SOLUTION BRIEF

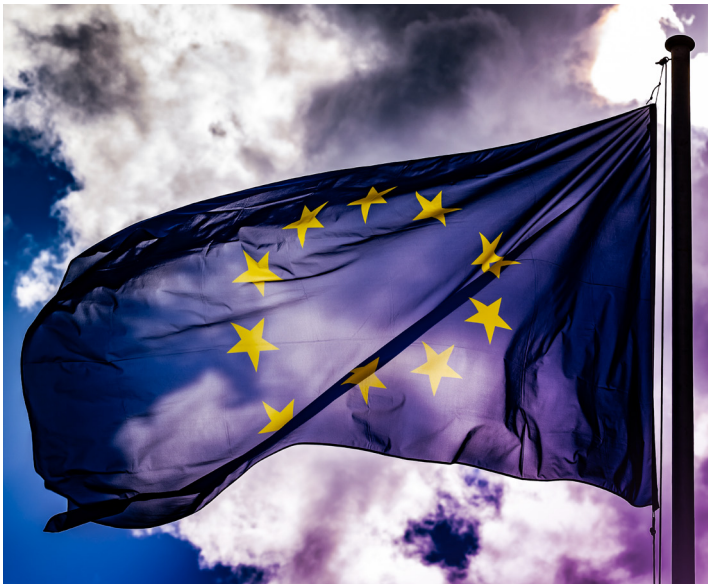
Commvault

Verwendung von Commvault Cloud zur Unterstützung der DORA-Compliance

Das Gesetz zur digitalen Betriebsresilienz, oder DORA, ist eine Verordnung der Europäischen Union, die darauf abzielt, die Cyber-Resilienz im Finanzsektor zu verbessern.

DORA legt Anforderungen für Finanzinstitutionen und verwandte Unternehmen fest, um sicherzustellen, dass ihre Systeme Cyberangriffen und anderen Störungen standhalten können. Dies hilft, das Finanzsystem stabil zu halten und die Verbraucher zu schützen.

WAS IST RESILIENZ?



Resilienz in der Welt der Cybersicherheit bezieht sich auf die Fähigkeit einer Organisation, sich von Cyberangriffen und anderen Sicherheitsvorfällen zu erholen. Angriffe zu verhindern und sich gegen Bedrohungsakteure zu verteidigen, sind Schlüsselelemente jeder Cyberstrategie, aber darauf vorbereitet zu sein, effektiv zu reagieren und sich zu erholen, ist möglicherweise noch wichtiger. Dies gilt insbesondere, da die Realität des heutigen Geschäftslebens ist, dass es nicht die Frage ist, ob Sie angegriffen werden, sondern wann und wie schlimm es sein wird.

Resilienz wird ein Differenzierungsmerkmal für Ihr Unternehmen sein, da sowohl Sie als auch andere in Ihrem Bereich täglich von modernen Cyberangriffen getestet werden. Wenn Sie die Geschäftskontinuität sicherstellen und Ausfallzeiten sowie Datenverluste minimieren können, hilft dies Ihnen, das Vertrauen Ihrer Kunden zu bewahren und das Geschäft derjenigen zu gewinnen, die nicht so gut vorbereitet waren. in the cybersecurity world refers to an organization's ability to bounce back from cyberattacks and other security incidents.

Aus diesem Grund haben Regierungen und Regulierungsbehörden weltweit festgelegt, was erforderlich ist, damit Organisationen weiterhin bestehen können und die Märkte vor den negativen Auswirkungen von Cyberangriffen geschützt werden. DORA ist nur ein Beispiel dafür.

WAS VERLANGT DORA?

Informations- und Kommunikationstechnologie (IKT) hat immer wieder gezeigt, dass sie ein Risiko für Unternehmen darstellt, indem sie Daten und persönliche Informationen von Verbrauchern preisgibt, wenn sie von Angreifern durchbrochen werden. Während viele Gesetze und Vorschriften darauf abzielen, Angriffe zu verhindern, nimmt DORA die Perspektive der Unvermeidlichkeit eines Angriffs ein und konzentriert sich darauf, was notwendig ist, um sicherzustellen, dass Organisationen einem Angriff standhalten und weiterhin operieren können. Dies ist besonders wichtig, wenn es um grundlegende Sektoren wie Finanzdienstleistungen geht.

Risikomanagement

Der Zweck des Rahmens besteht darin, IKT-Risiken zu identifizieren und anzugehen. Dies umfasst Dinge wie unbefugten Zugriff, Datenverletzungen und Systemausfälle. Durch das proaktive Management dieser Risiken können Finanzinstitutionen die Auswirkungen von Cyber-Vorfällen minimieren.

Schwerpunkte:

1. Identifizieren und inventarisieren Sie Ihre Assets, einschließlich Daten und Infrastruktur.
2. Implementieren Sie Sicherheitskontrollen, um Assets zu schützen, Sicherheitsverletzungen zu verhindernund das Risiko von Datenexfiltration oder unbefugter Zerstörung zu minimieren.
3. Nutzen Sie Technologien zur Bedrohungserkennung, die es Ihrem Sicherheitsteam ermöglichen, Anomalien in Ihrer Umgebung zu finden und Abhilfemaßnahmen auszulösen, um Bedrohungen zu neutralisieren.

Management und Minderung von Risiken Dritter

Zusätzlich zu den Risiken für Ihr Unternehmen müssen Organisationen auch im Angesicht von Ausfällen Dritter resilient sein. Die heutige Abhängigkeit von Cloud-Technologien und -Diensten, die unter der Kontrolle anderer stehen (Hosting, Offshoring, Berater), bedeutet, dass Sie in der Lage sein müssen, nicht nur Ihre eigenen Daten wiederherzustellen, sondern diese auch zu einem anderen Anbieter mit intakten Diensten zu verschieben. Diese Portabilität ist als Teil einer Resilienzstrategie entscheidend und sollte sowohl die Infrastruktur (sicherstellen, dass Sie Ihr Geschäft bei einem anderen Anbieter einrichten und betreiben können) als auch die Portabilität auf Anwendungs- und Arbeitslastebene (ob Ihre Apps schnell auf dieser neuen Infrastruktur hochgefahren werden können) abdecken.

Tests zur Wiederherstellung und Wiederherstellung

Indem Sie Cyber-Wiederherstellungsübungen in Ihre Sicherheitsstrategie integrieren und Ihre Wiederherstellungspläne testen, können Sie proaktiv Schwachstellen identifizieren und angehen, bevor eine Reaktion erforderlich ist. Dieser proaktive Ansatz baut Resilienz auf und ermöglicht es Ihrer Organisation, den Sturm von Cyberangriffen zu überstehen und gestärkt hervorzugehen.

Die Einzigartigkeit der Infrastruktur und Datenarchitektur jeder Organisation bedeutet auch, dass es keinen universellen Ansatz oder Vorlage gibt, die Sie verwenden können, um Resilienz zu gewährleisten. Eines ist jedoch sicher - wenn Sie einen Plan nicht vollständig üben oder testen, bevor er bei einem Verstoß benötigt wird, werden Sie auf die harte Tour herausfinden, wo es Lücken gibt.

Es gibt mehrere Möglichkeiten, Ihre Cyber-Wiederherstellungspläne zu testen:

Tabletop-Übungen

Simulieren Sie ein CyberangriffSzenario in einer nachgebildeten Umgebung, um Kommunikation, Entscheidungsfindung und Reaktionsprotokolle zu üben.

Cleanroom-Wiederherstellung

Dies schafft einen sicheren, isolierten Raum, um Wiederherstellungsverfahren zu testen, ohne das Risiko einer erneuten Infektion Ihrer Produktionssysteme einzugehen.

Hier können Sie Daten und Anwendungen wiederherstellen und sehen, ob sie wie vorgesehen funktionieren.

Durchgänge oder Audits

Durchlaufen Sie Pläne, ohne tatsächlich etwas wiederherzustellen. Dies hilft, Lücken und klärungsbedürftige Bereiche zu identifizieren

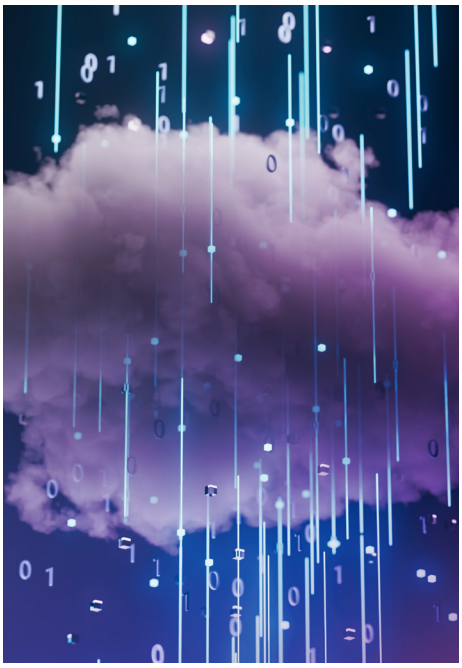
Vorfallreaktion, -management und -handhabung

Moderne Cyber-Vorfälle erfordern weit mehr als nur Ihre eigenen internen Systeme, Menschen und Prozesse. Die Anforderungen zur Dokumentation und Offenlegung von Verstößen sind zahlreich (GDPR, CCPA und kürzlich eingeführte Regeln für börsennotierte Unternehmen an US-Börsen durch die SEC, um nur einige zu nennen).

Aufgrund dieser Anforderungen müssen Organisationen ein robustes Programm haben, um sowohl ihre interne Reaktion zu handhaben, als auch die Prüfbarkeit durch Dritte zu ermöglichen und es dem Management zu ermöglichen, einen Cyber-Vorfall angemessen offenzulegen.

Selbst kompromittierte Daten in einer sauberen Umgebung zu halten, ermöglicht Dinge wie forensische Analysen und Berichte darüber, wie sich ein Vorfall entwickelt hat, welche Daten betroffen waren und die Taktiken, Techniken und Verfahren (TTPs) des Angreifers. Dies wird auch für Cyber-Versicherer zu einem wichtigen Thema, da sie genau wissen wollen, was passiert ist, um zu entscheiden, ob ein Anspruch unter ihren Policen zahlbar ist.

COMMVAULT CLOUD FÜR CYBER-RESILIENZ



Commvault ist der Goldstandard in der Cyber-Resilienz und führt den Kampf an, die Welt vor Ransomware und anderen Cyber-Bedrohungen zu schützen, indem es Unternehmen hilft, Risiken zu reduzieren, Ausfallzeiten zu minimieren und Kosten zu kontrollieren. Es ist die einzige Cyber-Resilienz-Plattform, die für die hybride Welt gebaut wurde und bietet die beste Datensicherheit für alle Workloads, überall, kombiniert mit schneller, unternehmensweiter Wiederherstellung.

Verstehen und Risiken für Ihre Daten reduzieren

Mit der Commvault-Risikoanalyse können Organisationen mühelos sensible Daten in ihrer gesamten Infrastruktur sichern und verteidigen. Sie gewinnen Einblick in Datenrisiken, um sensible Daten leicht zu identifizieren und zu kategorisieren, um problemlos zusammenzuarbeiten und potenzielle Datenverletzungen zu mildern, während sie gleichzeitig Kosten durch intelligente proaktive Datenmanagementstrategien einsparen.

Unstrukturierte Daten können auch mit Commvault Threat Scan gescannt werden, wodurch Betriebsteams die Kontrolle übernehmen und ihre Backup-Daten verteidigen können, indem sie proaktiv Malware-Bedrohungen identifizieren, um eine erneute Infektion während der Wiederherstellung zu reduzieren. Threat Scan analysiert Backup-Daten, um verschlüsselte oder beschädigte Dateien zu finden, sodass Benutzer schnell vertrauenswürdige Versionen ihrer Daten wiederherstellen können.

Bedrohungen und Anomalien in Ihrer Umgebung erkennen

Da Commvault Cloud bereits Ihre Daten sichert, haben wir die Möglichkeit, Bedrohungen für diese Daten intelligent zu erkennen. Die Commvault Cloud-Plattform kann nach frühen Warnungen für verdächtige Aktivitäten suchen, indem sie Ereigniszeitpläne analysiert und das Basisverhalten für jede Maschine festlegt. Durch den Vergleich von Dateimerkmalsänderungen mit etablierten Baselines werden abnormale Verhaltensweisen identifiziert und gemeldet. Dies ermöglicht es Administratoren, sofort zu handeln und das Risiko zu mindern.

Zusätzlich zur Überwachung einzelner Dateien auf Anomalien und Änderungen kann Commvault Threatwise Angreifer aufdecken, indem es Köder verwendet. Diese Köder sind so gestaltet, dass sie attraktive Ziele für Angreifer, die möglicherweise Aufklärung in Ihrer Umgebung betreiben, genau nachahmen. Sie sind für legitime Benutzer unsichtbar, aber für einen Angreifer unglaublich attraktiv. Sobald ein Angreifer auf eine dieser Fallen anspringt, kann Commvault sofort hochwertige Alarme für Sicherheitsteams auslösen und gleichzeitig die Interaktionen der Bedrohungsakteure für forensische Untersuchungen bewahren.

Testen Sie Ihre Pläne

Commvault® Cloud Cleanroom™ Recovery bietet eine erschwingliche, saubere, sichere, isolierte Wiederherstellungsumgebung auf Abruf zum Testen von Cyber-Wiederherstellungsplänen, zur Durchführung sicherer forensischer Analysen und zur ununterbrochenen Geschäftskontinuität.

Im Gegensatz zu allen anderen Datensicherheitsangeboten, die auf Katastrophenwiederherstellung beschränkt sind und durch eine begrenzte Anzahl von Workloads und Wiederherstellungsoptionen eingeschränkt sind, und im Gegensatz zu traditionellen isolierten Wiederherstellungsumgebungen, die zu teuer sind, um regelmäßig ausgeführt zu werden und für die meisten Organisationen zunehmend komplex zu verwalten sind, bietet nur Commvault Cloud Cleanroom Recovery die Möglichkeit, Workloads von AWS, Azure, GCP, OCI und On-Prem-Umgebungen in eine sichere, auf Abruf isolierte Cleanroom-Umgebung zu übertragen. Diese umfassende Wiederherstellungsplattform verringert die Komplexität und die Kosten der Verwendung verschiedener Werkzeuge und liefert stattdessen die stärkste und zuverlässigste Cyber-Resilienz und Bereitschaft.

Probieren Sie Commvault Cloud heute aus

Commvault Cloud kann Ihrer Organisation helfen, eine bessere Resilienz zu erreichen und mehrere Elemente on DORA einzuhalten. Commvault stärkt Ihr IKT Risikomanagement, indem es die Risikoüberwachung automatisiert und Echtzeiterkennung von Anomalien und Bedrohungen bietet. Das Incident Management kann mit der Planung der Cyber-Wiederherstellung rationalisiert werden. Und jetzt können Sie die Cleanroom-Technologie nutzen, um Ihre Resilienzstrategien auf effiziente, proaktive und kostengünstige Weise zu testen und umzusetzen.

VEREINBAREN SIE NOCH HEUTE EINE LIVE-DEMO ÜBER COMMVAULT CLOUD.

Demo vereinbaren →