PSR

2021 Payment Security Report insights

PCI DSS v4.0
Whitepaper

Verizon Cyber
Security Consulting

Das neueste Update des Payment Card Industry Data Security Standard (PCI DSS) erleichtert modernen Unternehmen die Ausrichtung ihrer Datensicherheitsmaßnahmen auf eine sich ständig ändernde Bedrohungslandschaft. Doch da es sich hier um die einschneidendste Modifikation des PCI DSS seit seiner ersten Veröffentlichung im Jahr 2004 handelt, bereitet es vielen Verantwortlichen Mühe, die Auswirkungen der neuen Bestimmungen auf ihren Geschäftsbetrieb zu überblicken. Wenn auch Sie nach einer fundierten vereinfachten Darstellung der kommenden Anforderungen suchen, empfehlen wir Ihnen die Lektüre des vorliegenden Verizon Payment Security Report (PSR).

Dieser Bericht basiert auf jahrzehntelanger rigoroser Forschung und eignet sich daher bestens als Leitfaden für zukunftsfähige Sicherheits- und Compliancestrategien in der Kreditkartenbranche. Er ist Teil einer seit 2010 laufenden Reihe, die speziell auf die Bedürfnisse aller relevanten Beteiligten zugeschnitten ist – von der Vorstandsetage über den Sicherheitsausschuss bis hinunter zu den Sicherheits- und Complianceteams spezifischer Unternehmensbereiche.

All diesen Experten bietet der PSR unter anderem Antworten auf die folgenden Fragen rund um die Sicherung von Bezahlsystemen:

- Wie können die Verantwortlichen die richtigen Prioritäten und Arbeitsschwerpunkte setzen?
- Wie sollten sie bei der Wahl ihrer Zielsetzungen vorgehen?
- Wie können sie sich einen Überblick über die neuen Anforderungen verschaffen und eventuelle Hindernisse aus dem Weg räumen?

Wenn das Geschäft läuft, liegt dies üblicherweise daran, dass sich die Angestellten in produktiver Weise engagieren und eine klare Vorstellung von der Strategie ihres Unternehmens haben. Gleiches gilt für Sicherheits- und Complianceinitiativen, die letztlich nur dann erfolgreich sein können, wenn alle Mitarbeiter, Teams und Abteilungen an einem Strang ziehen und auf ein gemeinsames Ziel hinarbeiten.

Deshalb sollten Sie sich fragen: Wie viele Mitarbeiter Ihres Unternehmens haben eine genaue Vorstellung von Ihren aktuellen Zielsetzungen in Sachen Sicherheit und Compliance? Welche Kriterien können Sie anlegen, um eine optimale Nutzung der knappen personellen Ressourcen Ihres Sicherheitsteams sicherzustellen? Treffen Sie im Hinblick auf Ihre Zielsetzungen und Problemlösungsstrategien die richtigen Entscheidungen?

Zugleich können wir Ihnen – trotz aller eventuellen Zweifel – versichern, dass die meisten Unternehmen der erfolgreichen Umsetzung und dauerhaften Einhaltung des PCI-Standards näher sind, als sie glauben. Als entscheidender Faktor erweist sich dabei die Umsetzung der im PSR dargelegten Maßnahmen und Schritte.

So hat der PSR im Laufe von mehr als zehn Jahren bereits zahllosen Unternehmen als praktischer Ratgeber und Wegweiser für die Entwicklung innovativer Sicherheitsprogramme gedient. Denn sein ebenso aussagekräftiges wie praxisrelevantes Framework erleichtert Sicherheitsexperten die Planung und Implementierung sicherer Geschäftsmodelle, robuster Betriebsprozesse und zielführender Strategien.

In dieser Tradition bietet Ihnen die aktuelle Ausgabe nützliche Tipps und Empfehlungen zur Umsetzung von PCI DSS v4.0, der zehnten veröffentlichten Version und bislang umfassendsten Überarbeitung des PCI-Standards. Damit möchten wir Ihnen und Ihrem Unternehmen die Vorbereitung auf die kommenden Anforderungen erleichtern.

Seien Sie sich bewusst, dass die Einführung von PCI DSS v4.0 tiefgreifende Auswirkungen auf Ihre Geschäfts- und Betriebsprozesse haben wird. Deshalb sollten Sie sich unbedingt die nötige Zeit nehmen, um Ihre Zielsetzungen, Strategien, Maßnahmen, Zuständigkeiten, Initiativen und Prozesse auf den neuen Standard auszurichten.

Inhaltsverzeichnis

Die Vorbereitung auf PCI DSS v4.0 3

- Informationen zur Übergangsphase
- Stärkere Datensicherheit durch eine ganzheitliche Strategie
- Die Entwicklung effizienter Kontrolldesigns
- Erweiterte Validierungsverfahren und -prozesse
- Maßgeschneiderter Ansatz und Kompensationskontrollen im Vergleich
- Implikationen des maßgeschneiderten Ansatzes
- Hohe Risiken durch mangelnden Weitblick: Was wir aus der Havarie der Ever Given lernen können

Das Modell der Ziele, Anforderungen und Beschränkungen: Ein Ansatz zur Lösung komplexer Probleme 10

- Die Engpasstheorie und ihre Relevanz im Bereich Zahlungssicherheit
- Verschaffen Sie sich den nötigen Überblick

Empfehlungen und Tipps rund um PCI DSS v4.0 14

- Warum Sie Vorlagen zur Dokumentation von Kontrolldesigns verwenden sollten
- Eine kurze Wiederholung der wichtigsten Punkte

Die Vorbereitung auf PCI DSS v4.0

Übersicht über die verschiedenen Versionen des PCI DSS

PCI DSS v4.0, die zehnte Version des PCI-Standards, wurde im März 2022 veröffentlicht. Das letzte umfassendere Update (Version 3.0) ist bereits neun Jahre alt, während das letzte Zwischenupdate (mit geringfügigen Veränderungen) aus dem Jahr 2018 stammt und damit vier Jahre zurückliegt.

Davor vergingen zwischen Version 2.0 vom Oktober 2010 und der Veröffentlichung von PCI DSS v3.0 im November 2013 lediglich etwas mehr als drei Jahre.

Versionen des PCI DSS

Datum der Veröffentlichung		Version
2004	Dezember	1.0
2006	September	1.1
2008	Oktober	1.2
2009	Juli	1.2.1
2010	Oktober	2.0
2013	November	3.0
2015	April	3.1
2016	April	3.2
2018	Mai	3.2.1
2022	März	v4.0

Verizon dokumentiert im PSR seit mehr als einem Jahrzehnt die vielschichtigen Compliancetrends und technologischen Neuerungen im Bereich Zahlungssicherheit. In diesem Zeitraum haben sich die geschäftlichen Aktivitäten von Verbrauchern und Unternehmen in zunehmendem Maße ins Internet verlagert, wodurch die Zahl der Kreditkartentransaktionen signifikant gestiegen ist. Parallel dazu haben sich die Methoden der Cyberkriminellen weiterentwickelt, sodass die Angreifer nun alte und neue Bedrohungen auf raffinierte Weise miteinander kombinieren und vorhandene Schwachstellen in Zahlungssystemen und -prozessen skrupellos ausnutzen können. Und schließlich kommen im Zuge der digitalen Transformation vermehrt Cloud-Technologien zum Einsatz. All diese Entwicklungen haben direkte Auswirkungen auf die Zahlungssicherheit und bringen zusätzliche Schwierigkeiten für CISOs und andere leitende Sicherheitsexperten mit sich.

Als dringend benötigte Reaktion auf diese Herausforderungen wurde der PCI DSS v4.0 veröffentlicht. Schon auf den ersten Blick ist zu erkennen, dass es sich hier um das einschneidendste und bedeutendste Update des PCI-Standards seit der Veröffentlichung von DSS v1.0 vor 17 Jahren handelt. Zwar werden im PCI DSS v4.0 die fundamentale Struktur der bisherigen Versionen des PCI-Standards und insbesondere die 2006 eingeführten zwölf Hauptanforderungen sowie deren übergeordnete Kontrollziele (Control Objectives) beibehalten. Doch enthält die neue Version eine Vielzahl von Modifikationen, die die Zukunftsfähigkeit der diversen Bestimmungen sichern sollen. Im Einzelnen zählen hierzu zahlreiche Klarstellungen, aktualisierte und neue Anforderungen sowie Anforderungen mit verlängerten Umsetzungsfristen.

In Anbetracht dessen stellt sich die Frage, warum das PCI Council den PCI DSS von Grund auf überarbeitet hat, wo doch bereits Version 3.2 aus dem Jahr 2016 als ziemlich ausgereift galt.

Hier zeigt sich bei genauerer Betrachtung, dass die vorgenommenen Änderungen den tiefgreifenden Umbrüchen in der Kreditkartenbranche und den Risiken einer immer komplexeren, hochdynamischen Bedrohungslandschaft Rechnung tragen. Mit anderen Worten: PCI DSS v4.0 soll den Unternehmen neue Orientierungspunkte bieten und den Verantwortlichen die Implementierung effektiver Kontrollen und Complianceprozesse für moderne IT-Umgebungen erleichtern.

So unterstützt PCI DSS v4.0 speziell den Einsatz von Cloud-Lösungen, serverlosen Umgebungen und anderen Schlüsseltechnologien. Außerdem können Unternehmen, die die PCI-DSS-Anforderungen gegenwärtig mithilfe von Kompensationskontrollen erfüllen, künftig einen genau zu ihren Sicherheitsanforderungen passenden maßgeschneiderten Implementierungsansatz wählen.

Darüber hinaus enthält der aktualisierte Standard flexiblere Formulierungen der PCI-DSS-Anforderungen und erweitert diese um Angaben zum jeweiligen Zweck. Anschaulich wird dies auf den Seiten 6 und 7 dieses Whitepapers, wo wir die beiden wichtigsten Neuerungen in PCI DSS v4.0 beleuchten: kontinuierliche Assessments sowie maßgeschneiderte Kontrollen und Kontrollinfrastrukturen.

Die jüngste Version des PCI-Standards wird als so wichtig betrachtet, dass das Payment Card Industry Security Standards Council (PCI SSC) zwischen 2009 und Mitte 2021 mehr Feedback zum Entwurf von PCI DSS v4.0 eingeholt hat als je zuvor. Während sich die Feedbackoptionen bei früheren Überarbeitungen auf einen festgelegten Zeitrahmen und die am PCI SSC beteiligten Organisationen und Sachverständigen beschränkten, hatte das PCI SSC in diesem Fall die Beteiligungsmöglichkeiten für Partner und Stakeholder maximiert.[1]

1 Siehe PCI Security Standards Council, PCI DSS v4.0: Anticipated Timelines and Latest Updates.
https://blog.pcisecuritystandards.org/pci-dss-v4-0-anticipated-timelines-and-latest-updates
https://www.pcisecuritystandards.org/about_us/press_releases/pr_10242019
https://www.pcisecuritystandards.org/get_involved/request_for_comments

Somit lässt sich zusammenfassend feststellen, dass die Aktualisierung des PCI DSS vor allem auf die folgenden Punkte zielt:

- die Anpassung des Datensicherheitsstandards an die aktuellen und künftigen Anforderungen der Kreditkartenbranche
- mehr Flexibilität durch zusätzliche Umsetzungsmethoden
- die Ausrichtung der Sicherheitsanforderungen auf die Entwicklung neuer Technologien in den Bereichen Bezahlsysteme, mobile Kommunikation, Cloud usw.
- die Bekämpfung neuartiger Bedrohungen, unter anderem durch verbesserte Protokolle und Validierungsmethoden
- die Förderung kontinuierlicher Datensicherheits- und Complianceprozesse

Zu Beginn sollten Sie sich unbedingt die wichtigste Frage stellen:

“ Was muss in unserem Unternehmen zur Vorbereitung auf die Umstellung getan werden?“

Informationen zur Übergangsphase

Zwar bleibt Unternehmen bis zum Inkrafttreten des PCI DSS v4.0 noch etwas Zeit, aber sie wird schneller vergehen, als viele erwarten. Da der Standard bereits im März 2022 veröffentlicht wurde und erst zwei Jahre später in 2024 verbindlich wird, bleibt den Unternehmen eine gewisse Übergangsphase für die Umstellung. Diese Phase begann mit der Veröffentlichung sämtlicher Ressourcen zu PCI DSS v4.0 und erstreckt sich über einen Zeitraum von 18 Monaten, in denen Version 3.2.1 ihre Gültigkeit behält. Erst danach wird PCI DSS v3.2.1 endgültig durch v4.0 abgelöst. Darüber hinaus gewährt der aktualisierte Standard eine verlängerte Umsetzungsfrist für die als „zukünftig“ identifizierten Anforderungen.

In Anbetracht dessen kann bei den Verantwortlichen in den Unternehmen eventuell der falsche Eindruck entstehen, dass ihnen noch reichlich Zeit für die Anpassung der Complianceprozesse und Datensicherheitskontrollen bleibt. Doch wie bei allen großen Änderungen empfiehlt sich auch hier, so früh wie möglich mit der Vorbereitung auf die Erfüllung der neuen Anforderungen – einschließlich des maßgeschneiderten Implementierungsansatzes – zu beginnen.

Stärkere Datensicherheit durch eine ganzheitliche Strategie

Das PCI SSC verfolgt mit der Festlegung verbindlicher Anforderungen seit jeher das Ziel, Unternehmen und Institutionen bei der Umsetzung von Best Practices rund um die Datensicherheit zu unterstützen. Deshalb hält der PCI DSS die Verantwortlichen dazu an, für eine konsistente Implementierung der Bestimmungen zu sorgen und dabei die Abstimmung, Planung, Priorisierung, Realisierung und Weiterentwicklung ihrer Zielsetzungen und Strategien so zu verbessern, dass eine effektive Kontrollinfrastruktur entsteht. Diese Absicht tritt im PCI DSS 4.0 möglicherweise deutlicher zutage, als dies in früheren Versionen des PCI-Standards der Fall war.

Damit tragen die Herausgeber der Tatsache Rechnung, dass viele Unternehmen seit der ersten Version des PCI DSS im Jahr 2004 Schwierigkeiten bei der Implementierung und Aufrechterhaltung der geforderten Maßnahmen zur Sicherung von Kreditkartendaten haben. Die Unternehmen, denen es gelingt, die PCI-DSS-Anforderungen das ganze Jahr über einzuhalten (und die nicht vor jedem der alljährlichen Assessments erneute Korrekturen durchführen müssen), zeichnen sich durch effiziente, auf wohlüberlegten Zielsetzungen basierende Strategien und Designs aus. Das bedeutet: Wenn die Verantwortlichen klare Zielsetzungen formulieren, erleichtert dies die Implementierung maßgeschneiderter Kontroll- und Validierungsdesigns.

Auf der Grundlage dieses Prinzips ist bereits einigen Unternehmen die Umstellung auf sicherheitsorientierte Geschäfts- und Betriebsprozesse gelungen. Zugleich zeigen die Umfrageergebnisse aus dem PSR 2020 „State of Compliance“, dass sich bedauerlicherweise knapp drei Viertel (72,1 %) der teilnehmenden Manager auf das PCI-DSS-Assessment konzentrieren, anstatt wirklich effiziente Kontrollinfrastrukturen aufzubauen. Natürlich können auch effektive Kontrollinfrastrukturen manchmal versagen, doch das wird in der Regel schnell bemerkt und behoben. In den weniger effektiven Kontrollinfrastrukturen der meisten Unternehmen fehlen jedoch die dazu erforderlichen Funktionen.

Daher wird in PCI DSS v4.0 noch stärker als in früheren Versionen betont, wie wichtig der Übergang zu einem sicherheitsorientierten Routinebetrieb und die verstärkte Erfassung von Validierungsinformationen für ununterbrochene Sicherheitsprozesse sind.

Die Entwicklung effizienter Kontrolldesigns

Wo es weder klare Ziele noch eine ambitionierte Strategie für die Datensicherheit gibt, weisen die Sicherheitssysteme zu oft Schwachstellen auf. Aus diesem Grund sollten CISOs und Sicherheitsmanager sich die Zeit nehmen, die spezifischen Anforderungen ihres Unternehmens und geeignete Lösungen zu formulieren, bevor sie mit der Implementierung der neuen Vorgaben beginnen. Jede neue oder aktualisierte Vorgabe sollte sorgfältig geprüft werden, denn Projektmanager benötigen eine klare Vorstellung des Projektumfangs, der Ziele und Einschränkungen, bevor sie mit der Aufgabenverteilung beginnen.

Leider wird die Implementierung durchdachter Datensicherheits- und Compliancelösungen zu oft zu einer zweit- oder gar drittrangigen Überlegung, weil Architekten und Techniker mit Personalmangel und einer Flut von Warnmeldungen zu kämpfen haben. Unter diesen Bedingungen bleibt oft nur die Zuflucht zu jährlichen Complianceprojekten, die schon als Erfolg gelten, wenn sich ihre hastig durchgeführten Maßnahmen zur Behebung von Mängeln in der angestrebten Weise im PCI-DSS-Konformitätsbericht niederschlagen. Dabei ist klar, dass ein solcher Ansatz den eigentlichen Zweck des PCI DSS verfehlt.

Zusätzliche Validierungs-verfahren und -prozesse

Zu den wichtigsten Änderungen im PCI DSS v4.0 zählen überarbeitete Vorgaben für die Validierungsmethoden und -prozesse. Neben dem bekannten definierten Ansatz kann nun auch ein zielorientierter, maßgeschneiderter Ansatz verwendet werden. Damit setzt das PCI SSC einen Plan um, der bereits 2019 bei verschiedenen Communitymeetings vorgestellt wurde.

Davor gab es einzig den altbekannten definierten Ansatz, bei dem alle einschlägigen Sicherheitskontrollen in einer vorgeschriebenen Form implementiert werden müssen. Zwar bleibt diese traditionelle Methode der PCI-DSS-Validierung auch in Version 4.0 erhalten, sodass sich die Verantwortlichen auch weiterhin für ein Verfahren mit sehr konkreten Anforderungen und Prüfprozessen entscheiden können. Doch hat diese Variante in einigen Fällen den Nachteil, dass das zertifizierte Kontrollsystem nicht notwendigerweise effektiv und effizient ist. Deshalb gibt es nun zusätzlich die Möglichkeit zur Wahl des neuen maßgeschneiderten (auch: kundenspezifischen) Ansatzes, der ein Abweichen von den konventionellen PCI-DSS-Anforderungen erlaubt, sofern die gewählte Alternative nachweislich den Zweck der fraglichen Bestimmungen und das Effektivitätskriterium erfüllt.

Die Verantwortlichen können nun also für jeden PCI-DSS-Bewertungsprozess den konventionellen oder den neuen Validierungsansatz oder sogar eine Kombination aus beiden wählen. So erlaubt der PCI DSS v4.0 unter anderem eine hybride Vorgehensweise, bei der die Unternehmen die Umsetzung bestimmter Anforderungen auf der Basis des definierten Ansatzes nachweisen und in Bezug auf andere Anforderungen dem maßgeschneiderten Ansatz folgen. Darüber hinaus besteht sogar die Möglichkeit, die Realisierung der verschiedenen Aspekte eines bestimmten Kriteriums teils auf Basis des definierten Ansatzes, teils anhand des maßgeschneiderten Ansatzes zu belegen, sofern das betreffende Unternehmen die Sicherheitsziele der fraglichen Anforderung erfüllt. Allerdings ist in diesem Zusammenhang zu beachten, dass einige Anforderungen explizit von der Validierung mithilfe des maßgeschneiderten Ansatzes ausgeschlossen sind.

Maßge-schneiderter Ansatz und Kompensations-kontrollen im Vergleich

Der definierte Ansatz

Diese Bezeichnung bezieht sich auf den klassischen, seit der Einführung des PCI-Standards möglichen Ansatz für die Implementierung von Sicherheitskontrollen und der Compliancеprüfung. Als Grundlage dienen hier relativ strikte Vorschriften hinsichtlich der Anforderungen, Kontrollen und Testprozesse. Daher enthält der PCI-Standard genaue Beschreibungen der unternehmensseitig zu implementierenden Kontrollen sowie der Kriterien, die bei ihrer Validierung anzulegen sind.

Wenn sich die Verantwortlichen für den definierten Ansatz entscheiden, wählen sie damit die bereits in früheren Versionen des PCI DSS schriftlich festgelegten Anforderungen und Testprozesse. Dieser Ansatz behält auch in Version 4.0 seine Gültigkeit, sodass die Unternehmen weiterhin die Möglichkeit haben, von detaillierten Vorschriften zur Umsetzung der formulierten Ziele zu profitieren. In Anbetracht dessen werden viele Entscheidungsträger zu dem Schluss kommen, dass ein Umschwenken auf einen maßgeschneiderten Ansatz nicht erforderlich ist.

Der maßgeschneiderte Ansatz

Der maßgeschneiderte (auch: kundenspezifische oder benutzerdefinierte) Ansatz erlaubt es einem Unternehmen, das erklärte Ziel bestimmter Anforderungen mithilfe eigener Sicherheitsmaßnahmen zu erfüllen, selbst wenn diese nicht in der Liste definierter Kontrollen aufgeführt sind. Dadurch wird der klassische, auf strikten Detailvorschriften basierende Ansatz der PCI-DSS-Validierung um eine zielorientierte Variante der Compliancеprüfung erweitert. Allerdings ist dies – wie bereits erwähnt – nur unter der Voraussetzung möglich, dass alle maßgeschneiderten Kontrollen den expliziten Zielsetzungen der jeweiligen Anforderungen genügen.

Ein maßgeschneiderter Ansatz bedeutet meist einen erhöhten Dokumentationsaufwand. Denn für eine zügige Entscheidung benötigen die Prüfer genaue Informationen über die:

- Kontrolldesigns, einschließlich stichhaltiger Belege der Eignung für die relevanten Kontrollziele und Zwecke
- Testprozesse, denen die Kontrollen unternehmensintern unterzogen werden
- Risiken, die durch die Kontrollen eingedämmt werden sollen
- Performance der Kontrollen
- Effektivität der Kontrollen
- Wartung und Pflege der Kontrollen
- Compliancetests und Validierungsprozesse für eine Zertifizierung

Generell soll durch die Neugestaltung der Anforderungen und Validierungsoptionen in PCI DSS v4.0 zum einen der Fokus auf konkrete Sicherheitsziele geschärft, zum anderen das Spektrum der möglichen Methoden zur Umsetzung des PCI-Standards erweitert werden. Deshalb enthalten die Vorgaben für Unternehmen nun Angaben zum Zweck der einzelnen Anforderungen sowie eine genaue Darstellung der Ergebnisse, die bei einer maßgeschneiderten Implementierung erzielt werden müssen. Das verschafft den Verantwortlichen mehr Klarheit und eröffnet ihnen darüber hinaus erweiterte Handlungsspielräume zur Realisierung der gewünschten Resultate.

Außerdem kann der PCI DSS dank des flexiblen maßgeschneiderten Ansatzes die Nutzung neuer Sicherheitslösungen und Technologien unterstützen, ohne dass er jedes Mal angepasst werden muss. Hier erweist es sich als entscheidender Vorteil, dass die Validierungsverfahren nun stärker auf spezifische Ergebnisse fokussiert sind und den Unternehmen so die Möglichkeit eröffnen, die Effektivität ihrer bevorzugten Sicherheitsmaßnahmen vor diesem Hintergrund zu belegen.

Zugleich ist zu beachten, dass diese Alternative nur dann für die Entwicklung und Einrichtung eigener Designs und Sicherheitskontrollen zur Verfügung steht, wenn die folgenden Voraussetzungen erfüllt sind:

- Die zum Erreichen eines bestimmten Sicherheitsziels erforderlichen Kontrollen sind genau definiert.
- Der gewählte Complianceansatz wird im Detail dokumentiert, seine Effektivität stichhaltig demonstriert und die entsprechende Dokumentation dem Qualifizierten Sicherheitsprüfer (Qualified Security Assessor, QSA) vorgelegt.
- Der QSA analysiert diese Dokumente und entscheidet dann, ob die Kontrollen als effektiv anerkannt werden.

Implikationen des maßgeschneiderten Ansatzes

Design und Umsetzung maßgeschneiderter Sicherheitskontrollen erfordern ein strukturiertes Vorgehen, das in gut messbaren und genau vorhersehbaren Ergebnissen mündet. Infolgedessen sind Unternehmen mit einer ausgereiften Kontrollinfrastruktur mit höherer Wahrscheinlichkeit in der Lage, die Vorteile des neuen maßgeschneiderten Ansatzes in vollem Umfang zu nutzen. Unter anderem sollte es diesen Firmen vergleichsweise leichter fallen, bestehende Test- und Prüfprozesse so umzugestalten, dass sich damit die Umsetzung der neuesten PCI-DSS-Anforderungen belegen lässt.

Zugleich ist absehbar, dass die neue Validierungsmethode zumindest anfänglich einen gewissen Mehraufwand bedeutet, da die Verantwortlichen neben der erforderlichen Dokumentation auch das eigentliche Kontrolldesign erstellen sowie Evaluationen und Risikodaten für den QSA vorbereiten müssen.

Und obwohl der neue Ansatz den Unternehmen mehr Freiräume bei der Umsetzung der 12 Hauptvorgaben des PCI DSS lässt, wird ausdrücklich erwartet, dass jede maßgeschneiderte Implementierung sowohl die Vorgaben als auch die Ziele des Standards im vollen Umfang umsetzt.

Infolgedessen erfordert jede Variante des maßgeschneiderten Ansatzes robuste Methoden für Design und Management der gewünschten Sicherheitskontrollen und die Wartung und Pflege der Kontrollinfrastruktur. Darüber hinaus benötigen die Verantwortlichen leistungsstarke Prozesse und ausgereifte Funktionen zur Erstellung und Umsetzung des Kontrolldesigns, zur Bewertung der relevanten Risiken sowie zur Implementierung und Überwachung der vorgesehenen Kontrollen.

Fehlen diese Voraussetzungen, so wird dem betreffenden Unternehmen im Vorfeld einer maßgeschneiderten PCI-DSS-Implementierung die schrittweise Anhebung des Reifegrads der entsprechenden Funktionen und Prozesse empfohlen. Auf diese Weise können die dortigen Entscheidungsträger mögliche unbeabsichtigte Folgen durch umfassende Modifikationen ihrer Kontrollinfrastruktur vermeiden.

Des Weiteren sind die Unternehmen angehalten, bei der Vereinbarung und Entwicklung maßgeschneiderter Testprozesse eng mit dem QSA oder dem Internen Sicherheitsprüfer (Internal Security Assessor, ISA) zusammenzuarbeiten. Zudem müssen sich die Verantwortlichen gegen mögliche unbeabsichtigte Folgen der Implementierung maßgeschneiderter Kontrollen wappnen und sollten daher umfassend über die toten Winkel ihrer Sicherheitsprozesse sowie die Wechselbeziehungen zwischen Kontrollen, Kontrollsystemen und Kontrollumgebung informiert sein.

All dies macht deutlich, dass die zielorientierte Entwicklung und Implementierung eigener Kontrollmechanismen neue Risiken mit sich bringt. Die zuständigen Manager müssen sich dessen – und der größeren Verantwortung, die sie mit einem solchen Ansatz übernehmen – bewusst sein. Sie sollten ermitteln, ob ihr Unternehmen über sämtliche Fähigkeiten und Kompetenzen verfügt, die für die Entwicklung, Implementierung, Pflege und Überwachung maßgeschneiderter Kontrollen und die Umsetzung aller zwölf Schlüsselanforderungen erforderlich sind. In Anbetracht dieser umfangreichen Voraussetzungen ist der neue Ansatz möglicherweise nicht für alle Firmen, sondern vorrangig für Unternehmen mit ausgereiften Security, Compliance und Risk Assessment Processes geeignet.

Ein Überblick über die einschlägigen Reifegrade und Kennzahlen findet sich im Verizon Payment Security Report 2019 (S. 21 bis 29).

Was sind unbeabsichtigte Folgen?

Der Begriff „unbeabsichtigte Folge“ bzw. „unvorhergesehene Folge“ stammt vom US-amerikanischen Soziologen Robert K. Merton und bezeichnet einen ungewollten oder unerwarteten Effekt zweckgerichteten Handelns. Im Einzelnen unterscheidet der Autor in seinem Grundlagenwerk „The Unintended Consequences of Purposive Social Action“ drei verschiedene Arten unbeabsichtigter Folgen:

- **Unerwartete positive Effekte**, die manchmal auch als unverhoffter Gewinn oder Serendipität bezeichnet werden
- **Unerwartete negative Effekte**, die gewissermaßen als Nebenwirkung eines erwarteten positiven Effekts auftreten
- **Perverse Effekte** , d. h. ein negatives Ergebnis ohne die ursprünglich angestrebten positiven Effekte oder Vorteile[2]

2 „Unbeabsichtigte Folgen“, Wikipedia. https://de.wikipedia.org/wiki/Unbeabsichtigte_Folgen

Hohe Risiken durch mangelnden Weitblick: Was wir aus der Havarie der Ever Given lernen können

Die unbeabsichtigten Folgen der Implementierung eines neuen Sicherheitsdesigns werden hinsichtlich ihrer Gefährlichkeit allzu leicht unterschätzt – ungeachtet der Tatsache, dass schon minimale Änderungen an komplexen Systeme weitreichende unvorhergesehene Konsequenzen haben können. Doch auch wenn sich die Verantwortlichen von Anfang an um ein klares Bild der zu erwartenden Auswirkungen bemühen, werden entsprechende Prognosen häufig durch komplexe Wechselbeziehungen und Abhängigkeiten erschwert. Daher lassen sich unbeabsichtigte potenzielle Beeinträchtigungen der Zahlungssicherheit nur auf der Basis eines umfassenden, gut durchdachten Designansatzes vermeiden. Das gilt insbesondere dann, wenn die Verantwortlichen den maßgeschneiderten Implementierungsansatz wählen und die Umstellung auf PCI DSS v4.0 parallel zur Einführung von 5G, kontaktlosen Zahlungsprozessen, Blockchain-Lösungen, künstlicher Intelligenz und maschinellem Lernen vorantreiben.

Ein eindrückliches Beispiel für die fatalen Folgen einer mangelnden Voraussicht bei Design und strategischer Planung war die Blockade des Suezkanals durch das havarierte Containerschiff Ever Given im März 2021. Hier führte die Verkettung mehrerer unglücklicher Umstände zu einer Katastrophe, die die Ever Given für mehr als sechs Tage festsetzte:

1 **Containerschiffe sind heute mindestens doppelt so groß (und breit) wie 2000, doch die Schifffahrtsbranche und die Suezkanal-Behörde haben nur beschränkt durch Regulierungen oder Zusammenarbeit auf diese Entwicklung reagiert.[3]**

2 **Im Gegensatz zu anderen Teilen des Kanals wurde der enge Abschnitt, in dem die Ever Given – eines der längsten Containerschiffe der Welt – in Querlage geriet und steckenblieb, beim Suezkanal-Projekt von 2015 nicht erweitert.**

3 **Aus der Hydrodynamik ist bekannt, dass ein breites Containerschiff in einem flachen, engen Kanal Gefahr läuft, durch den sogenannten „Bank Effect" ans Ufer gedrückt zu werden und an Manövrierfähigkeit zu verlieren.[4] Am Havarietag trugen zudem starker Wind und schlechte Sicht aufgrund eines Sandsturms dazu bei, dass das Schiff außer Kontrolle geriet.**

> **„Die besten Pläne von Mäusen und Menschen schlagen oft fehl."**
>
> —Robert Burns[5]

Um solche Unglücksfälle zu vermeiden, sollten CISOs und Sicherheitsmanager unbedingt das sogenannte „Vorsorgeprinzip"[6] befolgen. Dieses fordert vorbeugende Maßnahmen zur Vermeidung potenzieller Gefahren und wird von politischen Entscheidungsträgern vor allem dann genutzt, wenn noch keine definitiven Angaben bezüglich Art, Ausmaß oder Eintrittswahrscheinlichkeit möglicher Schadensfälle vorliegen.

„Das Vorsorgeprinzip zwingt uns dazu, viele schwierige Fragen bezüglich der Art der Risiken, der Unsicherheit, der Eintrittswahrscheinlichkeit, der Rolle der Regierung und der ethischen Aspekte zu stellen. Außerdem kann es uns dazu veranlassen, unsere Intuitionen hinsichtlich der richtigen Entscheidungen in bestimmten Situation zu hinterfragen", heißt es in einem auf der Website von Farnam Street veröffentlichten Blogbeitrag.[7] Derartige Überlegungen können Unternehmen dabei helfen, das Risiko kostspieliger Datenschutzverletzungen schon bei der Planung anstehender Änderungen zu minimieren.

3 „The Impact of Mega-Ships", The Organisation for Economic Co-operation and Development (OECD), International Transport Forum, 2015. https://www.itf-oecd.org/sites/default/files/docs/15cspa_mega-ships.pdf

4 Marc Vantorre et al., „Maneuvering in Shallow and Confined Water", Encyclopedia of Maritime and Offshore Engineering, abgerufen am 20. April 2017. https://doi.org/10.1002/9781118476406.emoe006

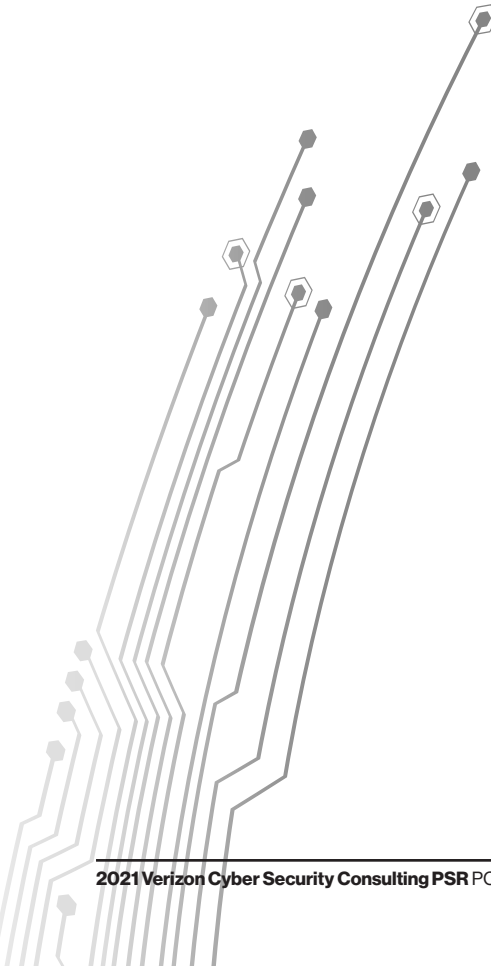
5 „To a Mouse", Wikipedia. https://en.wikipedia.org/wiki/To_a_Mouse

6 „Vorsorgeprinzip", Wikipedia. https://de.wikipedia.org/wiki/Vorsorgeprinzip

7 „The Precautionary Principle: Better Safe than Sorry?" Farnam Street, Juni 2021. fs.blog/2021/06/precautionary-principle

Das Modell der Ziele, Anforderungen und Beschränkungen: Ein Ansatz zur Lösung komplexer Probleme

Eine fundierte Strategie und ein zuverlässiges Geschäftsmodell sind zwei zentrale Voraussetzungen für ein effizientes Kontrolldesign. Vor allem aber benötigen CISOs und Sicherheitsmanager insbesondere seit der Veröffentlichung des PCI DSS v4.0 und der Einführung maßgeschneiderter Implementierungsoptionen ein detailliertes Verständnis jeder einzelnen Standardvorgabe, ihrer Zielsetzungen und Einschränkungen sowie des Aufwands für ihre Umsetzung. In Anbetracht dessen hat Verizon das sogenannte Modell der Ziele, Anforderungen und Engpässe als Verfahren zur Erstellung effizienter maßgeschneiderter Sicherheitsdesigns entwickelt. Dieses Modell wird im PSR 2022 ausführlich beschrieben.



Angewandtes logisches Denken

Die Mehrzahl der von Unternehmen entworfenen und implementierten Kontrollinfrastrukturen könnten sowohl effektiver als auch effizienter sein. Das wirft die Frage auf, ob es nicht besser wäre, wenn die Verantwortlichen bei der Erstellung und Umsetzung entsprechender Strategien bewährten Methoden oder Verfahren folgten. Fakt ist: Einige der erfolgreichsten Produkte und effizientesten Prozesse sind auf diese Weise entstanden. Zahnärzte arbeiten eine Reihe festgelegter Schritte ab, wenn sie eine Füllung einsetzen. Bautrupps verdichten zunächst den Untergrund und errichten ein Fundament, bevor sie mit dem Bau eines Hauses beginnen. Warum also sollten Sicherheitsexperten beim Design von Kontrollsystemen nicht auch eine bewährte Methode anwenden? Die Antwort ist: weil viele Unternehmen keine strukturierte Methode zur Formulierung und Umsetzung klarer Zielsetzungen haben. Letztlich lassen sich Modernisierungsprozesse nur durch angewandtes logisches Denken in inkrementelle Schritte mit vorhersehbaren Konsequenzen gliedern.

Die schlagzeilenträchtige Havarie der Ever Given verdeutlicht auf einprägsame Weise, welche drastischen Folgen mangelnder Weitblick und das Auseinanderfallen von strategischen Zielen, regulatorischen Vorgaben und bestehenden Beschränkungen haben können. Daher sollten Sicherheitsmanager unbedingt unser auf drei Säulen basierendes Modell anwenden, um Fehler im Designprozess zu verhindern.

So können sie möglicherweise vermeiden, zu einem späteren Zeitpunkt mit dem QSA über substantielle Maßnahmen zur ordnungsgemäßen Umsetzung einer Anforderung aus dem PCI DSS diskutieren zu müssen. Derartige Diskussionen entstehen häufig, weil ein QSA üblicherweise zunächst den aktuellen Zustand der Kontrollinfrastruktur analysiert und diesen dann vor dem Hintergrund der getroffenen (oder unterlassenen) Entscheidungen und Maßnahmen der Unternehmensführung betrachtet. Dabei kommen unweigerlich auch die Sicherheits- und Complianceziele des Unternehmens zur Sprache. In den meisten Fällen kommt der Prüfer dabei zu dem Schluss, dass bei der Einrichtung und Verwaltung der Kontrollinfrastruktur zu wenig auf Ziele, Anforderungen und Beschränkungen geachtet wurde, und fällt ein negatives Urteil.

In solchen Fällen ist die mangelnde Eignung einer Kontrolle für einen bestimmten Zweck oft auf eine Kombination aus Schwächen im Design und mangelhaften Implementierungs- und Wartungsprozessen zurückzuführen. Abgesehen davon sollten Sie stets im Gedächtnis behalten, dass jede PCI-DSS-Kontrolle immer Teil eines übergeordneten Kontrollsystems ist und dementsprechend dessen Funktionstüchtigkeit beeinträchtigen kann. So treten zahlreiche Mängel und Fehlfunktionen vor allem deshalb auf, weil das Zusammenspiel von abhängigen oder in Wechselwirkung stehenden Kontrollen vor der Implementierung nicht ausreichend geprüft wurde. Zusätzlich kann die Effektivität einer Kontrolle leiden, wenn ihre Betriebsprozesse nicht in ausreichendem Maße durch eine effiziente Kontrollinfrastruktur unterstützt werden.

Was sind Zielsetzungen?

In Zielsetzungen werden die angestrebten Ergebnisse und die Mission des Unternehmens in Form von Kennzahlen und messbaren Erfolgen formuliert. Das gilt auch für die wichtigsten Ziele im Bereich Sicherheit und Compliance, deren Verwirklichung (oder Verfehlung) sowohl in der Implementierungsphase als auch im laufenden Betrieb jederzeit anhand quantitativer Indikatoren klar erkennbar sein sollte.

Darüber hinaus können die Verantwortlichen dem Arbeitsalltag ihrer Angestellten durch eine klare Kommunikation der festgelegten Ziele sowohl Sinn als auch Richtung verleihen. Denn klare Vorgaben ermöglichen klare Zuständigkeiten und dienen sämtlichen Teammitgliedern als Orientierungspunkte für den eigenen Verantwortungsbereich. So entsteht ein solides Fundament für die gemeinsame Arbeit an der Umsetzung der formulierten Ziele.

In Bezug auf die Implementierung des neuen PCI DSS bedeutet das:

- Eindeutige Vorgaben in den Bereichen Sicherheit und Compliance erleichtern die Konzentration auf zielführende Aktivitäten.
- Die klare Kommunikation der Zielsetzungen motiviert die Mitarbeiter und steigert ihr Engagement.
- Feste Ziele regen die Mitarbeiter dazu an, ihr bestehendes Wissen zum Einsatz zu bringen oder sich erforderliche Kenntnisse anzueignen.
- Regelmäßige Erinnerungen fördern das kontinuierliche Hinarbeiten auf ehrgeizige Ziele.

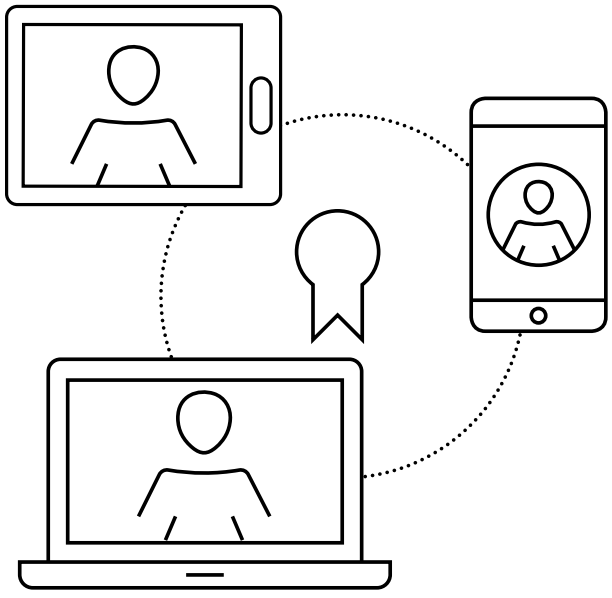
Stellen Sie sich die folgenden Fragen:

- Welche Ziele wurden in Sachen Datensicherheit und Compliance unternehmensintern vereinbart und kommuniziert?
- Würden die Mitglieder der vier Sicherungslinien (siehe PSR 2019, S. 12) dieselben Ziele nennen, wenn man sie danach fragte?
- Welcher Prozentsatz der implementierten PCI-DSS-Kontrollen ist tatsächlich und nachweisbar effektiv und effizient?
- In welchem Umfang ist der Erfolg der Datensicherheitsmaßnahmen auf ein fundiertes Design (statt auf bloßes Glück) zurückzuführen?

Die kausale Beziehung zwischen dem Fehlen klar definierter Ziele und Mängeln in Sachen Compliance, Effizienz und Effektivität sollte offensichtlich sein, ist vielen Verantwortlichen aber dennoch nicht bewusst. Aber es ist schlicht unwahrscheinlich, dass Unternehmen Ziele erreichen, die sie sich nicht gesetzt haben. Nur in sehr wenigen Unternehmen gehören effiziente, langfristig wirksame Sicherheitskontrollen zu den explizit formulierten Zielen für die Kontrollumgebung. Wie es scheint, orientiert sich derzeit lediglich eine Minderheit an der oft in unseren Publikationen geäußerten Empfehlung, beim Aufbau berechenbarer, konsistenter und dauerhaft zuverlässiger Kontrollinfrastrukturen auf ein fundiertes Design statt auf bloßes Glück zu vertrauen.

Fakt ist: Werden keine detaillierten Zielsetzungen festgelegt, treten die für Sicherheit und Compliance zuständigen Teams auf der Stelle, weil sie nicht die nötigen Mittel erhalten und keine überzeugenden Ergebnisse vorzuweisen haben.

Dies gilt ungeachtet der Tatsache, dass CISOs und Sicherheitsteams oft sehr stark ausgelastet sind. Wie Verizon bereits im PSR 2020 ausführlich berichtete, entstehen im alltäglichen Betrieb immer wieder drängende akute Herausforderungen, deren Bewältigung eine höhere Priorität eingeräumt wird als der Zukunftsplanung und der sorgfältigen Prüfung der bestehenden Prozesse. Trotzdem sind präzise Datensicherheits- und Complianceziele sowie eine klare Zukunftsvision letztlich unerlässlich – insbesondere für die Teams und Mitarbeiter, die zu den Mitgliedern der vier Sicherungslinien zählen und für die Kontrollumgebung zuständig sind oder deren Sicherheit beeinflussen können.



Die Engpass-theorie und ihre Relevanz im Bereich Zahlungs-sicherheit

Bei der sogenannten Engpasstheorie (Theory of Constraints, TOC) handelt es sich um eine bewährte Methode für das Prozessmanagement. Damit lassen sich zum einen die wichtigsten Hindernisse, Störfaktoren und Einschränkungen auf dem Weg zu einer effizienten Kontrollinfrastruktur und zur Realisierung der gewünschten Zielsetzungen identifizieren. Zum anderen gibt sie den Verantwortlichen strukturierte Verfahren zur Beseitigung der ermittelten Hürden an die Hand.

Mit anderen Worten: Die Engpasstheorie geht von der Annahme aus, dass es in jedem steuerbaren System eine überschaubare Anzahl von Nadelöhren gibt, die das Erreichen seiner Ziele gefährden. Darauf aufbauend nutzt sie einen wissenschaftlichen Ansatz zur zielorientierten Optimierung dieser Systeme. Deshalb beschreibt ihr Schöpfer, der Autor Eliyahu M. Goldratt, die Engpasstheorie als „Prozess der fortgesetzten Verbesserung" bzw. als Denkansatz zur Entwicklung einfacher Lösungen für komplexe Probleme.[8]

Da die Theorie grundsätzlich auf jedes System anwendbar ist, kann sie auch in den Bereichen PCI-Compliance und Datensicherheit eingesetzt werden. Hier ermöglicht die TOC zunächst das Identifizieren des Engpasses, der das reibungslose Zusammenspiel der verschiedenen Abläufe in der Kontrollinfrastruktur behindert – ganz gleich, ob es sich dabei um einen Prozess, eine bestimmte Abteilung oder gar die Unternehmensleitung handelt. Anschließend unterstützt sie die zielorientierte Verbesserung dieses schwächsten Gliedes, damit es das Gesamtsystem nicht länger ausbremst. Das hat zur Folge, dass nun ein anderer Teil des Systems oder eine externe Größe zum wichtigsten Engpass wird (der dann eventuell in einem weiteren Schritt beseitigt werden kann). Auf diese Weise lassen sich kontinuierlich jene Beschränkungen eliminieren, die einen effektiven und wirtschaftlichen Betrieb der Kontrollinfrastruktur verhindern.

Verschaffen Sie sich den nötigen Überblick

Damit erweist sich die TOC erstens als ausgeklügelte Methode zur Priorisierung von Optimierungsmaßnahmen, zur Analyse komplexer Systeme und zur Prüfung und Korrektur bislang nicht hinterfragter Annahmen. Das hilft Ihnen dabei, jeden Schritt und Ablauf innerhalb bestimmter Prozesse oder Bereiche sehr genau zu untersuchen. Zugleich nehmen Sie ganz von selbst eine holistische Perspektive ein, da Sie dazu angehalten werden, Ihr gesamtes Unternehmen als Kette von Abteilungen und Funktionsbereichen zu betrachten.

Zweitens trägt die Theorie der Tatsache Rechnung, dass moderne Unternehmen höchst dynamische Strukturen mit vielfältigen Prozessen sind. Sie erfahren, wo Ihre Optimierungsmaßnahmen den größten Effekt auf die Umsetzung Ihrer Ziele haben, und können diese mit mehreren nur in der TOC verfügbaren Tools auf strukturierte und konsistente Weise umsetzen, ohne Ihr Budget zu sprengen oder Ihre wichtigsten Zielsetzungen aus dem Blick zu verlieren.

So können Sie immer wieder aufs Neue dafür sorgen, dass Ihre Optimierungsinitiativen dort ansetzen, wo sie die größte Wirkung entfalten. Außerdem erhalten Sie die volle Kontrolle über Ihre Prozesse und einen umfassenden Überblick über ungenutzte Kapazitäten, die Ihnen ohne zusätzliche Investitionen zur Verfügung stehen. Kurz: Die TOC hält Sie dazu an, zunächst Ihre bestehende Infrastruktur bestmöglich zu nutzen, bevor Sie in zusätzliche Geräte oder Ressourcen investieren. Damit ist sie genau die Lösung, die viele Unternehmen zur Verbesserung ihrer PCI-Complianceprozesse benötigen. (Ausführliche Details zur Optimierung von Sicherheitsprogrammen mithilfe der Engpasstheorie finden Sie im PSR 2022.)

8 Eliyahu M. Goldratt, „What is this thing called Theory of Constraints and how should it be implemented?" The North River Press, 1999.

Die Engpasstheorie erleichtert die Beantwortung der folgenden Fragen:

- Warum ist eine Änderung nötig? (Was ist das Ziel?)
- Was sollten wir ändern? (Wo liegt das Problem und was ist dessen Ursache?)
- Welcher Effekt wird angestrebt? (Wie sieht die Lösung des Problems aus?)
- Wie lässt sich der angestrebte Wandel herbeiführen? (Wie gelingt die Implementierung?)

Damit unterstützt sie die Verantwortlichen in Ihrem Unternehmen bei der:

- Klärung der relevanten Zielsetzungen und dazu passenden Anforderungen
- Bestimmung der kritischen Erfolgsfaktoren, von denen die Realisierung der Zielsetzungen abhängt (jeweils drei bis fünf Faktoren pro Ziel)
- Darstellung der Spielräume und Bedingungen für die Realisierung der systemspezifischen Zielsetzungen
- Identifizierung der Voraussetzungen für die Implementierung jedes wichtigen Erfolgsfaktors[9]

Voraussetzung hierfür ist die strikte Unterscheidung zwischen notwendigen und hinreichenden Voraussetzungen. Denn erst auf dieser Grundlage lässt sich nachvollziehen und erklären, wie die verschiedenen PCI-DSS-Sicherheitskontrollen einander und andere, nicht im PCI DSS enthaltene Sicherheitsmaßnahmen beeinflussen und zusammenwirken, um den erforderlichen Grad an Effektivität und Effizienz zu erzielen. Dieser Aspekt erlangt besondere Bedeutung, wenn sich die Verantwortlichen eines Unternehmens für ein maßgeschneidertes Kontrolldesign und den maßgeschneiderten Validierungsansatz entscheiden.

9 H. William Dettmer, „The Logical Thinking Process: A Systems Approach to Complex Problem Solving", American Society for Quality Press, 2007.

Empfehlungen und Tipps rund um PCI DSS v4.0

1. Handeln Sie jetzt

Ihr Unternehmen sollte die Vorbereitung auf PCI DSS v4.0 umgehend in Angriff nehmen, obwohl der neue Standard noch nicht in Kraft getreten ist. Das gilt auch für Unternehmen, die die Vorgängerversion (PCI DSS v3.2.1) bereits in vollem Umfang umsetzen.

2. Schaffen Sie eine gute Ausgangsbasis – setzen Sie PCI DSS v3.2.1 um

Wenn Sie PCI DSS 3.2.1 noch nicht in vollem Umfang umsetzen, sollten Sie dies jetzt tun, um die kommende Umstellung aus einer Position der Stärke anzugehen. Ermitteln Sie hierfür zunächst, inwiefern Ihre Infrastruktur und Prozesse zur Erfassung und Verarbeitung von Karteninhaberdaten (Card Holder Data, CHD) den aktuell geltenden Anforderungen des definierten Ansatzes genügen und wie es um die Zuverlässigkeit und Widerstandsfähigkeit Ihrer Kontrollsysteme bestellt ist. Danach sollten Sie Ihre Prozesse zur raschen Identifizierung und Behebung fehlerhafter Kontrollmechanismen optimieren. Prüfen Sie dabei jeweils genau, ob die angegebenen Zielsetzungen der einschlägigen Anforderungen genau erfüllt sind.

3. Verschaffen Sie sich einen Überblick über sämtliche Anforderungen des PCI DSS v4.0

Machen Sie sich sorgfältig mit allen Anforderungen des PCI DSS v4.0 vertraut, um einen detaillierten Überblick über sämtliche neuen, geänderten, neu nummerierten oder aus dem Standard entfernten Kontrollen sowie über alle Kontrollen mit verlängerten Umsetzungsfristen zu erlangen. Dabei sollten Sie auch sicherstellen, dass Sie die Kontrollziele und den Zweck jeder Anforderung im Kontext des gesamten PCI DSS nachvollziehen können. Die gravierendsten Auswirkungen ergeben sich aus den Änderungen der Schlüsselanforderungen 12, 11, 10 und 8. (Die Reihenfolge spiegelt den Umfang der erwarteten Konsequenzen wider.)

4. Wählen Sie Ihre Kontrolldesigns- und Validierungsoptionen sorgfältig aus

Wenn Sie sich für den maßgeschneiderten Ansatz entscheiden, kommt in der Anfangsphase eventuell mehr Aufwand auf Sie zu, weil Sie die Compliancеprüfung Ihrer Sicherheitskontrollen entsprechend vorbereiten müssen. Zusätzlich ergibt sich potenziell ein erhöhtes Risiko bei der Implementierung der Kontrollen, das jedoch in vielen Fällen dadurch aufgewogen wird, dass Ihr Unternehmen eine robuste, zukunftsfähige Kontrollinfrastruktur erhält, die – im Unterschied zu einem definierten Ansatz mit Kompensationskontrollen – keine schriftliche Begründung unter Verweis auf geschäftliche oder technische Einschränkungen erfordert. (Die Messung der Effektivität implementierter Kontrollen wird im PSR 2018 auf den Seiten 23 und 41 anhand von Beispielen erläutert.) Des Weiteren ist in diesem Zusammenhang zu beachten, dass für jede maßgeschneiderte Kontrolle (genau wie für definierte Kontrollen) ein Nachweis der dauerhaften Effektivität und der langfristigen Eignung zur unterbrechungsfreien Umsetzung eines bestimmten Kontrollziels erforderlich ist.

5. Wählen Sie den maßgeschneiderte Ansatz erst nach sorgfältiger Erwägung

Falls Sie den maßgeschneiderten Ansatz für bestimmte Teile ihrer Kontrollinfrastruktur in Erwägung ziehen, sollten Sie unbedingt auf den damit verbundenen Arbeitsaufwand vorbereitet sein. Zum einen müssen Sie in der Designphase sicherstellen, dass die vorgeschlagenen Kontrollen in der vorgesehenen Umgebung das nötige Maß an Effektivität und Effizienz erreichen. Zum anderen benötigen Sie stichhaltige schriftliche Belege dafür, dass Ihre Alternativen zur Verwirklichung der relevanten Zielsetzungen geeignet sind. Seien Sie sich also der Tatsache bewusst, dass jede individuelle Anpassung Ihrer Kontrollinfrastruktur eine solide Struktur und umfassende Dokumentation erfordert. Außerdem benötigen Sie einen kompetenten Mitarbeiter, der vor jeder externen Validierung eine interne Eignungs- und Funktionsprüfung der betreffenden Kontrollen vornimmt.

6. Nutzen Sie Vorlagen zur Dokumentation Ihrer Kontrolldesigns

Dass die Prüfung der Effektivität implementierter Kontrollen ein wichtiger Bestandteil regelmäßiger Compliance-Assessments ist, sollte unmittelbar einleuchten. Als Grundlage hierfür müssen die Verantwortlichen für jedes Kontrolldesign eine eigene Dokumentation erstellen, was jedoch schnell zu einem zeitraubenden Unterfangen wird, wenn der Prozess nicht hinreichend strukturiert ist. Daher zählt die Entwicklung und konsistente Verwendung einer Vorlage zur Erstellung eines standardisierten Designprofils für jede erforderliche Sicherheitskontrolle bzw. jedes Kontrollsystem zu den empfohlenen Best Practices – insbesondere für Unternehmen, die sich für den maßgeschneiderten Implementierungsansatz entscheiden. (Weitere Informationen zu diesem Thema finden Sie auf Seite 16 unter der Überschrift „Warum Sie Vorlagen zur Dokumentation von Kontrolldesigns verwenden sollten“.)

7. Lassen Sie Ihre Kontrolldesigns frühzeitig validieren

Kontrolldesigns sollten im Rahmen des Entwicklungsprozesses so früh wie möglich an die zuständigen Prüfer (ISAs und QSAs) weitergeleitet werden, damit sie bezüglich ihrer Eignung zur Erfüllung der relevanten Anforderungen und Sicherheitszielsetzungen beurteilt werden können. So können Sie vermeiden, dass sich die Zertifizierung maßgeschneiderter Kontrolldesigns verzögert, weil ihre Struktur und Funktion oder die vorgesehenen Betriebs-, Wartungs- und Prüfprozesse nicht wie erforderlich dokumentiert wurden.

8. Bereiten Sie sich auf kontinuierliche Prüfungen vor

Formulieren Sie in Zusammenarbeit mit Ihrem Sicherheitsteam konkrete Anforderungen bezüglich der kontinuierlichen Weiterentwicklung, Pflege und Prüfung Ihrer Designs. Dafür ist zunächst einmal eine fundierte Kapazitätsplanung und das durchgängige Engagement der entsprechenden Mitarbeiter nötig. Außerdem müssen Routineprozesse für die interne Erfassung und Aufbewahrung von PCI-DSS-Compliancenachweisen eingerichtet werden.

Warum Sie Vorlagen zur Dokumentation von Kontrolldesigns verwenden sollten

Vorlagen erleichtern die Optimierung implementierter Kontrollsysteme beträchtlich und sorgen außerdem für mehr Transparenz und Konsistenz bei Einrichtung, Betrieb und Wartung. Dadurch ermöglichen sie unter anderem die frühzeitige Identifizierung von Schwächen und Problemen in neuen und bestehenden Kontrolldesigns. Außerdem tragen sie nicht nur zur Effektivität und Härtung der gesamten Kontrollumgebung bei, sondern bieten auch den erforderlichen Überblick über den Zweck, die Funktion und die betrieblichen Beschränkungen der einzelnen Komponenten.

Aus all diesen Gründen sollten Sie für jedes Kontrollsystem ein PCI-DSS-Profil erstellen, das die folgenden 12 Punkte abdeckt:

1. **Kontrollziele**
   Aufstellung der Kontrollziele, die im Hinblick auf die betreffende Kontrolle bzw. das betreffende Kontrollsystem relevant sind

2. **Eigentümer**
   Informationen zu den Verantwortlichen und ihren Zuständigkeiten und Pflichten

3. **Funktion**
   Beschreibung der Funktion der Kontrolle, bspw. Management, betrieblich oder technisch

4. **Typ**
   Zuordnung der Kontrolle zu einer Kategorie, wie etwa Prävention, Erkennung, Korrektur oder Richtliniendurchsetzung

5. **Architektur**
   Definition der Kontrollarchitektur, beispielsweise durch ihre Kennzeichnung als systemspezifisch, gängig oder hybrid

6. **Maßgebliche Risiken**
   Darstellung der Risiken, die durch die Kontrolle gemindert werden – beispielsweise auf Basis der Kontroll/Risiko-Matrix

7. **Eignungsprüfung**
   Beschreibung der vorgesehenen Testprozesse und -standards oder Verweis auf entsprechende Quellen

8. **Implementierung**
   Angaben zu Umfang, Struktur und Abhängigkeiten des Einrichtungsprozesses – unter Bezugnahme auf die primären PCI-DSS-Kontrollen und alle davon abhängigen Kontrollen

9. **Betrieb**
   Spezifikation der Betriebsprozesse der Kontrolle, Dokumentation ihrer Abhängigkeiten von unterstützenden Abläufen und Angabe der Support-Anforderungen sowie der Auswirkungen der verschiedenen Komponenten auf Mitarbeiter, Systeme, Prozesse und Drittunternehmen

10. **Pflege und Wartung**
    Angaben zur Pflege und Wartung der Kontrolle sowie zum Umfang der Wartungsprozesse

11. **Leistungskennzahlen**
    Auflistung von KPIs und anderen Kennzahlen, die laut PCI DSS zur Messung der Leistung der vorgesehenen Kontrolle genutzt werden können

12. **Governance**
    Verweise auf einschlägige Richtlinien, Standards, Frameworks und Bestimmungen[10]

10 Weitere Details zur Dokumentation von Kontrollprofilen finden sich im Payment Security Report, Verizon, 2018, S. 12. https://enterprise.verizon.com/resources/reports/2018/2018_payment_security_report_en_xg.pdf

2021 Verizon Cyber Security Consulting PSR
PCI DSS v4.0: Einblicke

Veröffentlicht am
4. November 2021

Redaktionsteam:

Leitender Autor
Ciske van Oosten

Co-Autorin
Cynthia B. Hanson

Redaktionsleitung
Cynthia B. Hanson

Beitragende
Abdelkrim Aoued Ahmed Bacha, Claire Lavelle, John Galt, Michelle Wire, Mikhail Banguerski, Sean Sweeney

Beratung für Zahlungssicherheit:

Managing Director (Security) Verizon Cyber Security Consulting
Kristof Philipsen

Global Lead
Sam Junkin

Nord- und Südamerika
Matthew Arntsten

Region APAC
Ferdinand Delos Santos

Region EMEA
Loic Breat

Global Intelligence
Ciske van Oosten

Team-E-Mail:
paymentsecurity@verizon.com

Die Erstellung und Pflege entsprechender Kontrollprofile kann sich positiv auf die Effektivität der einzelnen Kontrollen und der Kontrollumgebung insgesamt auswirken. Denn ein klares Design und eine detaillierte Dokumentation der Betriebsprozesse bilden ein solides Fundament für die Formulierung von Leistungserwartungen, die Identifizierung designbedingter Leistungsgrenzen und eine Auflistung der Administrations- und Wartungsanforderungen der wichtigsten Kontrollen. Sind solche Unterlagen dagegen nicht vorhanden, fehlen Sicherheits- und Complianceteams oft die nötigen Orientierungspunkte für die frühzeitige Identifizierung und rasche Behebung von Abweichungen, die eine spätere Zertifizierung verhindern können. Generell gilt die Faustregel: Je detailreicher das Kontrollprofil, desto effektiver ist die geplante Kontrolle und desto berechenbarer ihre Leistung.

Damit leisten Vorlagen zur strukturierten Dokumentation von Kontrolldesigns einen wichtigen Beitrag zum Erfolg des Zertifizierungsprozesses und zur Aufrechterhaltung einer konsistenten, zuverlässigen und reaktionsschnellen Kontrollinfrastruktur.

Eine kurze Wiederholung der wichtigsten Punkte

Der PCI DSS spezifiziert ein Set von wechselseitig abhängigen Kontrollen, die jeweils genau an die Kontrollumgebung des betreffenden Unternehmens angepasst werden müssen, damit sie das angestrebte Maß an Effektivität und Effizienz erreichen können. Deshalb erfordert die Entwicklung und Implementierung von Kontrolldesigns eine systematische Methode. Ohne ein solches Verfahren hängt der Wirkungsgrad der eingerichteten Kontrollen vor allem vom Engagement der zuständigen Mitarbeiter oder Teams ab und lässt sich nicht vor dem Hintergrund präziser Effektivitäts- und Effizienzvorgaben messen.

Besonders häufig bleiben unter diesen Bedingungen Lücken offen, wo mehrere Kontrollen zusammenwirken müssen. Dieses Problem ist so wichtig, dass es immer wieder aufs Neue in den Vordergrund gerückt werden muss, und resultiert vor allem aus der Tatsache, dass zahlreiche Unternehmen vorgefertigte PCI-DSS-Kontrollen implementieren. Viele Verantwortliche gehen einfach davon aus, dass einmal eingerichtete Kontrollen dauerhaft funktionieren und nicht weiter angepasst werden müssen. Deshalb werden vorbereitende Eignungsprüfungen von Kontrolldesigns und Prozesse zur Unterstützung ihres effizienten Betriebs oft erst dann etabliert, wenn akute Schwierigkeiten auftreten.

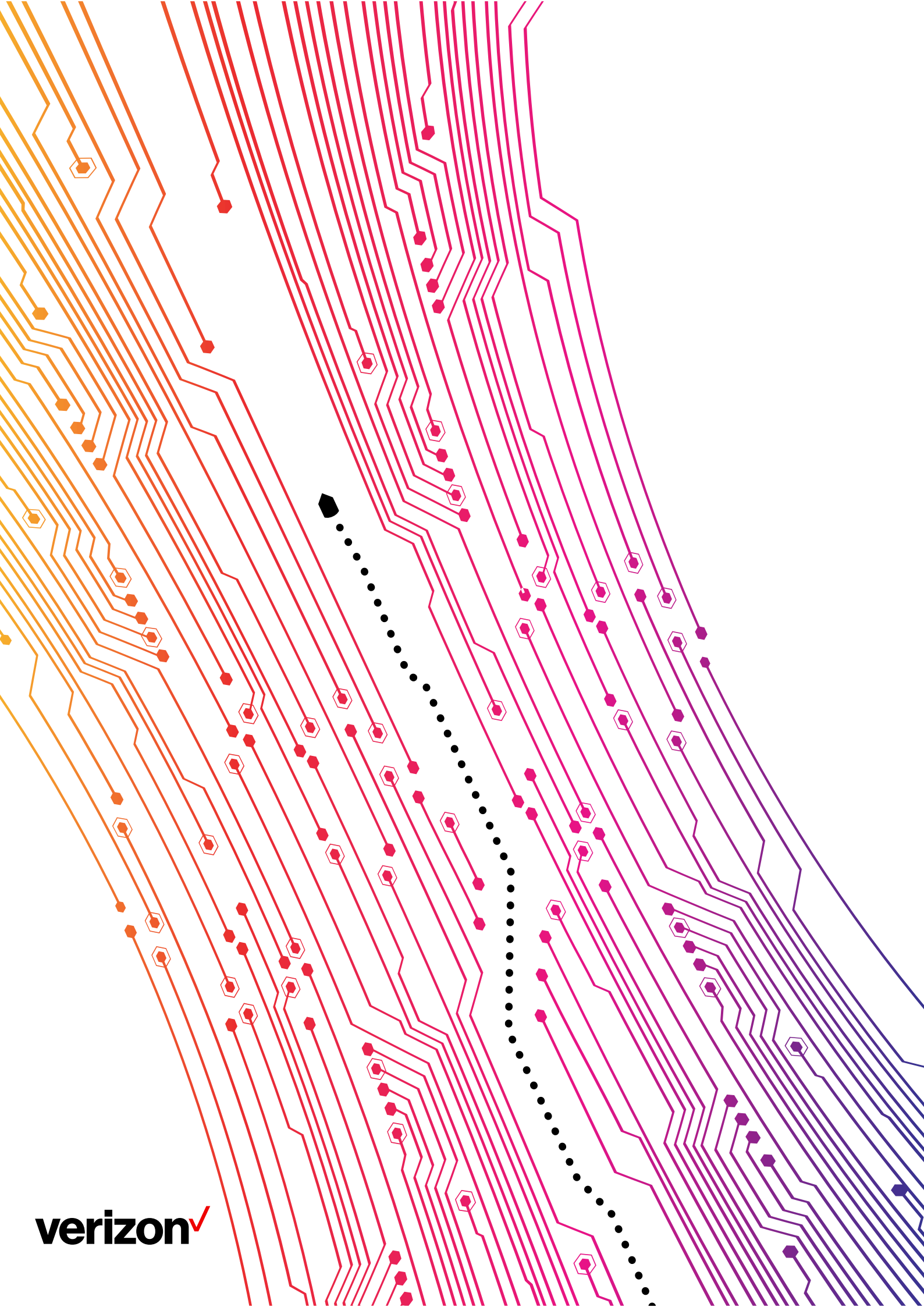
QSAs stellen bei ihren Assessments ein ums andere Mal mit Erstaunen fest, dass die zuständigen Teams und Experten Designfehler und betriebliche Defizite in ihren Sicherheitsprozessen nicht behoben haben, obwohl sie von deren Existenz wissen. Auch viele Manager betrachten beständige niedrigschwellige Kontroll- und Compliancedefizite als akzeptabel, selbst wenn diese mit geringem Aufwand vermieden werden könnten.

Weitere Ausgaben des Payment Security Report sowie diverse dazugehörige Ressourcen finden Sie unter: verizon.com/paymentsecurityreport

Über Verizon Cyber Security Consulting

Dieses Whitepaper wurde von Verizon Cyber Security Consulting herausgegeben, einem globalen Vorreiter im PCI-Sektor mit einem Sicherheitsteam von über 600 Beratern, die in 30 Ländern aktiv sind. Verizon beschäftigt eines der weltweit größten Teams aus PCI Qualified Security Assessors und bietet seit 2002 erstklassige PCI-Services, die sich über die Jahre bewährt haben. Unser Angebot umfasst PCI- und SWIFT-Beratung, Assessments und Services zur Verbesserung der Programmreife.

Verizon unterstützt Kunden dabei, Cyberbedrohungen zu identifizieren, rechtzeitig zu erkennen, effektiv darauf zu reagieren, nach einem Vorfall ihre Systeme wiederherzustellen und gleichzeitig entsprechende Richtlinien und Standards zu erfüllen.


verizon