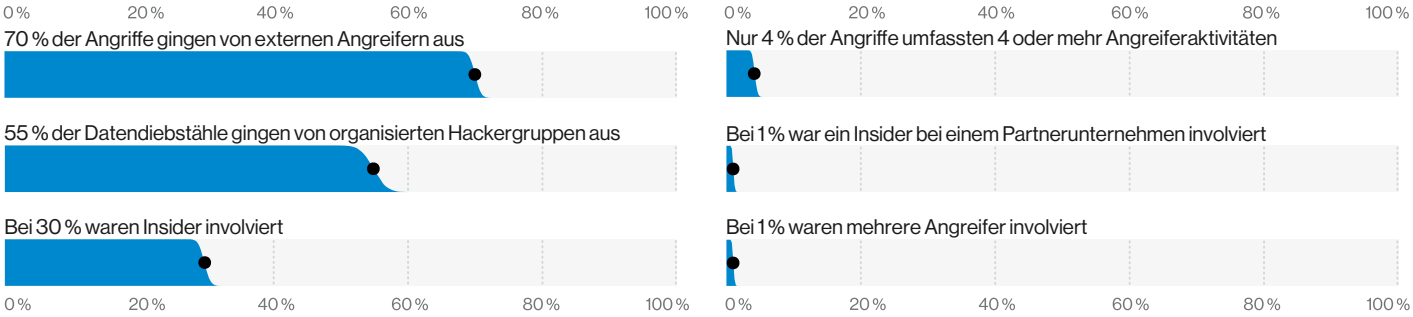
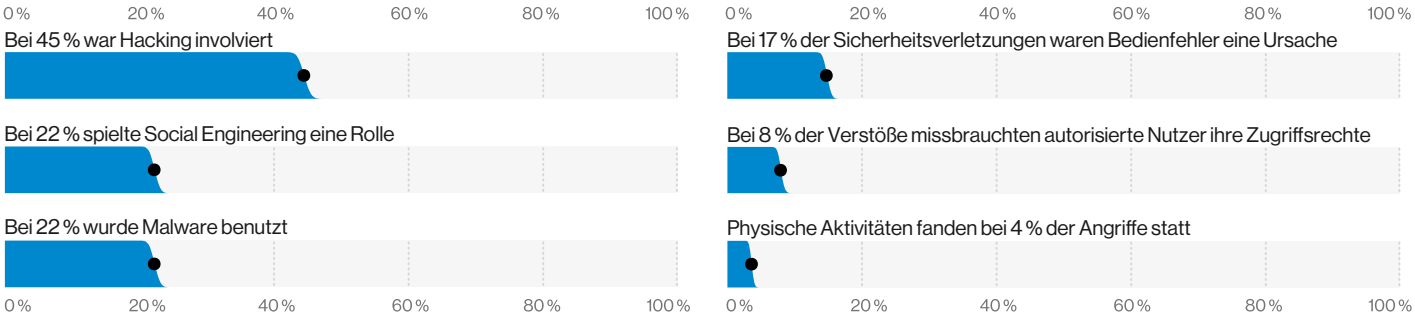


Abbildung 3: Welche Taktiken werden genutzt?



Die wichtigsten Erkenntnisse

Mythen auf dem Prüfstand

Die Bedrohung kommt von außen

Viele Verantwortliche glauben, dass die meisten Sicherheitsverletzungen auf böswillige Insider zurückzuführen sind. Doch auch der diesjährige DBIR zeigt, dass der größte Teil der Bedrohungen nach wie vor von außen kommt: 70 % der Sicherheitsverletzungen des vergangenen Jahres gingen auf das Konto externer Angreifer.

Die meisten Angriffe sind finanziell motiviert

Cyber-Spione sorgen immer wieder für Schlagzeilen, stecken jedoch nur hinter 10 % der im diesjährigen Bericht erfassten Sicherheitsverletzungen. Die überwiegende Mehrzahl der Angriffe (86 %) waren wieder auf finanzielle Motive zurückzuführen. Zugleich zeigt der DBIR 2020, dass die in der Medienberichterstattung ebenfalls sehr prominenten APT-Gruppen (Advanced Persistent Threats) lediglich für 4 % der analysierten Vorfälle verantwortlich waren.

Im Fokus: Angreifer und ihre Methoden

Die Zeiten ändern sich ... nicht

Ganze 67 % der Sicherheitsverletzungen sind auf den Diebstahl von Zugangsdaten, Social-Engineering-Angriffe (wie Phishing und CEO Fraud) sowie die Ausnutzung von fahrlässigen Verhaltensweisen oder Fehlern der Nutzer zurückzuführen. Da diese Taktiken äußerst effektiv sind, erfreuen sie sich seit Jahren einer großen Beliebtheit und werden immer wieder von Angreifern eingesetzt. Deshalb sollten Unternehmen ihre Sicherheitsmaßnahmen schwerpunktmäßig auf diese Risiken ausrichten.

Ransomware ist allgegenwärtig

Ransomware kommt mittlerweile bei 27 % aller Malware-basierten Angriffe zum Einsatz. Im vergangenen Jahr haben 18 % der Unternehmen mindestens eine Ransomware-Variante blockiert. Die Verantwortlichen sollten diese Gefahr auf keinen Fall ignorieren.

Gegen die Diebe ist kein‘ Cloud gewachsen

43 % der erfassten Sicherheitsverletzungen beinhalteten einen Angriff auf Webanwendungen. Damit hat sich dieser Anteil im Vergleich zum Vorjahr mehr als verdoppelt. Das deutet darauf hin, dass die Angreifer dem Trend zur Migration folgen und sich bei ihren Operationen verstärkt auf Cloud-Services konzentrieren, um Zugang zu sensiblen Daten zu erlangen. In über 80 % der Fälle wurden hierfür gestohlene oder mit der Brute-Force-Methode geknackte Passwörter verwendet, bei den restlichen knapp 20 % wurden Schwachstellen der betroffenen Anwendungen ausgenutzt.

Hacker nehmen es gern persönlich

Die Zahl der gemeldeten Diebstähle personenbezogener Daten steigt – oder zumindest werden mehr Fälle bekannt, weil Unternehmen durch neue Datenschutzverordnungen zu ihrer Offenlegung verpflichtet sind. So zeigt der diesjährige DBIR, dass bei 58 % der erfassten Vorfälle personenbezogene Daten abgefragt, offengelegt oder gestohlen wurden. Damit hat sich der Anteil im Vergleich zum Vorjahr fast verdoppelt. Die Hacker erbeuteten E-Mail- und Wohnadressen, Namen, Telefonnummern und andere Arten von Angaben, die in Datenbanken gespeichert oder in elektronischer Form verschickt werden.

Theorie und Praxis klaffen auseinander

Der diesjährige DBIR weist 881 Vorfälle aus, die auf fahrlässiges Verhalten oder Fehler der Nutzer zurückzuführen sind. Obwohl dies ein deutlicher Anstieg im Vergleich zu den 424 dokumentierten Fällen des Vorjahres ist, sind wir nicht überzeugt, dass die Mitarbeiter der Unternehmen insgesamt weniger sicherheitsbewusst agieren. Stattdessen ist die erhöhte Zahl wohl vor allem auf neue gesetzliche Meldepflichten zurückzuführen.

Langersehnte gute Neuigkeiten

Der Sieg über die Trojaner

Moderne Sicherheits-Tools werden bei der Abwehr gängiger Malware immer effektiver. So geht aus den DBIR-Daten der letzten Jahre hervor, dass der Anteil der auf Trojaner und ähnliche Malware-Varianten zurückzuführenden Vorfälle 2016 den Höchstwert von 50 % erreichte und mittlerweile auf 6,5 % zurückgegangen ist. Zugleich zeigen Stichprobenanalysen, dass es sich bei den aktuellen Malware-Varianten zu 45 % um Dropper, Backdoors oder Keylogger handelt. Diese Bedrohungen sind zwar weiterhin omnipräsent, werden jedoch größtenteils erfolgreich blockiert.

Rasch gepatcht ist halb gewonnen

Die Ausnutzung von Sicherheitslücken und Schwachstellen war im Berichtszeitraum lediglich bei 5 % der erfassten Vorfälle zu beobachten und machte nur 2,5 % der SIEM-Ereignisse aus. Unser Datenset zeigt also, dass derartige Angriffe eher selten sind. Das deutet darauf hin, dass Patches in den meisten Unternehmen zeitnah eingespielt werden. (Weiter so!)

Damit das Patching wirklich effektiv ist, muss es jedoch mit einem umfassenden Ressourcenmanagement kombiniert werden. In den meisten Unternehmensinfrastrukturen, die wir bei unserer Arbeit sehen, gibt es über das Internet zugängliche Ressourcen, die typischerweise auf mindestens fünf Netzwerke verteilt sind. Unter diesen Umständen können einzelne Geräte oder Systeme beim Patching leicht vergessen werden, sodass gefährliche Sicherheitslücken entstehen.

27 %

Ransomware kommt mittlerweile bei 27 % aller Malware-basierten Angriffe zum Einsatz.

Das Gros der beobachteten Sicherheitsverletzungen ist auf den Diebstahl von Zugangsdaten, Social-Engineering-Angriffe sowie die Ausnutzung von fahrlässigen Verhaltensweisen oder Fehlern der Nutzer zurückzuführen. Da Telearbeiter in dieser Hinsicht besonders gefährdet sind und ihre Zahl derzeit sehr groß ist, empfehlen wir, die Bedrohungsabwehr schwerpunktmäßig entsprechend auszurichten.

Branchenspezifische Erkenntnisse

Das Risiko eines Cyber-Angriffs besteht grundsätzlich für alle Unternehmen, doch die wahrscheinlichste Angriffsform ist nicht überall dieselbe. Deshalb sollten Sie sowohl die Sicherheitslage insgesamt als auch die Situation in Ihrer Branche berücksichtigen, um Ihr Sicherheitsbudget so effizient wie möglich zu nutzen. Aus diesem Grund haben wir die Zahl der untersuchten Branchen auf 16 erhöht. Außerdem enthält der diesjährige Bericht eine Analyse der unterschiedlichen Bedrohungen für kleine und große Unternehmen. Als Grundlage für die Klassifizierung von Unternehmen und Institutionen diente uns wieder das North American Industry Classification System (NAICS).

Hotel- und Gaststättengewerbe (NAICS 72)

In diesem Jahr sind Angriffe auf Kassen- und Bezahlsysteme nicht mehr die häufigste Angriffsform im Hotel- und Gaststättengewerbe. Stattdessen werden die auftretenden Sicherheitsverletzungen zu fast gleichen Teilen durch Malware, Fehler der Mitarbeiter, den Missbrauch gestohlener Anmeldedaten und andere Hackeraktivitäten verursacht. Trotzdem ist die Branche nach wie vor ein bevorzugtes Ziel finanziell motivierter Angreifer, die es auf gespeicherte Kreditkartendaten abgesehen haben.

Häufigkeit	125 Vorfälle, darunter 92 mit bestätigten Datenlecks
Häufigste Angriffsarten	61 % der Datendiebstähle gehen auf das Konto von Crimeware, Webanwendungen und Kassensystemen.
Täter	Extern (79 %), intern (22 %), mehrere Akteure (2 %), Partner (1 %) (Datendiebstähle)
Motive der Täter	Finanzielle Bereicherung (98 %), sekundärer Angriff (2 %) (Datendiebstähle)
Betroffene Daten	Zahlungsdaten (68 %), persönliche Daten (44 %), Anmeldedaten (14 %), sonstige (10 %) (Datendiebstähle)
Wichtigste Gegenmaßnahmen	Beschränkung und Kontrolle der Netzwerkports, -protokolle und -services (CSC 9), Perimeterschutz (CSC 12), Datenschutz (CSC 13)

Medien und Unterhaltung (NAICS 71)

Diese Branche war im aktuellen Berichtszeitraum besonders häufig von Angriffen auf Webanwendungen, Social-Engineering-Kampagnen und aus Fehlern der Mitarbeiter resultierenden Sicherheitsverletzungen betroffen. Außerdem geht aus den von uns erfassten Daten hervor, dass die Denial-of-Service-Angriffe hier höhere Traffic-Volumen erreichten als in anderen Branchen.

Häufigkeit	194 Vorfälle, darunter 98 mit bestätigten Datenlecks
Häufigste Angriffsarten	68 % der Datendiebstähle gehen auf das Konto von Webanwendungen, diversen Fehlern und „sonstigen Ursachen“.
Täter	Extern (67 %), intern (33 %), Partner (1 %), mehrere Akteure (1 %) (Datendiebstähle)
Motive der Täter	Finanzielle Bereicherung (94 %), Gelegenheitsvergehen (6 %) (Datendiebstähle)
Betroffene Daten	Persönliche Daten (84 %), Patientendaten (31 %), sonstige (26 %), Zahlungsdaten (25 %) (Datendiebstähle)
Wichtigste Gegenmaßnahmen	Perimeterschutz (CSC 12), sichere Konfigurationen (CSC 5, CSC 11), Programme zur Verbesserung des Sicherheitsbewusstseins und der entsprechenden Kenntnisse (CSC 17)

Baugewerbe (NAICS 23)

In dieser Branche sind Angriffe auf Webanwendungen und Social Engineering weit verbreitet. Auch der Missbrauch gestohlener Anmeldedaten ist weiterhin ein großes Problem. Positiv zu vermerken sind die vergleichsweise niedrigen Zahlen für Phishing-Angriffe und durch Mitarbeiterfehler verursachte Vorfälle.

Häufigkeit	37 Vorfälle, darunter 25 mit bestätigten Datenlecks
Häufigste Angriffsarten	95 % der Vorfälle gehen auf das Konto von Webanwendungen, Crimeware und „sonstigen Ursachen“.
Täter	Extern (95 %), intern (5 %) (Vorfälle)
Motive der Täter	Finanzielle Bereicherung (84 bis 100 %), Groll/Vergeltung (0 bis 16 %) (Vorfälle)[1]
Betroffene Daten	Persönliche und Anmeldedaten
Wichtigste Gegenmaßnahmen	Sichere Konfigurationen (CSC 5, CSC 11), Perimeterschutz (CSC 12), Kontomanagement und -monitoring (CSC 16)

Bildungswesen (NAICS 61)

Phishing-Angriffe (28 %) und Hackereinbrüche mit gestohlenen Anmeldedaten (23 %) sind in dieser Branche die prominentesten Ursachen von Sicherheitsverletzungen. Daher erweist es sich als großer Nachteil, dass Bildungsinstitutionen bei der Meldung und Eindämmung von Phishing-Kampagnen oft wertvolle Zeit verlieren. Bemerkenswert ist weiterhin, dass es sich bei den im Bildungswesen virulenten Malware-Varianten zu 80 % um Ransomware handelt.

Häufigkeit	819 Vorfälle, darunter 228 mit bestätigten Datenlecks
Häufigste Angriffsarten	81 % der Datendiebstähle gehen auf das Konto von Webanwendungen, diversen Fehlern und „sonstigen Ursachen“.
Täter	Extern (67 %), intern (33 %), Partner (1 %), mehrere Akteure (1 %) (Datendiebstähle)
Motive der Täter	Finanzielle Bereicherung (92 %), Spaß (5 %), Gelegenheitsvergehen (3 %), Spionage (3 %), sekundärer Angriff (2 %) (Datendiebstähle)
Betroffene Daten	Persönliche Daten (75 %), Anmeldedaten (30 %), sonstige (23 %), interne Daten (13 %) (Datendiebstähle)
Wichtigste Gegenmaßnahmen	Programme zur Verbesserung des Sicherheitsbewusstseins und der entsprechenden Kenntnisse (CSC 17), Perimeterschutz (CSC 12), sichere Konfigurationen (CSC 5, CSC 11)

Finanz- und Versicherungsbranche (NAICS 52)

Die Angriffe auf Unternehmen aus dieser Branche zielen in 63 % der Fälle auf den Diebstahl von Daten, die sich leicht zu Geld machen lassen. Zugleich sind 18 % der erfassten Sicherheitsverletzungen auf Insider mit finanziellen Motiven und 9 % auf Mitarbeiterfehler zurückzuführen. Im Vergleich zum Vorjahr stellt das einen Rückgang bei Insider-Angriffen und einen Anstieg bei versehentlich verursachten Sicherheitsverletzungen dar. Das mag positiv wirken, doch beide Arten von Vorfällen verursachen Schäden. Auch Angriffe auf Webanwendungen (oft mit gestohlenen Anmeldedaten) spielen in dieser Branche weiterhin eine wichtige Rolle.

Häufigkeit	1.509 Vorfälle, darunter 448 mit bestätigten Datenlecks
Häufigste Angriffsarten	81 % der Datendiebstähle gehen auf das Konto von Webanwendungen, diversen Fehlern und „sonstigen Ursachen“.
Täter	Extern (64 %), intern (35 %), Partner (2 %), mehrere Akteure (1 %) (Datendiebstähle)
Motive der Täter	Finanzielle Bereicherung (91 %), Spionage (3 %), Groll/Vergeltung (3 %) (Datendiebstähle)
Betroffene Daten	Persönliche Daten (77 %), Anmeldedaten (35 %), sonstige (35 %), Bankdaten (32 %) (Datendiebstähle)
Wichtigste Gegenmaßnahmen	Programme zur Verbesserung des Sicherheitsbewusstseins und der entsprechenden Kenntnisse (CSC 17), Perimeterschutz (CSC 12), sichere Konfigurationen (CSC 5, CSC 11)

Gesundheitswesen (NAICS 62)

Dieser Bereich ist nach wie vor ein bevorzugtes Ziel von finanziell motivierten Ransomware-Angriffen. Außerdem legen die von uns erhobenen Daten den Schluss nahe, dass diese Branche besonders mit verlorenen oder gestohlenen Ressourcen sowie mit falschen Verhaltensweisen und Fehlern der Mitarbeiter zu kämpfen hat. Bei den Letzteren handelt es sich zumeist um Pannen bei der Bereitstellung von Daten, während der Missbrauch von Zugriffsrechten zurückgegangen ist.

Häufigkeit	798 Vorfälle, darunter 521 mit bestätigten Datenlecks
Häufigste Angriffsarten	72 % der Datendiebstähle gehen auf das Konto von Webanwendungen, diversen Fehlern und „sonstigen Ursachen“.
Täter	Extern (51 %), intern (48 %), Partner (2 %), mehrere Akteure (1 %) (Datendiebstähle)
Motive der Täter	Finanzielle Bereicherung (88 %), Spaß (4 %), Gelegenheitsvergehen (3 %) (Datendiebstähle)
Betroffene Daten	Persönliche Daten (77 %), Patientendaten (67 %), Anmeldedaten (18 %), sonstige (18 %) (Datendiebstähle)
Wichtigste Gegenmaßnahmen	Programme zur Verbesserung des Sicherheitsbewusstseins und der entsprechenden Kenntnisse (CSC 17), Perimeterschutz (CSC 12), Datenschutz (CSC 13)

IT und TK-Beratung (NAICS 51)

In dieser Branche dominieren Angriffe auf Webanwendungen unter Ausnutzung von Schwachstellen sowie mithilfe gestohlener Anmeldedaten. Dabei spielen Fehler der Mitarbeiter – insbesondere bei der Konfiguration von Cloud-Datenbanken – eine signifikante Rolle. Außerdem ist eine steigende Zahl von Denial-of-Service-Angriffen zu verzeichnen.

Häufigkeit	5.741 Vorfälle, darunter 360 mit bestätigten Datenlecks
Häufigste Angriffsarten	88 % der Datendiebstähle gehen auf das Konto von Webanwendungen, diversen Fehlern und „sonstigen Ursachen“.
Täter	Extern (67 %), intern (34 %), mehrere Akteure (2 %), Partner (1 %) (Datendiebstähle)
Motive der Täter	Finanzielle Bereicherung (88 %), Spionage (7 %), Spaß (2 %), Groll/ Vergeltung (2 %), sonstige (1 %) (Datendiebstähle)
Betroffene Daten	Persönliche Daten (69 %), Anmeldedaten (41 %), sonstige (34 %), interne Daten (16 %) (Datendiebstähle)
Wichtigste Gegenmaßnahmen	Sichere Konfigurationen (CSC 5, CSC 11), kontinuierliches Schwachstellenmanagement (CSC 3), Programme zur Verbesserung des Sicherheitsbewusstseins und der entsprechenden Kenntnisse (CSC 17)

Fertigungsindustrie (NAICS 31-33)

Herstellungs- und Fertigungsunternehmen stehen im Visier von Cyber-Kriminellen, die mit Passwort-Dumpern und anderen Methoden erbeutete Anmeldedaten nutzen, um in Systeme einzudringen und Daten zu stehlen. Obwohl das Gros dieser Angriffe finanziellen Motiven dient, ist der Anteil der Industriespionage-Angriffe durchaus relevant. Ein weiteres hartnäckiges Problem sind unbefugte Datenzugriffe durch Mitarbeiter, die ihre Zugriffsrechte für kriminelle Zwecke missbrauchen.

Häufigkeit	922 Vorfälle, darunter 381 mit bestätigten Datenlecks
Häufigste Angriffsarten	64 % der Datendiebstähle gehen auf das Konto von Crimeware, Webanwendungen und missbrauchten Zugriffsrechten.
Täter	Extern (75 %), intern (25 %), Partner (1 %) (Datendiebstähle)
Motive der Täter	Finanzielle Bereicherung (73 %), Spionage (27 %) (Datendiebstähle)
Betroffene Daten	Anmeldedaten (55 %), persönliche Daten (49 %), sonstige (25 %), Zahlungsdaten (20 %) (Datendiebstähle)
Wichtigste Gegenmaßnahmen	Perimeterschutz (CSC 12), Programme zur Verbesserung des Sicherheitsbewusstseins und der entsprechenden Kenntnisse (CSC 17), Datenschutz (CSC 13)

Berg- und Tagebau, Erdöl- und Erdgasförderung sowie Ver- und Entsorgung (NAICS 21 + 22)

Auch wenn in dieser Branche ein breites Spektrum krimineller Aktivitäten zu beobachten ist, dominieren im Datenset Social-Engineering-Angriffe wie Phishing und Fake-Anrufe (wobei jedoch keine Angaben zur Häufigkeit von Datenlecks vorliegen). Darüber hinaus ist der Sektor von Cyber-Spionage und Angriffen auf Förder- und Produktionsanlagen betroffen.

Häufigkeit	194 Vorfälle, darunter 43 mit bestätigten Datenlecks
Häufigste Angriffsarten	74 % der Datendiebstähle gehen auf das Konto von Webanwendungen, Cyber-Spionage und „sonstigen Ursachen“.
Täter	Extern (75 %), intern (28 %), mehrere Akteure (2 %) (Datendiebstähle)
Motive der Täter	Finanzielle Bereicherung (63 bis 95 %), Spionage (8 bis 43 %), Gelegenheitsvergehen/sekundäre Angriffe/sonstige (jeweils 0 bis 17 %), Angst/Spaß/Groll/Vergeltung/ideologische Gründe (jeweils 0 bis 9 %) (Datendiebstähle)[1]
Betroffene Daten	Anmeldedaten (41 %), persönliche Daten (41 %), sonstige (35 %), interne Daten (19 %) (Datendiebstähle)
Wichtigste Gegenmaßnahmen	Sichere Konfigurationen (CSC 5, CSC 11), Perimeterschutz (CSC 12), Programme zur Verbesserung des Sicherheitsbewusstseins und der entsprechenden Kenntnisse (CSC 17)

Sonstige Dienstleister (NAICS 81)

Diese Kategorie umfasst unterschiedliche Unternehmen, darunter Anbieter von persönlichen Dienstleistungen und Reparaturservices sowie gemeinnützige und religiöse Organisationen. Die hier erfassten Angriffe sind größtenteils finanziell motiviert und richten sich in 39 % der Fälle gegen Webanwendungen. Dabei erbeuten die Hacker nicht nur Anmeldedaten, sondern vor allem personenbezogene Informationen. Zugleich ist festzustellen, dass zahlreiche Vorfälle in diesem Sektor aus Fehlern der Mitarbeiter resultieren – insbesondere bei der Konfiguration und der Bereitstellung von IT-Ressourcen.

Häufigkeit	107 Vorfälle, darunter 66 mit bestätigten Datenlecks
Häufigste Angriffsarten	83 % der Datendiebstähle gehen auf das Konto von Webanwendungen, diversen Fehlern und „sonstigen Ursachen“.
Täter	Extern (68 %), intern (33 %), mehrere Akteure (2 %) (Datendiebstähle)
Motive der Täter	Finanzielle Bereicherung (60 bis 98 %), Spionage (0 bis 28 %), Gelegenheitsvergehen/Angst/Spaß/Groll/Vergeltung/sekundäre Angriffe/sonstige (jeweils 0 bis 15 %) (Datendiebstähle)[1]
Betroffene Daten	Persönliche Daten (81 %), sonstige (42 %), Anmeldedaten (36 %), interne Daten (25 %) (Datendiebstähle)
Wichtigste Gegenmaßnahmen	Perimeterschutz (CSC 12), Programme zur Verbesserung des Sicherheitsbewusstseins und der entsprechenden Kenntnisse (CSC 17), sichere Konfigurationen (CSC 5, CSC 11)

Anbieter qualifizierter, technischer und wissenschaftlicher Dienstleistungen (NAICS 54)

In dieser Branche stehlen finanziell motivierte Angreifer nach wie vor Anmeldedaten, um sich Zugriff auf Webanwendungen zu verschaffen. Dazu nutzen sie vor allem Social Engineering in Form von Phishing und Fake-Anrufen. Zusätzlich werden Unternehmen aus diesem Sektor regelmäßig zum Ziel von Denial-of-Service-Angriffen.

Häufigkeit	7.463 Vorfälle, darunter 326 mit bestätigten Datenlecks
Häufigste Angriffsarten	79 % der Datendiebstähle gehen auf das Konto von Webanwendungen, diversen Fehlern und „sonstigen Ursachen“.
Täter	Extern (75 %), intern (22 %), Partner (3 %), mehrere Akteure (1 %) (Datendiebstähle)
Motive der Täter	Finanzielle Bereicherung (93 %), Spionage (8 %), ideologische Motive (1 %) (Datendiebstähle)
Betroffene Daten	Persönliche Daten (75 %), Anmeldedaten (45 %), sonstige (32 %), interne Daten (27 %) (Datendiebstähle)
Wichtigste Gegenmaßnahmen	Sichere Konfigurationen (CSC 5, CSC 11), Programme zur Verbesserung des Sicherheitsbewusstseins und der entsprechenden Kenntnisse (CSC 17), Perimeterschutz (CSC 12)

Öffentliche Verwaltung (NAICS 92)

Staatliche Behörden und Institutionen haben immer wieder mit Ransomware-Angriffen durch finanziell motivierte Kriminelle zu kämpfen. Zugleich sind in diesem Sektor weiterhin Vorfälle infolge von Fehlern bei der Bereitstellung und Konfiguration von IT-Ressourcen zu beobachten.

Häufigkeit	6.843 Vorfälle, darunter 346 mit bestätigten Datenlecks
Häufigste Angriffsarten	73 % der Datendiebstähle gehen auf das Konto von Webanwendungen, diversen Fehlern und „sonstigen Ursachen“.
Täter	Extern (59 %), intern (43 %), mehrere Akteure (2 %), Partner (1 %) (Datendiebstähle)
Motive der Täter	Finanzielle Bereicherung (75 %), Spionage (19 %), Spaß (3 %) (Datendiebstähle)
Betroffene Daten	Persönliche Daten (51 %), sonstige (34 %), Anmeldedaten (33 %), interne Daten (14 %) (Datendiebstähle)
Wichtigste Gegenmaßnahmen	Programme zur Verbesserung des Sicherheitsbewusstseins und der entsprechenden Kenntnisse (CSC 17), Perimeterschutz (CSC 12), sichere Konfigurationen (CSC 5, CSC 11)

Immobilien-, Wohnungs- und Leasing-Unternehmen (NAICS 53)

In dieser Branche kommt es häufig zum Diebstahl von Anmeldedaten, die dann für den unbefugten Zugriff auf geschäftlich genutzte Webanwendungen missbraucht werden. Außerdem nutzen die Kriminellen Social Engineering, um sich in die Prozesse zur Übertragung von Eigentumsrechten einzuschalten und die hierbei getätigten Zahlungen auf ihre eigenen Konten umzuleiten. Dabei profitieren sie von Konfigurationsfehlern, die hier – wie in zahlreichen anderen Branchen – als signifikanter Faktor in Erscheinung treten.

Häufigkeit	37 Vorfälle, darunter 33 mit bestätigten Datenlecks
Häufigste Angriffsarten	88 % der Datendiebstähle gehen auf das Konto von Webanwendungen, diversen Fehlern und „sonstigen Ursachen“.
Täter	Extern (73 %), intern (27 %) (Datendiebstähle)
Motive der Täter	Finanzielle Bereicherung (45 bis 97 %), Gelegenheitsvergehen/Spionage (jeweils 0 bis 40 %), Angst/Spaß/Groll/Vergeltung/ideologische Motive/sekundäre Angriffe/sonstige (jeweils 0 bis 21 %) (Datendiebstähle)[1]
Betroffene Daten	Persönliche Daten (83 %), interne Daten (43 %), sonstige (43 %), Anmeldedaten (40 %) (Datendiebstähle)
Wichtigste Gegenmaßnahmen	Sichere Konfigurationen (CSC 5, CSC 11), Programme zur Verbesserung des Sicherheitsbewusstseins und der entsprechenden Kenntnisse (CSC 17), Perimeterschutz (CSC 12)

Einzelhandel (NAICS 44-45)

In dieser Branche sind Angriffe auf Online-Shops die bei Weitem häufigste Bedrohung. Die (früher beträchtliche) Zahl der Angriffe auf die Kassen- und Bezahlsysteme in Verkaufsfilialen ist hingegen auch in diesem Jahr auf dem niedrigen Stand von 2019 geblieben. Das zeigt einmal mehr, dass Cyber-Kriminelle den Trend zur Migration in die Cloud auf ihre Weise mitgehen. Zugleich ist zu beobachten, dass nicht nur Kreditkarten- und Kontodaten, sondern auch Anmeldedaten und andere personenbezogene Informationen auf der Wunschliste der Angreifer stehen.

Häufigkeit	287 Vorfälle, darunter 146 mit bestätigten Datenlecks
Häufigste Angriffsarten	72 % der Datendiebstähle gehen auf das Konto von Webanwendungen, diversen Fehlern und „sonstigen Ursachen“.
Täter	Extern (75 %), intern (25 %), Partner (1 %), mehrere Akteure (1 %) (Datendiebstähle)
Motive der Täter	Finanzielle Bereicherung (99 %), Spionage (1 %) (Datendiebstähle)
Betroffene Daten	Persönliche Daten (49 %), Zahlungsdaten (47 %), Anmeldedaten (27 %), sonstige (25 %) (Datendiebstähle)
Wichtigste Gegenmaßnahmen	Perimeterschutz (CSC 12), sichere Konfigurationen (CSC 5, CSC 11), kontinuierliches Schwachstellenmanagement (CSC 3)

Transport und Logistik (NAICS 48-49)

Transport- und Logistikunternehmen müssen häufig feststellen, dass ihre Webanwendungen von organisierten Cyber-Kriminellen angegriffen werden. Außerdem werden viele Sicherheitsverletzungen in diesem Sektor durch Fehler der Mitarbeiter (beispielsweise bei der Einrichtung von Datenbanken) sowie durch Phishing-Kampagnen, Fake-Anrufe und andere Social-Engineering-Angriffe verursacht.

Häufigkeit	112 Vorfälle, darunter 67 mit bestätigten Datenlecks
Häufigste Angriffsarten	69 % der Datendiebstähle gehen auf das Konto von Webanwendungen, diversen Fehlern und „sonstigen Ursachen“.
Täter	Extern (68 %), intern (32 %) (Datendiebstähle)
Motive der Täter	Finanzielle Bereicherung (74 bis 98 %), Spionage (1 bis 21 %), Gelegenheitsvergehen (0 bis 15 %) (Datendiebstähle)[1]
Betroffene Daten	Persönliche Daten (64 %), Anmeldedaten (34 %), sonstige (23 %) (Datendiebstähle)
Wichtigste Gegenmaßnahmen	Perimeterschutz (CSC 12), Programme zur Verbesserung des Sicherheitsbewusstseins und der entsprechenden Kenntnisse (CSC 17), sichere Konfigurationen (CSC 5, CSC 11)

Die Situation der KMU

Obwohl es nach wie vor Unterschiede zwischen den Gefahren für kleine und mittlere Unternehmen (KMU) einerseits und Großkonzerne andererseits gibt, werden diese zusehends kleiner. Das liegt unter anderem an der zunehmenden Nutzung cloud- und webbasierter Tools und an der steigenden Zahl der Social-Engineering-Angriffe. Mit anderen Worten: Cyber-Kriminelle haben sich mittlerweile an die neuen Geschäftsmodelle der KMU angepasst und die schnellsten und einfachsten Angriffsmethoden für die neue Situation identifiziert.

	Klein (weniger als 1.000 Angestellte)	Groß (mehr als 1.000 Angestellte)
Häufigkeit	407 Vorfälle, darunter 221 mit bestätigten Datenlecks	8.666 Vorfälle, darunter 576 mit bestätigten Datenlecks
Häufigste Angriffsarten	70 % der Datendiebstähle gehen auf das Konto von Webanwendungen, diversen Fehlern und „sonstigen Ursachen“.	70 % der Datendiebstähle gehen auf das Konto von Crimeware, missbrauchten Zugriffsrechten und „sonstigen Ursachen“.
Täter	Extern (74 %), intern (26 %), Partner (1 %), mehrere Akteure (1 %) (Datendiebstähle)	Extern (79 %), intern (21 %), Partner (1 %), mehrere Akteure (1 %) (Datendiebstähle)
Motive der Täter	Finanzielle Bereicherung (83 %), Spionage (8 %), Spaß (3 %), Groll/Vergeltung (3 %) (Datendiebstähle)	Finanzielle Bereicherung (79 %), Spionage (14 %), Spaß (2 %), Groll/Vergeltung (2 %) (Datendiebstähle)
Betroffene Daten	Anmeldedaten (52 %), persönliche Daten (30 %), sonstige (20 %), interne Daten (14 %), Patientendaten (14 %) (Datendiebstähle)	Anmeldedaten (64 %), sonstige (26 %), persönliche Dedaten (19 %), interne Daten (12 %) (Datendiebstähle)

Ergebnisse für spezifische Regionen

Der neueste DBIR enthält erstmals nach Regionen aufgeschlüsselte Daten.

Abbildung 4: Nordamerika

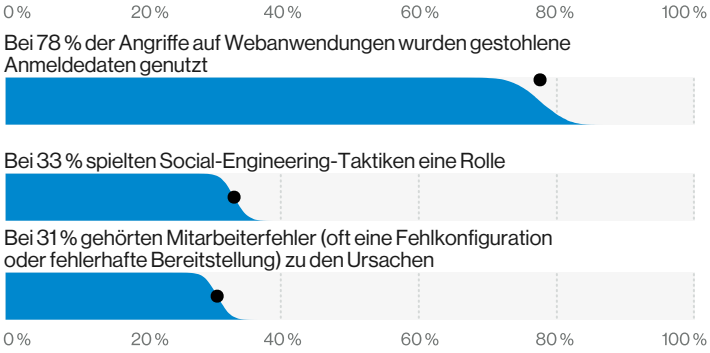


Abbildung 5: Europa, Naher Osten & Afrika (EMEA)

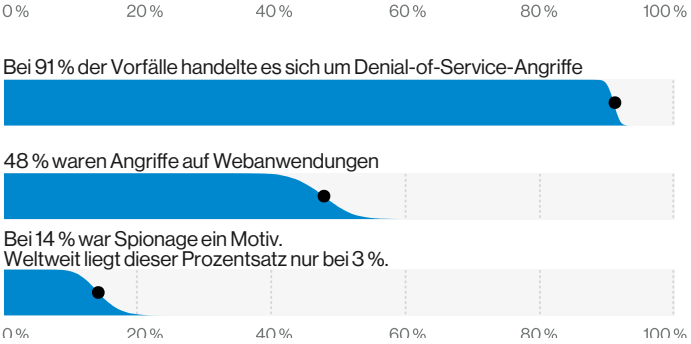


Abbildung 6: Asien & pazifischer Raum

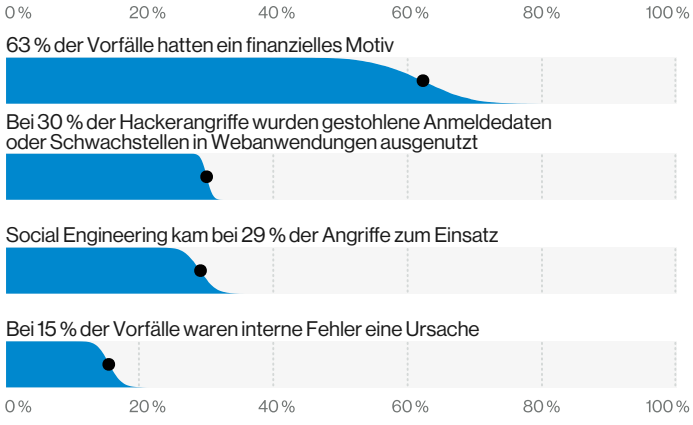
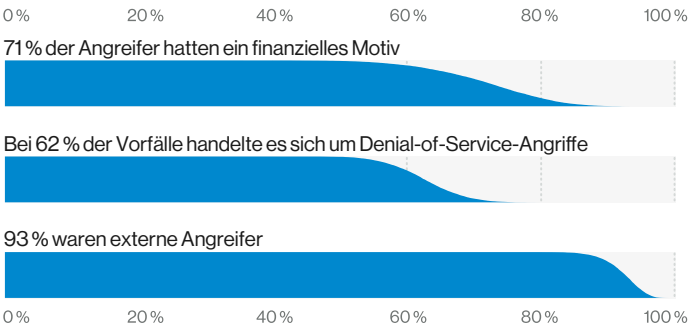


Abbildung 7: Lateinamerika & Karibik



Best Practices

In diesem Jahr bieten wir Ihnen zusätzlich konkrete Vorschläge für praktische Maßnahmen zur Stärkung der Sicherheit. Die im Folgenden aufgeführten Best Practices sind Ergebnis eines Abgleichs der im DBIR präsentierten Daten mit vom Center for Internet Security empfohlenen Critical Security Controls (CSC):

Kontinuierliches Schwachstellenmanagement (CSC 3)

Suchen und beheben Sie Fehlkonfigurationen und Schwachstellen im Anwendungscode, die für Angriffe ausgenutzt werden könnten.

Sichere Konfigurationen (CSC 5, CSC 11)

Stellen Sie sicher, dass alle Systeme nur die jeweils unbedingt nötigen Funktionen und Zugriffsmöglichkeiten bieten.

Sicherung von E-Mail-Systemen und Browsern (CSC 7)

Sichern Sie E-Mail-Clients und Browser, um Ihren Nutzern beim Surfen im Internet den bestmöglichen Schutz zu bieten.

Beschränkung und Kontrolle der Netzwerkports, -protokolle und -services (CSC 9)

Ermitteln Sie, über welche Services und Ports Ihre Systeme zugänglich sein müssen und deaktivieren Sie überflüssige Zugriffsmöglichkeiten.

Perimeterschutz (CSC 12)

Zusätzlich zu Ihren Firewalls sollten Sie die Implementierung von Monitoring-Lösungen, Proxyservern und Multifaktor-Authentifizierungsverfahren erwägen.

Datenschutz (CSC 13)

Verhindern Sie unbefugte Zugriffe auf sensible Informationen, indem Sie ein Verzeichnis dieser Daten anlegen und für deren umfassende Verschlüsselung sorgen. In diesem Zusammenhang sollte auch die Nutzung der von der IT-Abteilung genehmigten Cloud- und E-Mail-Anwendungen verbindlich durchgesetzt werden.

Kontomonitoring (CSC 16)

Verfolgen Sie die von den Nutzerkonten Ihres Unternehmens ausgehenden Aktivitäten, um Hackereinbrüche mit gestohlenen Anmeldedaten umgehend aufzudecken und zu unterbinden. Begleitend sollten Sie die Einführung von Multifaktor-Authentifizierungsverfahren in Angriff nehmen.

Programme zur Verbesserung des Sicherheitsbewusstseins und der entsprechenden Kenntnisse (CSC 17)

Klären Sie Ihre Mitarbeiter und Nutzer über gängige Angriffsmethoden und die Gefahren fahrlässiger Handlungsweisen auf.

Halten Sie sich und Ihr Team auf dem Laufenden

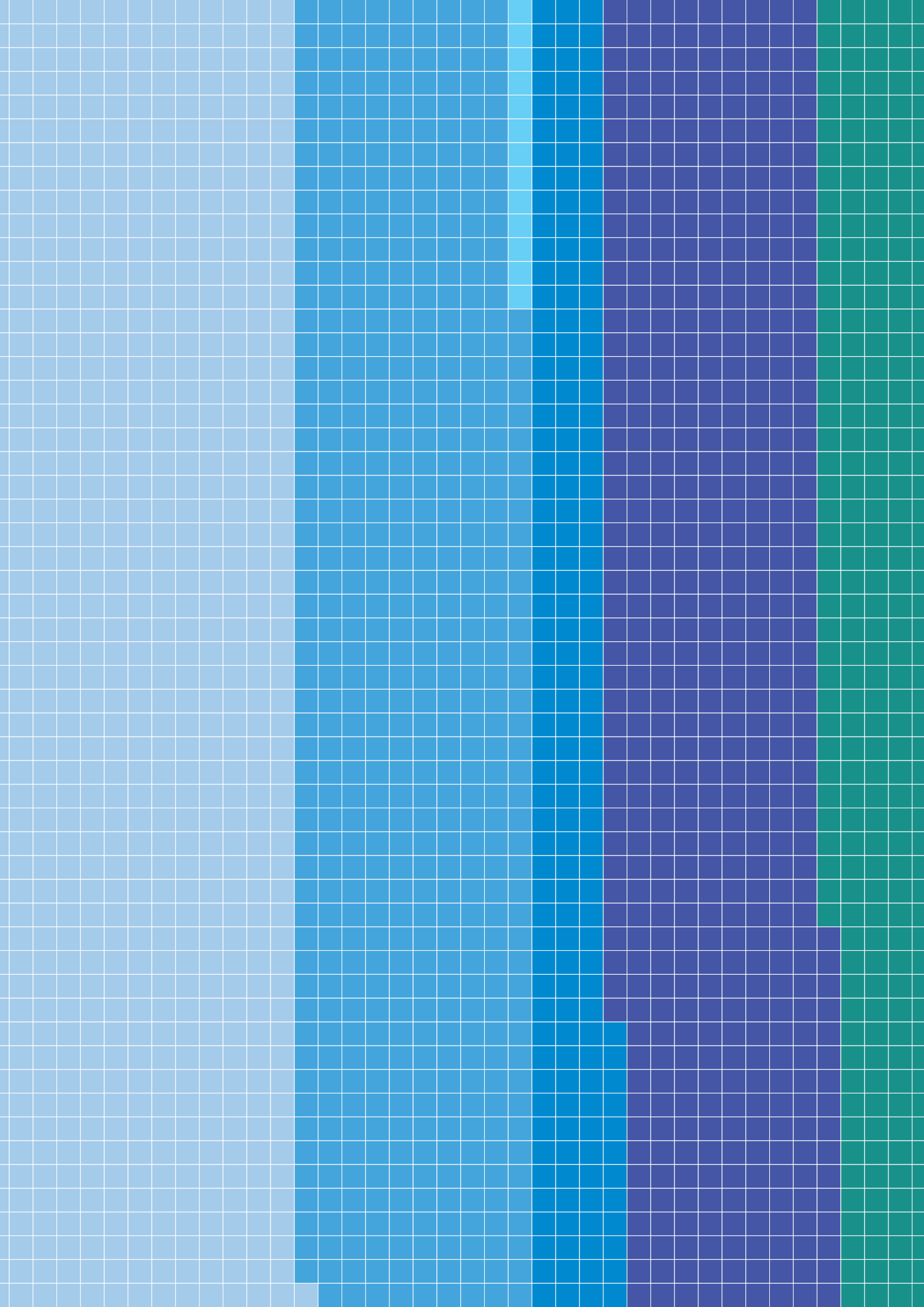
Um den aktuellen Bedrohungen die Stirn bieten zu können, benötigen Sie zuverlässige Informationen, anhand derer Sie Ihre Sicherheitsmaßnahmen gezielt stärken und Ihre Mitarbeiter schulen können. Deshalb bietet Ihnen die vollständige Ausgabe des DBIR einen detaillierten, praxisrelevanten Überblick über die Ziele, Methoden und Aktivitäten der Angreifer.

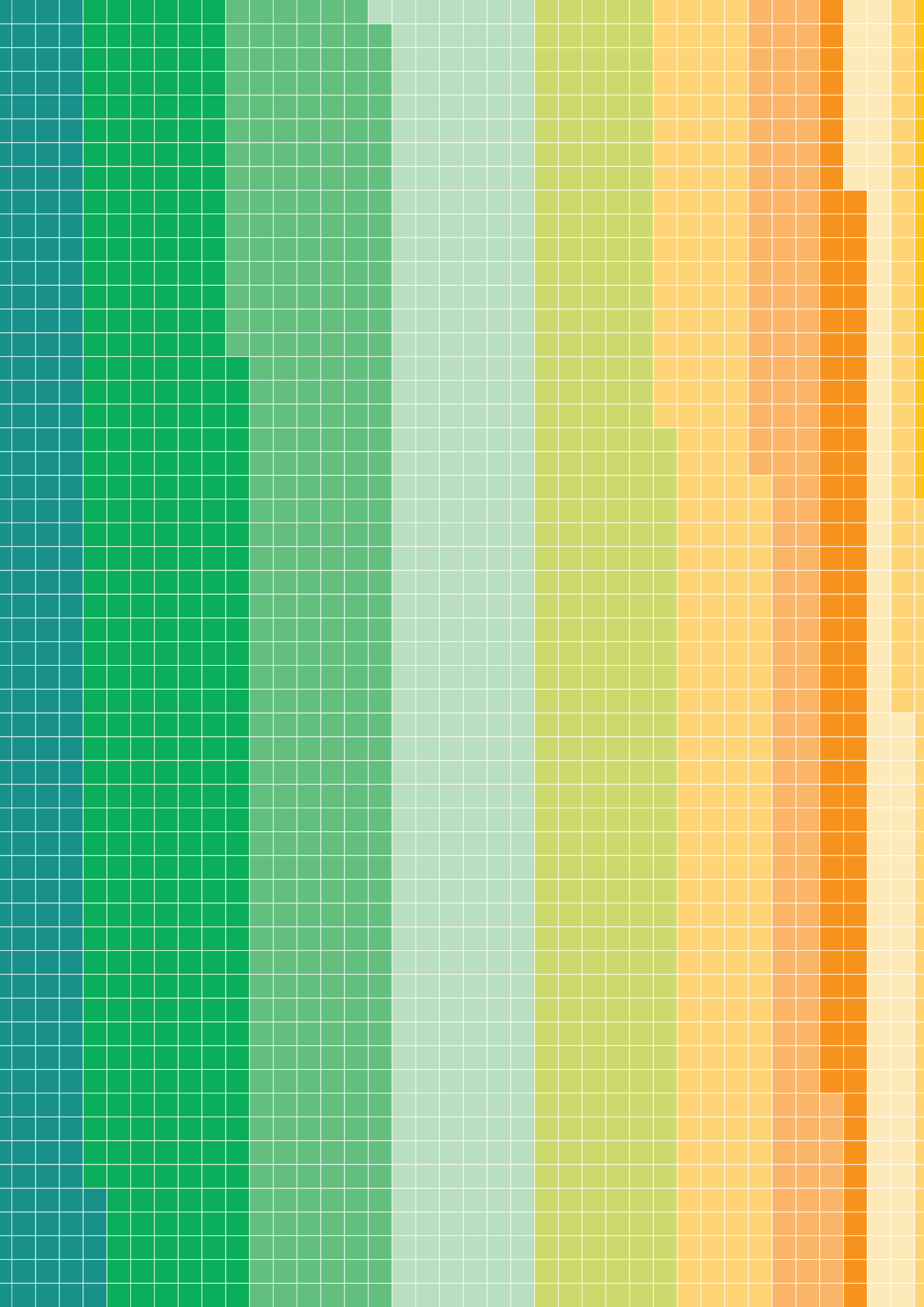
Sie erhalten den vollständigen DBIR 2020 unter https://enterprise.verizon.com/de-de/resources/reports/dbir.

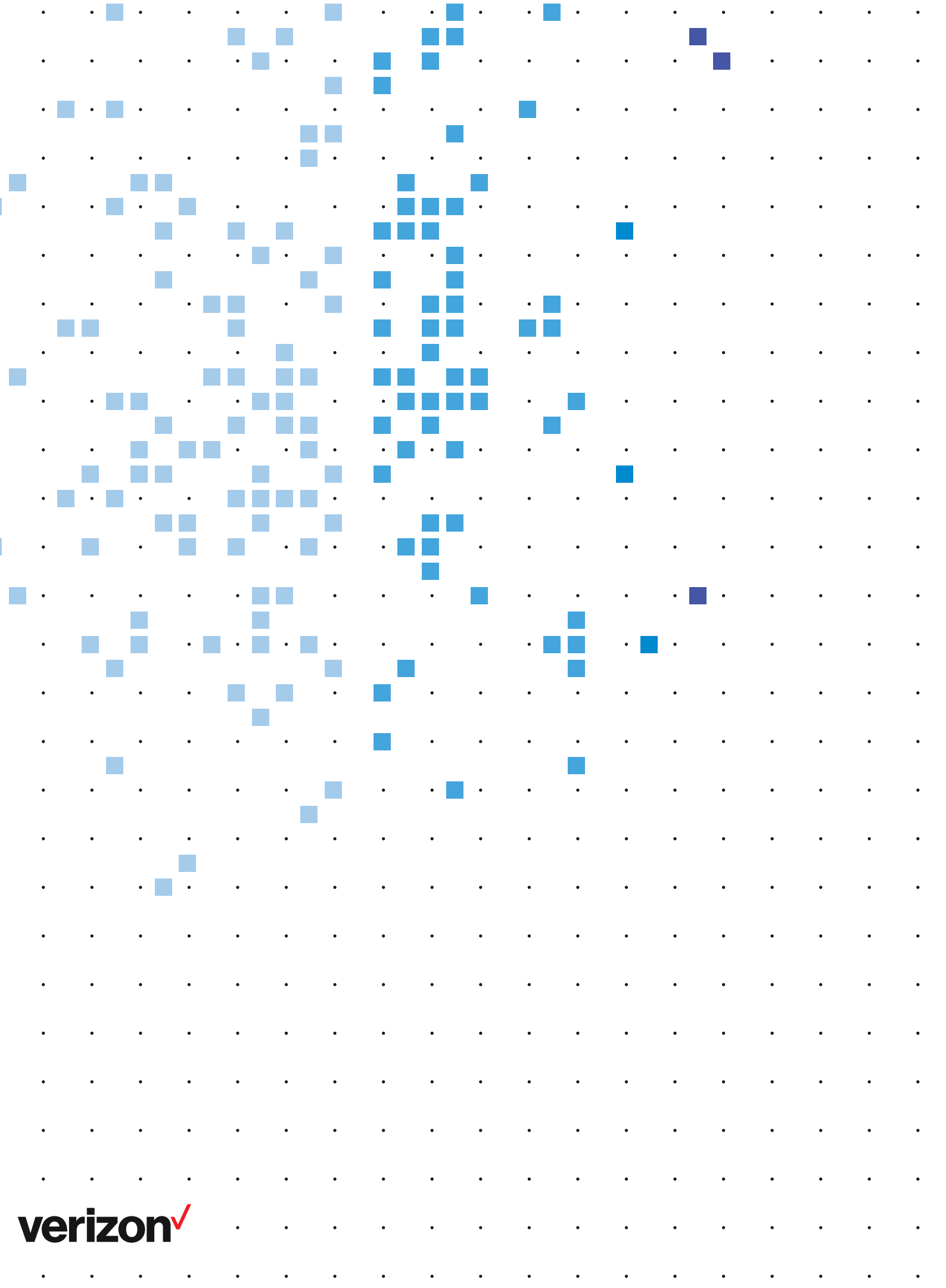
Möchten Sie dazu beitragen, die Welt sicherer zu machen?

Der DBIR basiert auf Beiträgen von Dutzenden von Unternehmen und könnte mit Ihrer Beteiligung noch besser werden. Falls Sie interessiert sind oder Verbesserungsvorschläge für den nächsten DBIR haben, 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

1 Aufgrund der relativ kleinen Stichproben geben wir hier das ganze Spektrum der Prozentsätze an, damit deutlich wird, wie groß das Konfidenzintervall für diese Branchen ist. Weitere Angaben zu diesem Ansatz finden Sie im ausführlichen Bericht.






verizon