Datenschutz: Ihre 9 Schritte zum Erfolg

Um Ihre Daten erfolgreich zu schützen, müssen Sie die potenziellen Risiken verstehen, denen Ihre Daten ausgesetzt sind. Und Sie müssen wissen, wie im Ernstfall zu reagieren ist.

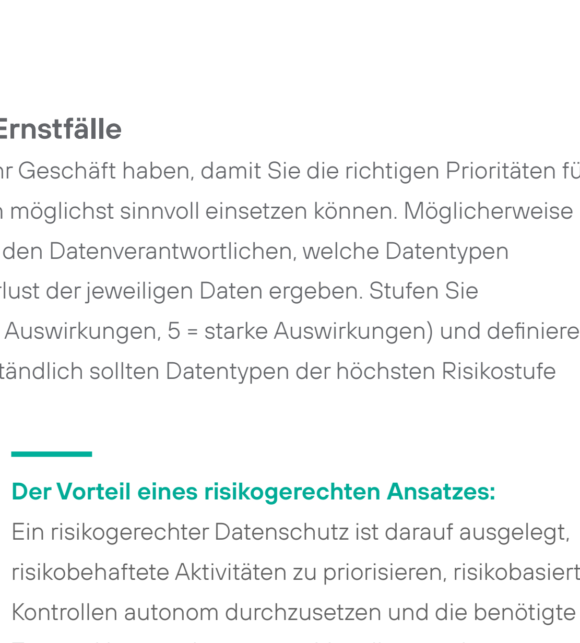
Wie aber bringen Sie nun effizientes Arbeiten und effektiven Datenschutz in Einklang?

Wir haben 9 Schritte zur Umsetzung von Datenschutzmaßnahmen für Sie zusammengestellt, die sich nahtlos in Ihren Arbeitsalltag integrieren lassen und messbare Erfolge liefern, und zeigen Möglichkeiten auf, wie Sie Ihre Lösung mit risikogerechtem Datenschutz ausstatten.

1

Erstellen Sie ein Informationsrisikoprofil

Mithilfe eines Risikoprofils lässt sich leichter verstehen, was Ihre Datenschutzlösung leisten muss. Definieren Sie zunächst die Risiken, die Sie reduzieren möchten, und listen Sie die jeweils betroffenen Datentypen auf. Sie können die Risiken auch nach Datentyp gruppieren. Anschließend definieren Sie die Netzwerke, Endpunkte und Cloud-Kanäle, über die diese Daten potenziell verloren gehen könnten, und listen die derzeit verwendeten Schutzmaßnahmen in diesen Bereichen auf.



2

Entwerfen Sie Aktionsszenarien für verschiedene Ernstfälle

Überlegen Sie, welche Bedeutung die einzelnen Datentypen für Ihr Geschäft haben, damit Sie die richtigen Prioritäten für die Reaktion im Ernstfall festlegen und Ihre Sicherheitsressourcen möglichst sinnvoll einsetzen können. Möglicherweise ist das für Ihr Unternehmen gar nicht so einfach. Besprechen Sie mit den Datenverantwortlichen, welche Datentypen geschützt werden müssen und welche Risiken sich durch den Verlust der jeweiligen Daten ergeben. Stufen Sie anschließend das Risiko auf einer Skala von 1 bis 5 ein (1 = geringe Auswirkungen, 5 = starke Auswirkungen) und definieren Sie für jede Risikostufe angemessene Reaktionszeiten. Selbstverständlich sollten Datentypen der höchsten Risikostufe zuerst gesichert werden.

Der Vorteil eines risikogerechten Ansatzes:
Ein risikogerechter Datenschutz ist darauf ausgelegt, risikobehaftete Aktivitäten zu priorisieren, risikobasierte Kontrollen autonom durchzusetzen und die benötigte Zeit zur Untersuchung eines Vorfalls zu verkürzen.

3

Definieren Sie Reaktionen auf Datenvorfälle pro Kanal und Schweregrad

Wer in Sachen Datenschutz keine bösen Überraschungen erleben möchte, muss bereits im Voraus wissen, wie in verschiedenen Situationen reagiert werden soll. Notieren Sie alle Kanäle in Ihrem Netzwerk, an Ihren Endpunkten und in der Cloud, über die Daten übermittelt werden. Legen Sie anschließend angemessene Reaktionen auf Vorfälle unterschiedlicher Schweregrade vor und berücksichtigen Sie dabei die Gegebenheiten des jeweiligen Kanals.

Der Vorteil eines risikogerechten Ansatzes:
Eine risikogerechte Lösung berücksichtigt die Risikostufe jedes Benutzers, der mit Ihren Daten interagiert. Dies ermöglicht Ihnen, Ihre Reaktionen auf Vorfälle an das individuelle Risiko anzupassen. Wenn Sie beispielsweise für Benutzer mit geringem Risiko die Reaktion „Nur prüfen“ und ausschließlich für Benutzer mit hohem Risiko die Reaktion „Sperren“ festlegen, kann Ihr Team effizient arbeiten, ohne dass die Datensicherheit oder die Benutzerproduktivität gefährdet werden.

Kanäle	Stufe 1 Niedrig	Stufe 2* Niedrig/Mittel	Stufe 3 Mittel	Stufe 4* Mittel/Hoch	Stufe 5* Hoch	Anmerkungen
E-Mail	Verschlüsseln	E-Mail-Anlagen löschen	In Quarantäne stellen	In Quarantäne stellen	Sperren	Verschlüsselung
Web	Prüfen	Prüfen/ Benachrichtigen	Sperren/ Benachrichtigen	Sperren/ Warnen		Proxy für Sperren
Sicheres Web						SSL-Inspektion
FTP						Proxy für Sperren
Netzwerkdrucker						
Benutzerdefiniert						DLP-Drucker-Agent installieren
Cloud-Anwendungen			Mit Hinweis in Quarantäne stellen	In Quarantäne stellen		

* Zusätzliche Granularität durch risikogerechten Datenschutz möglich

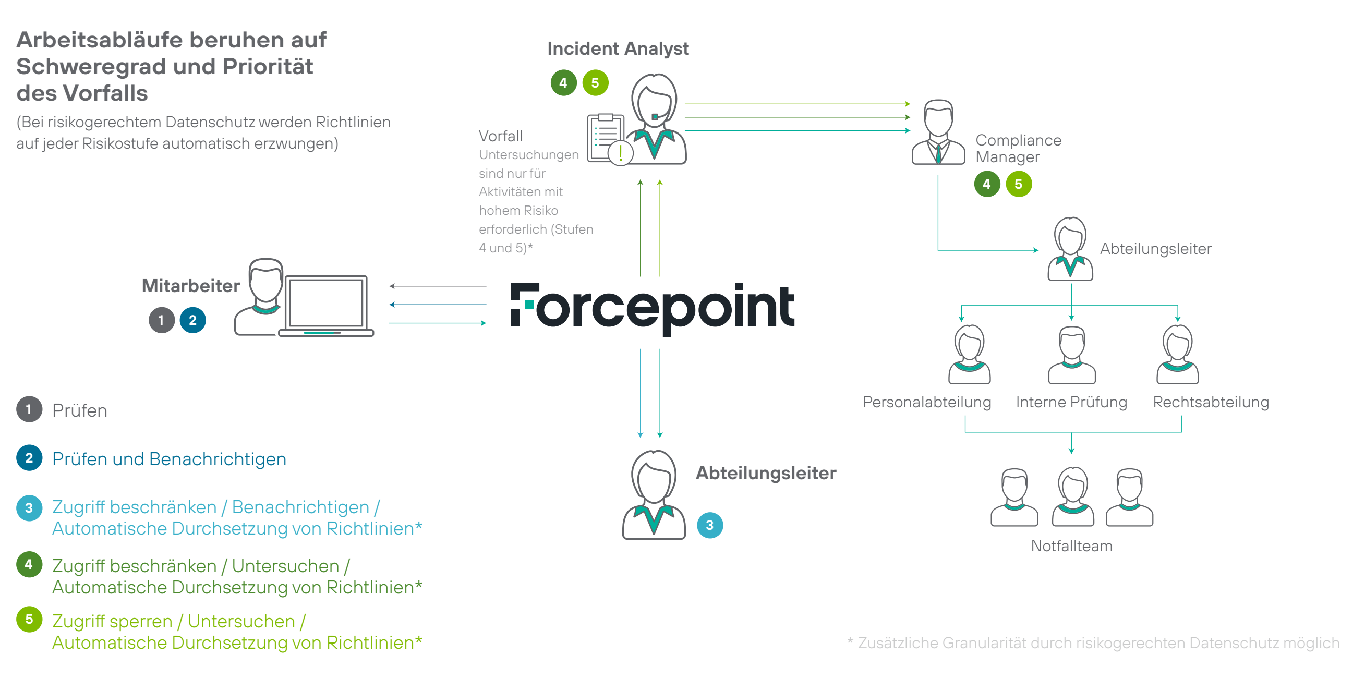
4

Definieren Sie einen Workflow zur Reaktion auf Vorfälle

Sorgen Sie dafür, dass Ihre Sicherheitsteams sofort zur Tat schreiten können, sobald ein Vorfall erkannt wird, indem Sie die Workflows für Vorfälle aller Schweregrade klar definieren. Die Reaktion auf Vorfälle mit geringfügigen Auswirkungen sollte möglichst automatisiert erfolgen. Sie sparen damit Bandbreite, die für die Problembehebung schwerwiegenderer Vorfälle benötigt wird.

Der Vorteil eines risikogerechten Ansatzes:
Eine risikogerechte Lösung ermöglicht die Analyse von Vorfällen basierend auf der individuellen Risikostufe. Sie müssen also keinen Incident Analyst benennen, der über die beste Vorgehensweise entscheidet. Vorfälle, die durch Personen mit geringem Risiko ausgelöst werden, sind wahrscheinlich nicht geschäftsschädigend. Wenn Sie hier etwas gelassener reagieren (und zusätzliche Schutzmaßnahmen wie Verschlüsselung für Dateiübertragungen über USB-Medien oder Löschen von E-Mail-Anhängen einrichten), können Ihre Mitarbeiter weiterhin produktiv arbeiten.

Administratoren können bei Personen und Vorfällen mit hohem Risiko ebenfalls proaktiv vorgehen und bestimmte Aktionen automatisch sperren oder einschränken, bis ein Incident Analyst die Angelegenheit genauer untersucht.



* Zusätzliche Granularität durch risikogerechten Datenschutz möglich

5

Weisen Sie Rollen und Verantwortlichkeiten zu

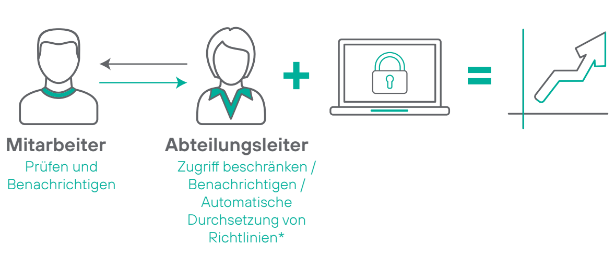
Erhöhen Sie die Stabilität, Skalierbarkeit und betriebliche Effizienz Ihres Datenschutzprogramms, indem Sie Ihren Mitarbeiten klare Aufgabenbereiche zuteilen. Benennen Sie technische Administratoren, Incident Analysts, forensische Ermittler und Prüfer und erteilen Sie entsprechende Berechtigungen und Zugriffsrechte.

6

Beginnen Sie Ihr Projekt im Überwachungsmodus

Sobald Ihre Datenschutz-Netzwerklösung eingerichtet ist, können Sie während einer Überwachungsphase Muster Ihrer Aktivitäten erkennen und Ausgangswerte etablieren, die als Maßstab für normales Nutzerverhalten gelten. Analysieren Sie nach Abschluss dieser Phase das beobachtete Verhalten und besprechen Sie die Ergebnisse mit der Geschäftsleitung. Unterbreiten Sie bei dieser Gelegenheit auch gleich Empfehlungen für Maßnahmen zur Risikoreduzierung. Setzen Sie diese Empfehlungen anschließend um, überwachen Sie den Erfolg und legen Sie Ihre Beobachtungen erneut der Geschäftsleitung vor.

Der Vorteil eines risikogerechten Ansatzes:
Durch die Analyse von Vorfällen im „Nur prüfen“-Modus (im Gegensatz zum abgestuften Durchsetzungsmodus) verdeutlicht eine risikogerechte Lösung die geringere Anzahl von Vorfällen, die eine Untersuchung erfordern, ohne dass Ihre Daten gefährdet werden. Darüber hinaus werden mehr Vorfälle korrekt eingeordnet und Ressourcen werden nicht unnötig durch Falschmeldungen überlastet.



7

Setzen Sie Datenschutz proaktiv um

Nutzen Sie die in der Überwachungsphase gewonnenen Erkenntnisse, um Ihren Reaktionsplan entschlossen umzusetzen und Vorfälle mit hohem Risiko zu sperren. Während Sie die Datenschutzlösung für Endpunkte und genehmigte Cloud-Anwendungen implementieren, überwachen und analysieren Sie Ihre Daten, tragen sie der Geschäftsleitung vor, optimieren die Abläufe und legen die Ergebnisse erneut der Geschäftsleitung vor.

8

Integrieren Sie Datenschutzmaßnahmen unternehmensweit

Legen Sie den Fokus stets auf Effizienz, wenn Sie die Verantwortung an Sicherheitsverantwortliche übertragen. Datenverantwortliche haften bereits im Fall eines Datenverlusts. Indem Sie sie zu Incident Managern ernennen, können sie besser verstehen, wie Daten von anderen Nutzern verwendet werden, und Risiken leichter einschätzen. So wird unnötiges Hin und Her vermieden.

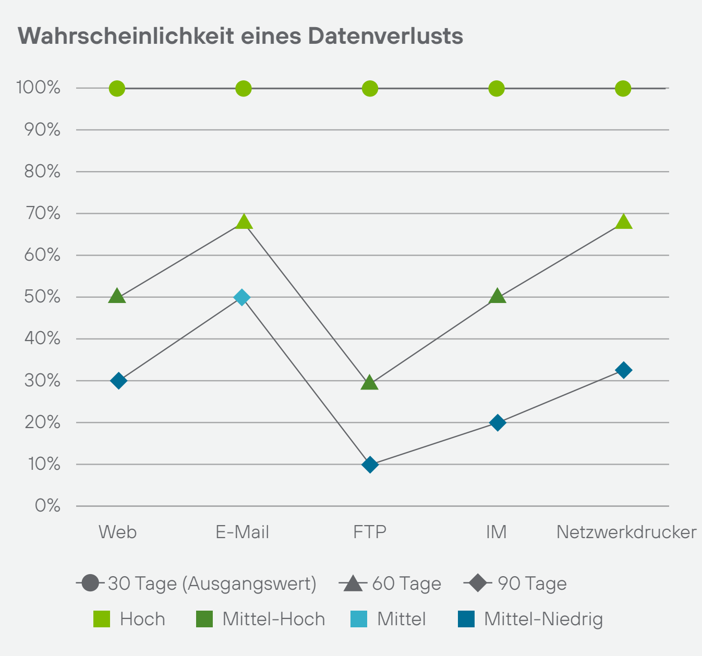
Nun wird es Zeit, die Verantwortung abzugeben: In einem Kickoff-Meeting erläutert das Sicherheitsteam anderen Mitarbeitern die neuen Datenschutzmaßnahmen. Neue Teammitglieder sollten besonders geschult werden. Legen Sie anschließend einen Zeitraum fest, in dem Sie noch Unterstützung bei der Reaktion auf Vorfälle leisten, bis alle Mitarbeiter mit den Prozessen vertraut sind. Auch Echtzeit-Coachings können sinnvoll sein, um die Abläufe zu verinnerlichen.

9

Messen Sie den Erfolg der Risikoreduzierung

Die Vorbereitungen haben Sie bereits in Schritt 6 getroffen. Nun müssen Sie nur noch zusammengehörige Vorfälle nach Kriterien wie Schweregrad, Kanal, Datentyp und Regulierung gruppieren. Legen Sie anschließend gleich lange Zeiträume für die Überwachung und die Risikoreduzierung fest (für den Anfang empfiehlt sich eine Dauer von 2 Wochen), damit Ihre Ergebnisse nicht verfälscht werden.

Wahrscheinlichkeit eines Datenverlusts



Number of Incidents over 90 Days

Vorfälle	Email	Web	FTP	IM	Netzwerkdrucker
30 Tage (Ausgangswert)	150	200	50	10	45
60 Tage	100	100	15	5	30
Risikoreduzierung nach 60 Tagen	33%	50%	70%	50%	33%
90 Tage	76	60	5	2	15
Risikoreduzierung nach 90 Tagen	49%	70%	90%	80%	67%

Ziele

60 Tage
Reduzierung um 25 % oder mehr

90 Tage
Reduzierung um 50 % oder mehr

Der Vorteil eines risikogerechten Ansatzes:
Bei Verwendung eines risikogerechten Ansatzes sollten Sie einen Vergleich der im Modus „Nur prüfen“ erfassten Vorfälle (alle Vorfälle) mit den Vorfällen mit abgestufter Durchsetzung erstellen. In der Zusammenfassung sollte die Anzahl der Vorfälle für jede Risikostufe 1–5 gegenüber den tatsächlich zu untersuchenden Vorfällen (Risikostufen 4–5) ersichtlich sein.

Diese bewährte Formel wird Sie zuverlässig zum Erfolg führen – sowohl mit einem herkömmlichen Ansatz als auch mit risikogerechtem Datenschutz.

Möchten Sie risikogerechten Schutz in Aktion sehen?

Zur Demo

Über Forcepoint
Forcepoint ist einer der weltweit führenden Anbieter von Cyber-Sicherheit im Bereich Anwender- und Datenschutz und hat es sich zur Aufgabe gemacht, Organisationen zu schützen und gleichzeitig die digitale Transformation und das Wachstum voranzutreiben. Die verhaltensbasierten Lösungen von Forcepoint passen sich in Echtzeit an das Nutzerverhalten an und ermöglichen Mitarbeitern einen sicheren Datenzugriff bei voller Produktivität. Forcepoint mit Sitz in Austin, Texas, schafft sichere, vertrauenswürdige Umgebungen für Tausende von Kunden weltweit. [23MAR2020]