SOLUTION BRIEF

Utilisation de Commvault Cloud pour Assister à la Conformité DORA

La Loi sur la Résilience Opérationnelle Numérique, ou DORA, est une réglementation de l'Union Européenne qui se concentre sur l'amélioration de la résilience cybernétique dans le secteur financier.

DORA établit des exigences pour les institutions financières et les entreprises associées pour garantir que leurs systèmes peuvent résister aux cyberattaques et autres perturbations. Cela aide à maintenir la stabilité du système financier et à protéger les consommateurs.

QU'EST-CE QUE LA RÉSILIENCE ?

Dans le monde de la cybersécurité, la résilience fait référence à la capacité d'une organisation à se remettre des cyberattaques et autres incidents de sécurité. Prévenir les attaques et se défendre contre les acteurs de menaces sont des éléments clés de toute stratégie cybernétique, mais être prêt à répondre et à se rétablir efficacement est peut-être encore plus important. Cela est particulièrement vrai car la réalité des affaires aujourd'hui est qu'il ne s'agit pas de savoir si vous allez être attaqué, mais quand et à quel point cela sera grave.

La résilience sera un différenciateur pour votre entreprise car vous et d'autres dans votre domaine serez testés quotidiennement par des cyberattaques modernes. Si vous êtes capable d'assurer la continuité des affaires et de minimiser les temps d'arrêt et la perte de données, cela vous aidera à rester digne de confiance pour vos clients et vous permettra de capturer les affaires de ceux qui n'étaient pas si bien préparés.

Pour cette raison, les gouvernements et les organismes de réglementation du monde entier ont codifié ce qui est nécessaire pour que les organisations restent viables et protègent les marchés des effets néfastes des cyberattaques. DORA est juste un exemple de cela.

QUE REQUIERT DORA ?

La technologie de l'information et de la communication (TIC) a prouvé maintes et maintes fois qu'elle présente un risque pour les entreprises en exposant les données et les informations personnelles des consommateurs lorsqu'elle est violée par des attaquants. Alors que de nombreux actes et réglementations visent à prévenir les attaques, DORA prend la perspective de l'inévitabilité d'une attaque et se concentre sur ce qui est nécessaire pour garantir que les organisations peuvent résister à une attaque et continuer à fonctionner. Cela est particulièrement important lorsqu'il s'agit de secteurs fondamentaux, comme les services financiers.

Gestion des risques

Le but du cadre est d'identifier et de traiter les risques TIC. Cela inclut des choses comme l'accès non autorisé, les violations de données et les pannes de système. En gérant proactivement ces risques, les institutions financières peuvent minimiser l'impact des incidents cybernétiques.

Domaines d'intervention:

1. Identifiez et inventoriez vos actifs, y compris les données et l'infrastructure.
2. Mettre en place des contrôles de sécurité pour protéger les actifs, prévenir les violations et minimiser le risque d'exfiltration de données ou de destruction non autorisée.
3. Utiliser des technologies de détection de menaces qui permettent à votre équipe de sécurité de trouver des anomalies dans votre environnement et de déclencher des actions de remédiation pour neutraliser les menaces.

Gestion et atténuation des risques liés aux tiers

En plus des risques pour votre entreprise, les organisations doivent être résilientes face aux défaillances de tiers. La dépendance actuelle aux technologies et services cloud qui sont sous le contrôle d'autres (hébergement, délocalisation, consultants) signifie que lorsque les systèmes vont mal, vous devez être capable de récupérer non seulement vos propres données, mais aussi de les transférer à un autre fournisseur avec des services toujours intacts. Cette portabilité est cruciale dans le cadre d'une stratégie de résilience et devrait couvrir à la fois l'infrastructure (assurant que vous pouvez configurer et gérer votre entreprise sur un autre fournisseur) mais aussi la portabilité au niveau des applications et des charges de travail (si vos applications peuvent être rapidement mises en service sur cette nouvelle infrastructure).

Tests pour la récupération et la restauration

En intégrant des exercices de récupération cybernétique et en testant vos plans de récupération dans votre stratégie de sécurité, vous pouvez identifier et aborder proactivement les faiblesses avant que la réponse ne soit nécessaire. Cette approche proactive renforce la résilience, permettant à votre organisation de résister à la tempête des cyberattaques et d'en sortir plus forte.

L'unicité de l'infrastructure et de l'architecture des données de chaque organisation signifie également qu'il n'y a pas d'approche ou de modelé universel que vous pouvez utiliser pour garantir la résilience. Une chose est certaine, cependant—si vous ne pratiquez ou ne testez pas pleinement un plan avant qu'il ne soit nécessaire lors d'une violation, vous découvrirez à la dure où se trouvent les lacunes.

Il existe plusieurs façons des réaliser des tests contre vos plans de récupération cybernétique :

Exercices

Simulate a cyberattack scenario using a mock environment to practice communication, decision-making, and response protocols.

Récuperation en salle blanche

Cela crée un espace sûr et isolé pour tester les procédures de récupération sans risquer de réinfecter vos systémes de production. Vous pouvez récupérer des données et des applications ici et voir si elles fonctionnent comme prévu.as intended.

Marches à suivre ou audits

Parcourir les plans sans réellement récuperer quoi que ce soit. Cela aide à identifier les lacunes et les zones nécessitant des éclaircissements.

Réponse aux incidents, gestion et traitement

Les incidents cybernétiques modernes nécessitent bien plus que vos propres systèmes internes, personnes et processus. Les exigences pour documenter et divulguer les violations sont nombreuses (GDPR, CCPA et les règles récentes mises en place pour les entreprises cotées en bourse aux États-Unis par la SEC, pour n'en nommer que quelques-unes).

En raison de ces exigences, les organisations doivent disposer d'un programme robuste pour gérer à la fois leur réponse interne, mais aussi fournir une auditabilité par des tiers et permettre à la direction de divulguer adéquatement un incident cybernétique.

Maintenir même des données compromises dans un environnement propre permet des choses comme l'analyse judiciaire et le rapport sur la façon dont un incident s'est déroulé, quelles données ont été affectées et les tactiques, techniques et procédures (TTP) de l'attaquant. Cela devient également un problème clé pour les assureurs cyber, car ils veulent voir exactement ce qui s'est passé pour déterminer si une réclamation est payable en vertu de leurs polices.

COMMVAULT CLOUD POUR LA RÉSILIENCE CYBERNÉTIQUE

Commvault est la référence en matière de résilience cybernétique, menant la charge pour protéger le monde contre les ransomwares et autres menaces cybernétiques en aidant les entreprises à réduire les risques, minimiser les temps d'arrêt et contrôler les coûts. C'est la seule plateforme de résilience cybernétique conçue pour le monde hybride, offrant la meilleure sécurité des données pour toutes les charges de travail, partout, combinée à une récupération rapide à l'échelle de l'entreprise.

Comprendre et réduire les risques pour vos données

Avec l'analyse des risques de Commvault, les organisations peuvent sécuriser et défendre sans effort les données sensibles à travers toute leur infrastructure. Ils obtiennent une visibilité sur les risques de données pour identifier et catégoriser facilement les données sensibles afin de collaborer facilement et de mitiger les violations de données potentielles, tout en économisant des coûts grâce à des stratégies de gestion de données proactives intelligentes.

Les données non structurées peuvent également être analysées avec Commvault Threat Scan, permettant aux équipes d'opérations de prendre le contrôle et de défendre leurs données de sauvegarde en identifiant proactivement les menaces de logiciels malveillants pour réduire la réinfection pendant la récupération. Threat Scan analyse les données de sauvegarde pour trouver des fichiers chiffrés ou corrompus afin que les utilisateurs puissent récupérer rapidement des versions fiables de leurs données.

Détectez les menaces et les anomalies dans votre environnement

Parce que Commvault Cloud sauvegarde déjà vos données, nous avons la capacité de détecter intelligemment les menaces pour ces données. La plateforme Commvault Cloud peut rechercher des signes avant-coureurs d'activité suspecte en utilisant l'apprentissage automatique, en analysant les chronologies des événements et en établissant un comportement de base pour chaque machine. En comparant les changements de caractéristiques des fichiers par rapport aux bases de référence établies, les comportements anormaux sont identifiés et signalés. Cela permet aux administrateurs de prendre des mesures immédiates et de mitiger les risques.

En plus d'examiner les fichiers individuels pour détecter des anomalies et des changements, Commvault Threatwise peut aider à faire surface des attaquants en utilisant des leurres. Ces leurres sont conçus pour imiter de manière convaincante des cibles attrayantes pour les attaquants qui pourraient effectuer des reconnaissances sur votre environnement. Ils sont invisibles pour les utilisateurs légitimes, mais incroyablement attrayants pour un attaquant. Une fois qu'un attaquant s'engage avec l'un de ces pièges, Commvault peut immédiatement déclencher des alertes de haute fidélité pour les équipes de sécurité, tout en préservant les interactions des acteurs de la menace pour l'enquête judiciaire.

Testez vos plans

La récupération en salle blanche Commvault® Cloud Cleanroom™ offre un environnement de récupération isolé, propre, sécurisé et abordable à la demande pour tester les plans de récupération cybernétique, réaliser des analyses judiciaires sécurisées et assurer une continuité d'activité ininterrompue.

Contrairement à toutes les autres offres de sécurité des données limitées à la récupération après sinistre et contraintes par un ensemble limité de charges de travail et d'options de récupération, et contrairement aux environnements de récupération isolés traditionnels, qui sont trop coûteux à exécuter régulièrement et sont devenus de plus en plus complexes à gérer pour la plupart des organisations, seule la récupération en salle blanche Commvault Cloud Cleanroom offre la capacité de récupérer des charges de travail depuis AWS, Azure, GCP, OCI et des environnements sur site, vers une salle blanche isolée dans le cloud à la demande. Cette plateforme de récupération complète réduit la complexité et le coût d'utilisation d'outils disparates et offre plutôt la résilience cybernétique et la préparation les plus solides et les plus fiables.

Essayez Commvault Cloud dès aujourd'hui

Commvault Cloud peut aider votre organisation à atteindre une meilleure résilience et à se conformer à plusieurs éléments de DORA. Commvault vous aide à renforcer votre gestion des risques informatiques en automatisant la surveillance des risques, en fournissant une détection en temps réel des anomalies et des menaces. La gestion des incidents peut être rationalisée grace à la planification de la cyber-reprise. Et maintenant, vous pouvez utiliser la technologie des salles blanches pour tester et executer vos stratégies de résilience de maniére efficace, proactive et rentable.

CONTACTEZ-NOUS POUR EN SAVOIR OBTENEZ UNE DÉMONSTRATION EN DIRECT DE COMMVAULT CLOUD AUJOURD'HUI

OBTENEZ UNE DEMONSTRATION À

Live demo →

To learn more, visit **commvault.com**