DATASHEET

DORA Compliance

Transformieren Sie Ihre DORA-Reise mit Mimecast.

Das Problem

Der Digital Operational Resilience Act (DORA) stellt einen entscheidenden Wendepunkt für Finanzinstitute in der Europäischen Union dar. Mit der näher rückenden Frist zur Einhaltung am 17. Januar 2025 stehen Organisationen unter enormem Druck, ihre digitalen Resilienzrahmen zu transformieren. Die Konsequenzen sind erheblich – Nichteinhaltung kann zu Geldbußen von bis zu 2 % des weltweiten Jahresumsatzes, operativen Einschränkungen und dauerhaften Reputationsschäden führen, die das Vertrauen der Kunden nachhaltig erschüttern.

Was DORA besonders herausfordernd macht, ist sein umfassender Geltungsbereich. Finanzinstitute müssen sich mit komplexen Anforderungen in den Bereichen ICT-Risikomanagement, Vorfallmeldungen und der Überwachung von Drittanbietern auseinandersetzen. Die Verordnung erfordert erhebliche organisatorische Veränderungen und Fachwissen, das viele Organisationen intern nur schwer aufbauen können. Während sich Finanzinstitute mit diesen miteinander verknüpften Herausforderungen und der Verwaltung ihrer kritischen ICT-Dienstleister auseinandersetzen, erfordert der Weg zur Compliance eine sorgfältige Navigation durch eine komplexe regulatorische Landschaft, die keinerlei Spielraum für Fehler lässt.

2 % GELDSTRAFE

des weltweiten Umsatzes bei Nichteinhaltung [1]

$6,08 MILLIONEN

durchschnittliche Kosten eines Datenschutzvorfalls. [2]

1 MIO. €

Geldstrafe für Einzelpersonen [3]

[1] https://www.avenga.com/magazine/guide-to-doras-penalties/
[2] https://securityintelligence.com/articles/cost-of-a-data-breach-2024-financial-industry/
[3] https://securityintelligence.com/articles/cost-of-a-data-breach-2024-financial-industry/

Die Lösung

Mimecast bietet einen umfassenden Lösungsrahmen, der die Anforderungen der DORA-Compliance abdeckt. Unsere Plattform vereint fortschrittliche Sicherheitslösungen für die Zusammenarbeit mit mehrschichtigen Datei-Inspektionsfunktionen, die durch KI und Bedrohungsintelligenz unterstützt werden, um komplexe E-Mail-Umgebungen zu schützen. Dank nahtloser Integration in bestehende Sicherheitsinfrastrukturen ermöglichen automatisierte Reaktionen und robuste Funktionen zum Teilen von Bedrohungsinformationen die Erkennung und Überwachung von Risiken. Organisationen profitieren von einer ganzheitlichen Bedrohungssicht durch kontextuelle E-Mail-Telemetrie und priorisierte Warnmeldungen.

Mimecast gewährleistet unterbrechungsfreien Kommunikationszugang – unabhängig von der Ursache eines Ereignisses. Mit den Human Risk Management-Funktionen von Mimecast bleiben Nutzer stets über die neuesten Bedrohungen informiert und werden gezielt am Punkt des Risikos eingebunden. Backup- und Wiederherstellungsfunktionen stellen sicher, dass kritische Kommunikationsdaten jederzeit wiederhergestellt werden können. Dieser integrierte Ansatz unterstützt Unternehmen bei der Erfüllung der DORA-Compliance und verschafft ihnen einen strategischen Vorteil im Management ihrer digitalen operativen Resilienz.

Wesentliche Vorteile:

- **Risikosichtbarkeit:** Gewinnen Sie einzigartige Einblicke in Human Risk innerhalb Ihrer Organisation, basierend auf dem Nutzerverhalten und realen Bedrohungen.
- **Anpassungsfähige Maßnahmen:** Bekämpfen Sie unsichere Verhaltensweisen mit zeitgerechtem Feedback und zielgerichtetem Training – genau dann, wenn es benötigt wird.
- **Proaktive Kontrollen:** Reduzieren Sie Human Risk, indem Sie Sicherheitskontrollen proaktiv anpassen, um Ihre Benutzer besser zu schützen.

DORA-Compliance leicht gemacht: Der Mimecast-Vorteil

Bei Mimecast erkennen wir, dass die Einhaltung von DORA ein vielseitiges Lösungsrahmen erfordert. Unser umfassender Ansatz deckt sowohl technische Anforderungen als auch richtlinienkonforme Kontrollen ab und bietet integriertes ICT-Risikomanagement, das Schutz, Prävention, Erkennung, kontinuierliches Lernen sowie robuste Backup- und Wiederherstellungsfunktionen umfasst. So unterstützen wir Finanzinstitute dabei, die kritischen Anforderungen von DORA zu erfüllen:

Schutz und Prävention
Unsere fortschrittliche Sicherheitslösung für die Zusammenarbeit wurde entwickelt, um selbst die komplexesten E-Mail-Umgebungen zu schützen, dank ihrer mehrschichtigen Inspektionsfunktionen, unterstützt durch traditionelle Verteidigungsmethoden, Bedrohungsintelligenz und fortschrittliche KI. Jedes Element einer E-Mail wird in Echtzeit überprüft, um Bedrohungen abzufangen, bevor sie Ihr Postfach erreichen. Mimecast integriert sich nahtlos in Ihre bestehende Sicherheitsinfrastruktur und bietet automatisierte Korrekturmaßnahmen. Dies ermöglicht IT- und Sicherheitsteams, Risiken effektiv zu steuern und gleichzeitig die Komplexität zu bewältigen, sodass Ihre Organisation sich gegen anspruchsvolle E-Mail-Angriffe verteidigen kann, ohne die Geschäftskontinuität zu gefährden. Mit Incydr erhalten Organisationen umfassende Einblicke in Datenexpositionen und eliminieren potenzielle blinde Flecken. Das System unterscheidet intelligent zwischen echten Bedrohungen und Low-Risk-Ereignissen, wodurch die Zeit für die Untersuchung von kritischen IP-Diebstahlvorfällen durch fortschrittliche Inhaltsinspektion und kontextuelle Analyse optimiert wird. Über unsere Technologiepartner sind automatisierte Netzwerktrennungsfunktionen verfügbar, um potenzielle Cyber-Vorfälle effektiv einzugrenzen.

Erkennung und Überwachung
Integration ist bei Mimecast von zentraler Bedeutung, und wir legen großen Wert auf den Austausch von Bedrohungsintelligenz mit Drittanbieter-Tools. Dies ermöglicht es Organisationen, ihre Sicherheitslage zu verbessern, indem sie kollektive Intelligenz aus mehreren Quellen nutzen, um eine ganzheitliche Bedrohungssicht und kontextuelle E-Mail-Telemetrie zu bieten. Die Generierung von priorisierten Warnmeldungen und automatisiertem Datenaustausch beschleunigt die Untersuchungen und reduziert den manuellen Aufwand durch Reaktionsmaßnahmen, sodass Sicherheitsteams effektiver auf aufkommende Bedrohungen reagieren können.

Reaktion und Wiederherstellung
Die Kontinuität gewährleistet unterbrechungsfreien Kommunikationszugang sowohl bei geplanten als auch unvorhergesehenen Ausfällen. Unterstützt durch geografisch verteilte Rechenzentren und abgesichert durch eine 100 % Serviceverfügbarkeits-Garantieleistung (SLA) ist diese Funktion unerlässlich für Finanzinstitute, die unter dem DORA-Rahmen kontinuierliche Betriebsabläufe sicherstellen müssen.

Kontinuierliches Lernen und Weiterentwicklung
Mimecast Engage wandelt potenzielle Sicherheitslücken in organisatorische Stärken um, indem gezielte Schulungen und Risikobewertungen durchgeführt werden. Die Human Risk Management-Funktionen liefern detaillierte Einblicke in das Verhalten und die Risikoprofile von Mitarbeitern, die in Ihre Sicherheitswerkzeuge integriert sind, und bieten maßgeschneiderte Sicherheitsbewusstseinstrainings, die sich an aufkommende Bedrohungen anpassen.

Umfassendes Backup und Wiederherstellung
Sync and Recover ermöglicht eine schnelle Wiederherstellung des Betriebs nach versehentlichem Datenverlust oder böswilligen Angriffen. Diese Funktion adressiert speziell E-Mail-basierte Bedrohungen wie Ransomware und ermöglicht eine schnelle, detaillierte Wiederherstellung von Postfächern, Kalendern und Aufgaben, mit konfigurierbaren Aufbewahrungsrichtlinien.

Darüber hinaus sind unsere Tools darauf ausgelegt, Ihre Anforderungen an Audits, integrierte Protokollierung und Bedrohungsweitergabe zu unterstützen, sodass Organisationen Compliance-Anforderungen erfüllen und aufrechterhalten können. Durch die Partnerschaft mit Mimecast können Finanzinstitute DORA-Compliance selbstbewusst umsetzen und gleichzeitig ihre digitale operative Resilienz stärken. Unsere Lösungen helfen nicht nur dabei, regulatorische Anforderungen zu erfüllen, sondern verschaffen auch einen strategischen Vorteil beim Management von ICT-Risiken in der heutigen komplexen digitalen Umgebung.

DORA-Verordnung	Details
9 - Schutz und Prävention	Collaboration Security • KI-gestützte Schutzmaßnahmen gegen Phishing- und BEC-Angriffe durch Beziehungsanalyse und NLP (Natural Language Processing) • Mehrschichtiger Malware-Schutz mit Sandboxing, URL-Sicherheit und QR-Code-Schutz • Zentralisierte Web-Konsole für plattformübergreifendes Management mit automatischer IAM-Synchronisation und intelligentem Routing Datenschutz • KI-gestützte Inhaltsinspektion zur Erkennung sensibler Daten und geistigen Eigentums in exfiltrierten Dateien • Kombination von Standard- und benutzerdefinierten Risikoinformationen zur Identifikation unbefugter Übertragungen privilegierter Inhalte und proprietärer Informationen • Bewertung der Inhaltsensitivität, Dateimetadaten und Klassifizierung für eine umfassende Exfiltrationsüberwachung
10 - Erkennung	• Bidirektionaler Threat Intelligence-Austausch zwischen Sicherheitsplattformen ermöglicht eine Echtzeit-Synchronisation zwischen Endpunkten, Firewalls und E-Mail-Sicherheit. • Umfassende Integration von Bedrohungsaustausch, Untersuchungen, täglichen Aufgaben und automatisierten Reaktionen. • SOAR- und XDR-Plattform-Integrationen ermöglichen die automatisierte Behebung von Bedrohungen, wodurch die Reaktionszeiten von Stunden auf Minuten verkürzt werden.
11 - Reaktion und Wiederherstellung	• Nahtlose Integration von Microsoft Outlook mit plattformübergreifender Unterstützung (mobil, web, Mac), vollständiger E-Mail-Funktionalität und SMS-Benachrichtigungen • Erweiterte E-Mail-Überwachung mit vom Administrator definierten Schwellenwerten und automatisierten Benachrichtigungen • Zielgerichtetes Event-Management zur Aufrechterhaltung der Kontinuität für Einzelpersonen oder Gruppen, wobei die Sicherheit gewährleistet bleibt und eine automatische Synchronisation der Postfächer für eine schnelle Wiederherstellung ermöglicht wird
12 - Backup-Politiken und -Verfahren, Wiederherstellungs- und Erholungsverfahren sowie -methoden	• Überwachung von eingehenden und ausgehenden E-Mails mithilfe von vom Administrator definierten Schwellenwerten • Automatisierte Benachrichtigungen erhalten, die eine event-spezifische Konsole mit wichtigen Informationen und einer One-Click-Aktivierung eines alternativen E-Mail-Pfads anzeigen • Schnelles Auslösen von Kontinuitätsereignissen, wenn primäre E-Mail-Systeme offline sind • Auslösen von Kontinuitätsereignissen für Einzelpersonen oder Gruppen, ohne ein unternehmensweites Ereignis auszulösen • Vollständiger E-Mail-Schutz während der Kontinuitätsereignisse bleibt erhalten • Reduzierung der Bereinigungszeit durch automatische Synchronisation der Postfächer
13 - Lernen und Weiterentwicklung	• Umfassende Risikobewertung basierend auf realen und simulierten Phishing-Daten zur Identifikation von Bedrohungen für die Organisation und hochriskanten Mitarbeitern • Echtzeit-Verhaltenscoaching durch Mikro-Lernmodule und Impulse, die bewährte Sicherheitspraktiken verstärken • Schnellstart-fähiges automatisiertes Sicherheitsbewusstseinsprogramm mit branchenüblicher Compliance und Phishing-Simulationsfunktionen

Über Mimecast

Sichern Sie Human Risk mit einer einheitlichen Plattform.

Die vernetzte Plattform von Mimecast für das Management von Human Risk schützt vor raffinierten Bedrohungen, die auf menschliche Fehler abzielen. Durch die Gewährleistung von Transparenz bezüglich Human Risk in Ihren Kollaborationslandschaften können Sie Ihre Organisation schützen, kritische Daten sichern und Mitarbeiter aktiv einbinden, um Risiken zu reduzieren und die Produktivität zu steigern.