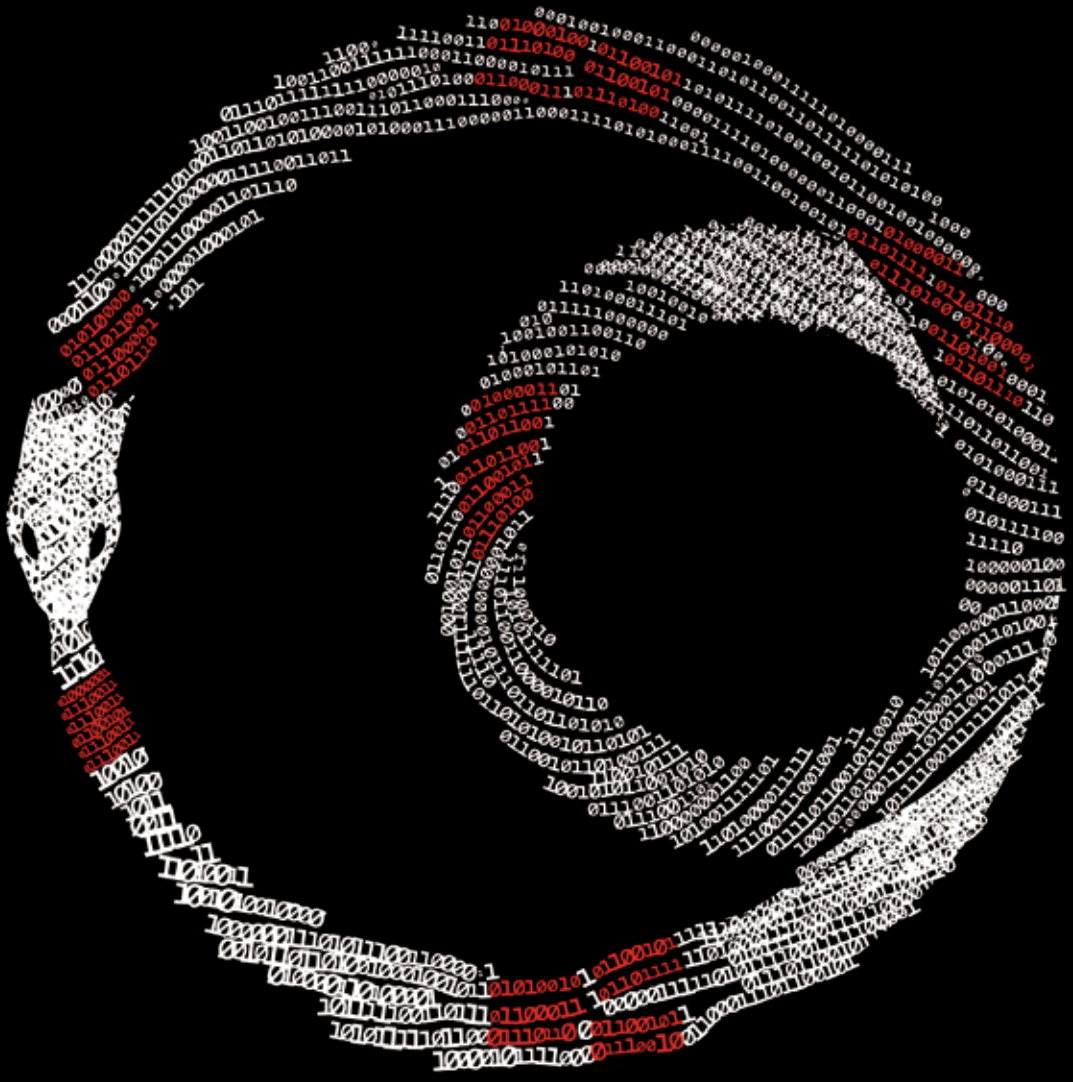
Kurzfassung

Verizon Incident Preparedness and Response Report

Schützen Sie Ihr Unternehmen vor Datendiebstahl



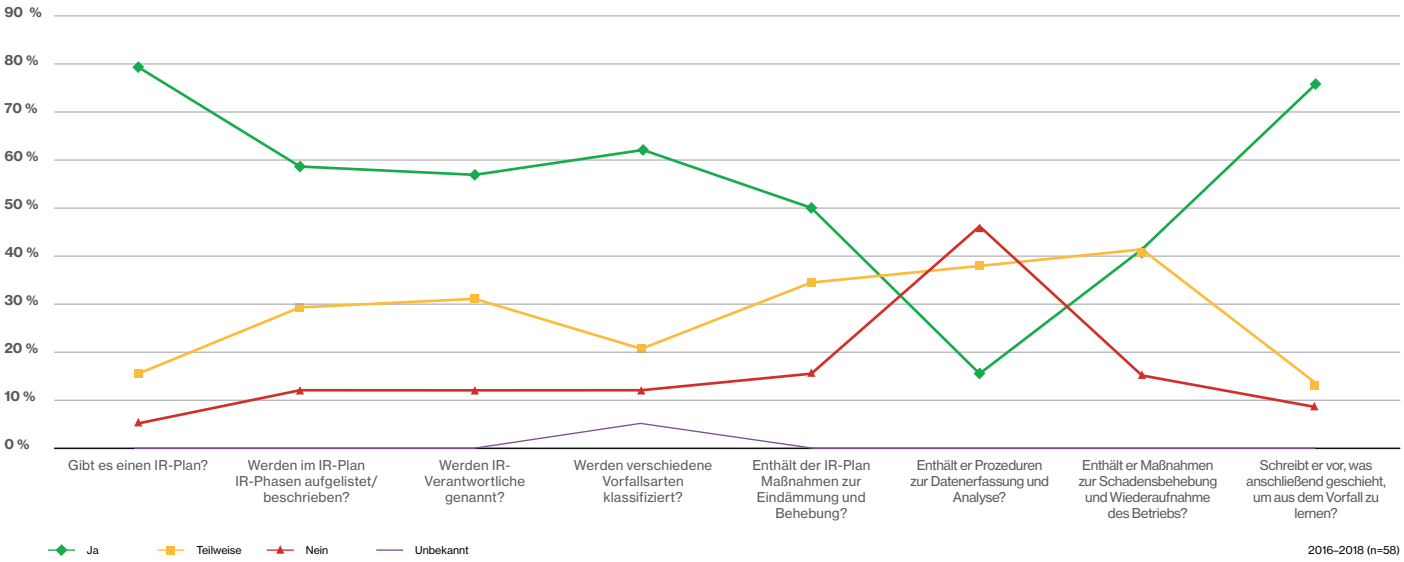
verizon

Im Krisenstab

Die Vorbereitung auf Datenschutzverletzungen und andere Cyber-Sicherheitsvorfälle ist keine triviale Aufgabe. Sie erfordert eine genaue Kenntnis Ihrer Umgebung und spezifischen Bedrohungen, effektive Teamarbeit und natürlich einen Notfallplan (auch Incident-Response-Plan oder kurz IR-Plan genannt).

Deshalb haben wir den vorliegenden Bericht Verizon Incident Preparedness and Response, VIPR (Bereitschaft zur Erkennung und Abwehr von Bedrohungen) erstellt. Er beruht auf Erfahrungen aus der Bewertung von IR-Plänen und der Simulation von Datensicherheitsverstößen im Zeitraum von 2016 bis 2018 und enthält viele der Empfehlungen, die wir auch unseren Kunden gegeben haben.

Bewertung von Plänen
Phasen 1–6: Auswahl der IR-Plan-Komponenten



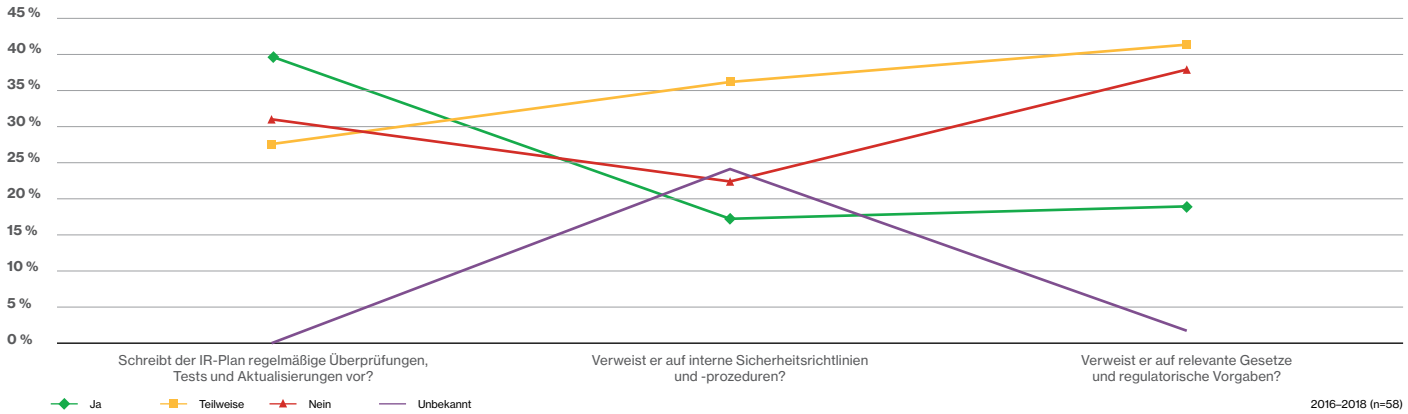
Diese Ausgabe von „Schützen Sie Ihr Unternehmen vor Datenfressern“ soll Ihnen helfen, sich in die Situation Ihrer verschiedenen IR-Verantwortlichen zu versetzen, damit Sie die Maßnahmen Ihres Unternehmens zur Reaktion auf Sicherheitsvorfälle und zur Schadensbegrenzung und -behebung effektiver definieren und stärken können.

Außerdem haben wir Szenarien für fünf Datensicherheitsverstöße in diesen Bericht aufgenommen (siehe auch „Nutzung der Simulationskits für Datenverluste“). Diese Szenarien veranschaulichen, aus welchen Schritten die jeweilige Phase des IR-Plans besteht und warum diese wichtig sind. Sie können dieses Layout als Vorlage für die Erstellung bzw. Aktualisierung Ihres eigenen IR-Plans und des dazugehörigen IR-Handbuchs verwenden. Die Szenarien eignen sich auch zur Bereicherung Ihrer Workshops und Planübungen.

Planung und Vorbereitung

Die sorgfältige Planung und Vorbereitung ist für die effektive Reaktion auf einen Cyber-Sicherheitsvorfall unerlässlich. In dieser Phase werden der IR-Plan erstellt und die relevanten Parteien identifiziert: interne IR-Verantwortliche, die für die taktische Reaktion verantwortlichen Personen und Teams sowie die eventuell hinzuzuziehenden externen Partner, wie Serviceanbieter, Regulierungsgremien und Berater.

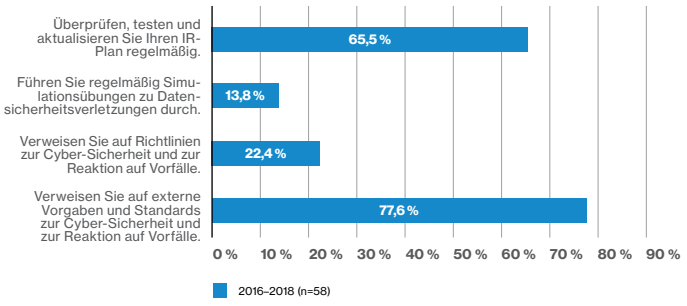
Bewertung von Plänen
Phase 1: Relevanz des Plans



Beobachtungen aus unseren Bewertungen

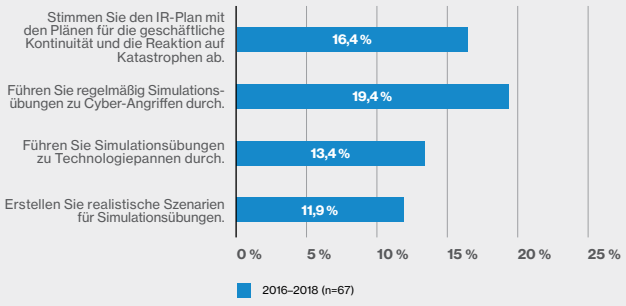
Nur in 40 % der von uns zwischen 2016 und 2018 bewerteten IR-Pläne wurde das regelmäßige Überprüfen, Testen und Aktualisieren des IR-Plans explizit erwähnt. In 31 % der Pläne fehlte dieser Punkt vollständig. 22 % der untersuchten IR-Pläne enthielten keinen Verweis auf interne Sicherheitsrichtlinien oder -prozeduren. In weiteren 30 % waren die diesbezüglichen Verweise unvollständig. Verweise auf gesetzliche Vorgaben oder Verordnungen zur Cyber-Sicherheit, Reaktion auf Vorfälle und Meldung von Sicherheitsverletzungen fehlten in 38 % der untersuchten IR-Pläne ganz und waren in weiteren 41 % nur teilweise vorhanden.

Empfehlungen aufgrund unserer Beurteilungen



Die am häufigsten ausgesprochenen Empfehlungen waren, Verweise auf externe Compliance-Vorgaben und Standards wie GLBA, ISO 27001 usw. in den IR-Plan aufzunehmen (78 %) und den IR-Plan regelmäßig zu überprüfen, zu testen und zu aktualisieren (66 %).

Empfehlungen für Simulationsübungen



In puncto Simulationen empfahlen wir 2016–2018 am häufigsten, Simulationsübungen zu Cyber-Angriffen und Technologiepannen durchzuführen (20 % bzw. 13 %).

Erkennung und Prüfung von Vorfällen

Eine effektive Reaktion setzt voraus, dass Cyber-Sicherheitsvorfälle rechtzeitig erkannt und richtig eingeordnet werden.

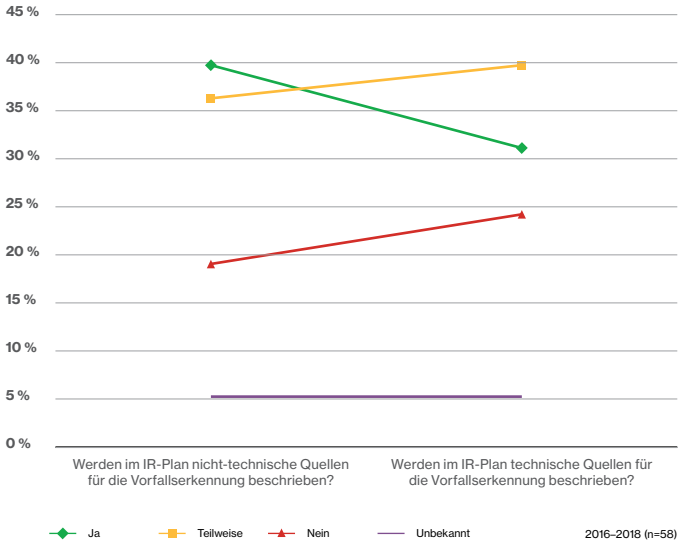
Beobachtungen aus unseren Bewertungen

Die Beschreibung der für die Vorfallserkennung genutzten Quellen ließ in den 2016–2018 bewerteten IR-Plänen zu wünschen übrig: nicht-technische Quellen wurden in 40 % der Pläne vollständig (und in weiteren 36 % teilweise) beschrieben. Technische Quellen wurden sogar nur in 31 % der Pläne vollständig (und in weiteren 40 % teilweise) beschrieben.

Empfehlungen aufgrund unserer Beurteilungen

Beschreiben Sie die technischen und nicht-technischen Quellen für die Erkennung von Sicherheitsverstößen.

Bewertung von Plänen
Phase 2: Quellen für die Bedrohungserkennung



Eindämmung und Behebung

In dieser Phase geht es darum, Cyber-Bedrohungen einzudämmen, um den Schaden zu minimieren und weitere Schäden zu vermeiden.

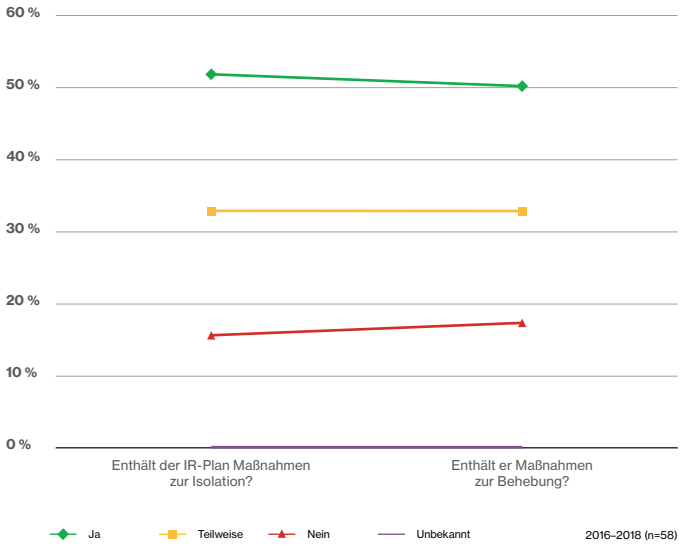
Beobachtungen aus unseren Bewertungen

In 52 % der 2016–2018 bewerteten IR-Pläne wurden die Maßnahmen für die Eindämmung ausführlich beschrieben und in 50 % wurden Maßnahmen für die Behebung aufgelistet. Teilweise Beschreibungen der Maßnahmen für die Eindämmung und Behebung fanden sich in je 33 % der bewerteten Pläne.

Empfehlungen aufgrund unserer Beurteilungen

Definieren Sie Maßnahmen für die Eindämmung und Behebung.

Bewertung von Plänen
Phase 3: Eindämmung und Behebung



Datenerfassung und Analyse

Die Erfassung und Analyse von Beweismaterialien kann wichtige Informationen über einen Sicherheitsvorfall liefern und die effektive Eindämmung und Abwehr, die Behebung von Schwachstellen und die Wiederaufnahme des Geschäftsbetriebs unterstützen.

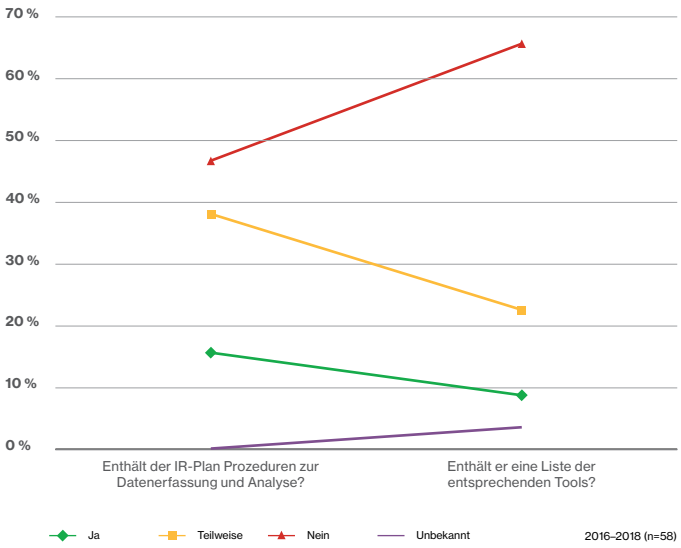
Beobachtungen aus unseren Bewertungen

Nur 16 % der 2016–2018 bewerteten IR-Pläne enthielten eine vollständige Beschreibung der Prozesse für die Datenerfassung und Analyse. Weitere 38 % enthielten eine teilweise Beschreibung. Eine vollständige Liste der zu verwendenden Erfassungs- und Analysetools war nur in 9 % der Pläne enthalten, weitere 22 % enthielten eine unvollständige Liste.

Empfehlungen aufgrund unserer Beurteilungen

Definieren Sie die Tools und Prozeduren für die Datenerfassung und Analyse.

Bewertung von Plänen
Phase 4: Datenerfassung und Analyse



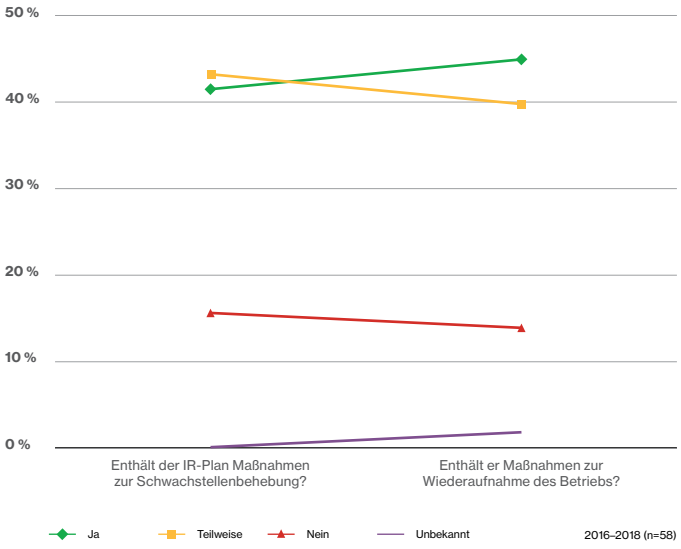
Schwachstellenbehebung und Wiederaufnahme des Betriebs

In dieser Phase werden zwei Ziele verfolgt: Das Beheben der durch den Vorfall aufgedeckten Schwachstellen, damit sie in Zukunft nicht wieder ausgenutzt werden können, und die Wiederaufnahme des normalen Geschäftsbetriebs.

Beobachtungen aus unseren Bewertungen

Nur 41 % der 2016–2018 bewerteten IR-Pläne enthielten eine vollständige Beschreibung der Maßnahmen zur Behebung der aufgedeckten Schwachstellen, weitere 43 % enthielten eine teilweise Beschreibung. Die Maßnahmen zur Wiederaufnahme des Betriebs wurden in 45 % der Pläne vollständig und in weiteren 40 % teilweise beschrieben.

Bewertung von Plänen
Phase 5: Schwachstellenbehebung und Wiederaufnahme des Betriebs



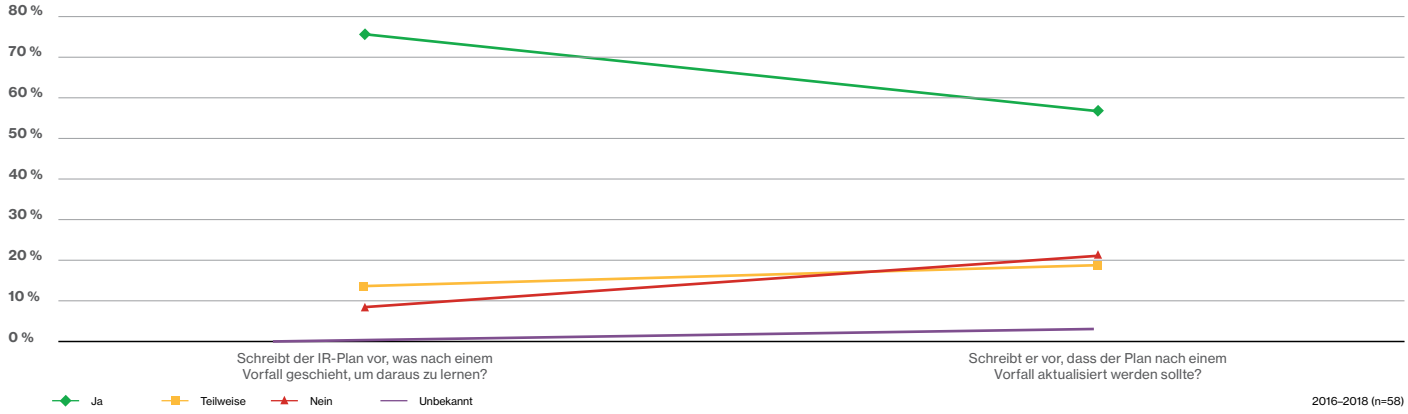
Empfehlungen aufgrund unserer Beurteilungen

Definieren Sie die Prozesse für die Schwachstellenbehebung und die Wiederaufnahme des Betriebs formell.

Bewertung und Anpassung

In der letzten Phase des IR-Prozesses werten Sie Ihre Reaktion rückblickend aus, um systemische Schwächen und Lücken zu identifizieren und zu beheben und die bestehenden Maßnahmen und Prozesse zu verbessern.

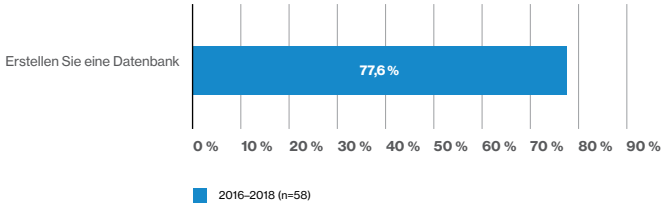
Bewertung von Plänen
Phase 6: Anwendung der gewonnenen Erkenntnisse



Beobachtungen aus unseren Bewertungen

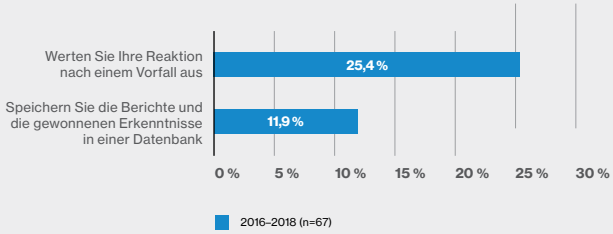
76 % der 2016–2018 bewerteten Pläne enthielten eine vollständige (und 14 % eine teilweise) Beschreibung der nach einem Sicherheitsvorfall durchzuführenden Aktivitäten. Eine Aktualisierung des IR-Plans aufgrund der dabei gewonnenen Erkenntnisse wurde von 60 % unbedingt (und von weiteren 19 % teilweise) vorgeschrieben.

Empfehlungen aufgrund unserer Beurteilungen



für Berichte über Sicherheitsvorfälle, die Reaktion darauf und die daraus gewonnenen Erkenntnisse (78 %).

Empfehlungen für Simulationsübungen



Die im Anschluss an 2016–2018 durchgeführte Simulationsübungen am häufigsten ausgesprochenen Empfehlungen waren, die Reaktion auf Sicherheitsvorfälle auszuwerten (25 %) und die dabei erstellten Berichte und gewonnenen Erkenntnisse in einer Datenbank festzuhalten (12 %).

Fazit

Wir hoffen, dass Sie sich die Zeit nehmen werden, den vollständigen VIPR-Bericht zu lesen, denn dort finden Sie eine Vielzahl von Erkenntnissen, Fakten und Best Practices rund um IR-Pläne. Als kleinen Vorgeschmack und nützliche Referenz haben wir hier die 20 wichtigsten Empfehlungen für den Aufbau effektiver Abwehrfunktionen und die Erstellung eines belastbaren IR-Plans für Sie zusammengestellt:

Phase	Wichtigste Ergebnisse
1 – Planung und Vorbereitung	1. Erstellen Sie einen klaren, effizienten IR-Plan. 2. Erstellen Sie IR-Handbücher für bestimmte Vorfallsszenarien. 3. Überprüfen, testen und aktualisieren Sie Ihren IR-Plan regelmäßig. 4. Verweisen Sie auf externe und interne regulatorische Vorgaben und Standards für die Cyber-Sicherheit und die Reaktion auf Sicherheitsvorfälle. 5. Führen Sie im IR-Plan die Verantwortlichen und deren Verantwortungsbereiche auf. 6. Verlangen Sie von den IR-Verantwortlichen, dass sie die aktuelle Bedrohungslage regelmäßig besprechen. 7. Bilden Sie Mitarbeiter oder Teams für die taktische Reaktion aus und halten Sie deren Fachkenntnisse auf dem neuesten Stand. 8. Überprüfen Sie die Services und die Kontaktdaten Ihrer Serviceanbieter für die Cyber-Sicherheit.
2 – Erkennung und Prüfung von Vorfällen	9. Definieren Sie sicherheitsrelevante Ereignisse (und Vorfälle). 10. Klassifizieren Sie Vorfälle nach Art und Schweregrad. 11. Beschreiben Sie die technischen und nicht-technischen Quellen für die Erkennung von Sicherheitsverstößen. 12. Beschreiben Sie die Mechanismen zur Verfolgung sicherheitsrelevanter Ereignisse und Vorfälle. 13. Beschreiben Sie die Prozesse für die Meldung und Eskalation von Vorfällen.
3 – Eindämmung und Behebung	14. Definieren Sie Maßnahmen für die Eindämmung und Behebung.
4 – Datenerfassung und Analyse	15. Definieren Sie die Tools und Prozeduren für die Datenerfassung und -analyse. 16. Definieren Sie die Prozesse für die Verarbeitung und Weiterleitung von Beweismaterialien.
5 – Schwachstellenbehebung und Wiederaufnahme des Betriebs	17. Definieren Sie die Prozesse für die Schwachstellenbehebung und die Wiederaufnahme des Betriebs.
6 – Bewertung und Anpassung	18. Werten Sie Ihre Reaktion nach einem Vorfall aus, um daraus zu lernen (und aktualisieren Sie den IR-Plan entsprechend). 19. Etablieren Sie Richtlinien für die Aufbewahrung von Daten und Dokumenten. 20. Zeichnen Sie den Vorfallsverlauf und die dazugehörigen Kennzahlen auf.

Verizon Incident Preparedness and Response Report – Kurzfassung

Informationsmaterialien zu Datensicherheitsverletzungen und zur Cyber-Sicherheit im Allgemeinen

https://enterprise.verizon.com/de-de/resources/

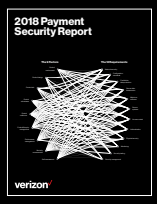
2019 Incident Preparedness and Response Bericht: Schützen Sie Ihr Unternehmen vor Datendiebstahl

Untersuchungsbericht zu Datensicherheitsverstößen 2019

Bericht zu Insider-Bedrohungen 2019: Out of sight should never be out of mind.

Mobile Security Index 2019: It's time to tackle mobile security.

Datensicherheitsverletzungen im Überblick 2018 (18 Szenarien)



Bericht zur Sicherheit von Bezahlvorgängen 2018

Leitfaden Cloud-Sicherheit für CISOs What to know and what to ask before you buy.

5 Punkte, die Sie bei der Bewertung moderner Sicherheitsplattformen für Unternehmen berücksichtigen sollten

Laden Sie den Verizon Incident Preparedness and Response Report herunter
enterprise.verizon.com/de-de/resources/reports/vipr/

verizon