DATASHEET

DORA Compliance

Transforma tu camino hacia el reglamento DORA con Mimecast.

El Problema

El Digital Operational Resilience Act (DORA) marca un punto de inflexión crucial para las instituciones financieras de la Unión Europea. A medida que se acerca la fecha límite de cumplimiento del **17 de enero de 2025**, las organizaciones enfrentan una presión sin precedentes para transformar sus marcos de resiliencia digital. Las consecuencias de no cumplir son significativas: las sanciones pueden llegar hasta el 2 % de la facturación anual global, restricciones operativas y daños reputacionales duraderos que erosionan la confianza del cliente.

Lo que hace que DORA sea especialmente desafiante es su alcance general. Las instituciones financieras deben navegar por requisitos complejos en gestión de riesgos ICT, informes de incidentes y supervisión de terceros. La regulación exige cambios organizacionales sustanciales y una experiencia que muchas organizaciones luchan por desarrollar internamente.

Mientras las instituciones financieras lidian con estos desafíos interconectados, mientras gestionan a sus proveedores ICT críticos, el camino hacia el cumplimiento requiere una navegación cuidadosa a través de un panorama regulatorio complejo, donde no hay margen para el error.

Beneficios Clave

- **Visibilidad del riesgo.** Obtén una visibilidad sin precedentes del riesgo humano dentro de tu organización, compilada en función del comportamiento de los usuarios y las amenazas reales.
- **Acciones adaptativas.** Aborda los comportamientos inseguros con retroalimentación oportuna y capacitación adaptada a sus necesidades, entregada a quienes la necesitan, cuando la necesitan.
- **Controles proactivos.** Mitiga el riesgo humano en todo tu panorama de seguridad, ajustando de manera proactiva los controles de seguridad para proteger mejor a los usuarios.

MULTA DEL 2%

sobre la facturación global debido a la no conformidad

6,08 MILLONES DE DÓLARES

costo promedio de una violación de datos

1 MILLÓN DE EUROS

de multa para individuos

La Solución

Mimecast ofrece un marco de solución integral que responde a los requisitos de cumplimiento de DORA. Nuestra plataforma combina seguridad avanzada para la colaboración con capacidades de inspección de archivos en múltiples capas, impulsadas por IA e inteligencia sobre amenazas, para proteger entornos de correo electrónico complejos. A través de una integración sin problemas con la infraestructura de seguridad existente, la remediación automatizada y las capacidades robustas de intercambio de inteligencia sobre amenazas permiten la detección y monitoreo, lo que permite a las organizaciones obtener una visibilidad completa de las amenazas con telemetría contextual del correo electrónico y alertas basadas en prioridades. Las organizaciones pueden mantener acceso ininterrumpido a las comunicaciones, independientemente del evento de origen. El aprendizaje continuo a través de las capacidades de Gestión del Riesgo Humano de Mimecast asegura que los usuarios estén al tanto de las amenazas más recientes y estén comprometidos en el punto de riesgo. Las capacidades de respaldo y recuperación aseguran que los datos de comunicación críticos puedan ser restaurados, sin importar el evento que originó la amenaza. Este enfoque integrado ayuda a las organizaciones a cumplir con el DORA y les proporciona una ventaja estratégica en la gestión de su resiliencia operativa digital.

Cumplimiento de DORA Simplificado: La Ventaja de Mimecast

En Mimecast, reconocemos que el cumplimiento de DORA requiere un marco de solución polifacético. Nuestro enfoque integral aborda tanto los requisitos técnicos, como los controles alineados con las políticas a través de una gestión de riesgos ICT integrada que abarca protección, prevención, detección, aprendizaje continuo y capacidades robustas de respaldo y recuperación. Así es como ayudamos a las entidades financieras a cumplir con los requisitos críticos de DORA:

Protección y Prevención

Nuestra seguridad avanzada para la colaboración está diseñada para mantener incluso los entornos de correo electrónico más complejos seguros, gracias a sus capacidades de inspección en múltiples capas, impulsadas por defensas tradicionales, inteligencia sobre amenazas y IA avanzada. Cada elemento de un correo electrónico es inspeccionado en tiempo real, deteniendo las amenazas antes de que lleguen a tu bandeja de entrada. Mimecast se integra perfectamente con tu infraestructura de seguridad existente, mientras proporciona capacidades de remediación automatizada. Esto permite a los equipos de TI y seguridad controlar eficazmente el riesgo mientras manejan la complejidad, permitiendo a tu organización defenderse contra ataques sofisticados de correo electrónico sin comprometer la continuidad empresarial de negocio. A través de Incydr, las organizaciones obtienen visibilidad completa de la exposición de datos, eliminando los posibles puntos ciegos. El sistema diferencia inteligentemente entre amenazas reales y eventos de bajo riesgo, optimizando el tiempo invertido en investigar incidentes críticos de robo de propiedad intelectual mediante una inspección avanzada del contenido y un análisis contextual. A través de nuestros socios tecnológicos, están disponibles capacidades de aislamiento automatizado de la red, para contener eficazmente los posibles incidentes cibernéticos.

Detección y Monitorización

La integración es clave en Mimecast, y valoramos el intercambio de inteligencia sobre amenazas con herramientas de terceros. Esto permite a las organizaciones mejorar su postura de seguridad aprovechando la inteligencia colectiva de múltiples fuentes, proporcionando visibilidad completa de las amenazas y telemetría contextual de los correos electrónicos. La generación de alertas basadas en prioridades y el intercambio automatizado de datos aceleran las investigaciones, mientras reducen el esfuerzo manual mediante acciones de respuesta, lo que permite a los equipos de seguridad responder de manera más efectiva a las amenazas emergentes.

Respuesta y Recuperación

La continuidad garantiza un acceso ininterrumpido a la comunicación durante interrupciones planificadas y no planificadas. Respaldada por centros de datos distribuidos geográficamente y un SLA de disponibilidad de servicio del 100%, esta capacidad es esencial para las entidades financieras que requieren operaciones continuas bajo el marco de DORA

Aprendizaje Continuo y Evolución

Mimecast Engage transforma las posibles vulnerabilidades de seguridad en fortalezas organizacionales mediante capacitación dirigida y puntuación de riesgos. Las capacidades de Human Risk Management proporcionan información detallada sobre los comportamientos de los empleados y los perfiles de riesgo, integrando tus herramientas de seguridad y ofreciendo formación personalizada en concienciación sobre seguridad que se adapta a las amenazas emergentes.

Backup y Recuperación Completos

Sync and Recover permite una restauración operativa rápida tras la pérdida accidental de datos o acciones maliciosas. Esto aborda específicamente amenazas basadas en correos electrónicos como el ransomware, ofreciendo una recuperación rápida y granular de buzones, calendarios y tareas, con políticas de retención configurables.

Además, nuestras herramientas están diseñadas para respaldar tus necesidades de auditoría, registro integrado y compartición de amenazas, permitiendo a las organizaciones cumplir y mantener la conformidad. Al asociarse con Mimecast, las entidades financieras pueden abordar con confianza el cumplimiento de DORA, mientras mejoran su resiliencia operativa digital global. Nuestras soluciones no solo ayudan a cumplir con los requisitos regulatorios, sino que también brindan una ventaja estratégica en la gestión de riesgos ICT en el entorno digital complejo de hoy.

Articulo DORA	Detalles
9 - Protección y prevención	**Seguridad en colaboración** • Protección potenciada por IA contra ataques de phishing y BEC mediante el análisis de relaciones y NLP • Defensa contra malware en múltiples capas con sandboxing, seguridad de URLs y protección de códigos QR • Consola web centralizada para la gestión multiplataforma con sincronización automática de IAM y enrutamiento inteligente **Protección de datos** • Inspección de contenido potenciada por IA que detecta datos sensibles e IP en archivos exfiltrados • Combina indicadores de riesgo estándar y personalizados para identificar transferencias no autorizadas de contenido privilegiado e información propietaria • Evalúa la sensibilidad del contenido, los metadatos de los archivos y la clasificación para una detección completa de exfiltración
10 - Detección	• Compartición bidireccional de inteligencia sobre amenazas entre plataformas de seguridad que permite la sincronización en tiempo real entre endpoints, cortafuegos y seguridad de correo electrónico • Integración completa entre compartir amenazas, investigación, tareas diarias y respuesta automatizada • Las integraciones con SOAR y XDR permiten la remediación automática de amenazas, reduciendo los tiempos de respuesta de horas a minutos
11 - Respuesta y recuperación	• Integración fluida con Microsoft Outlook y soporte multiplataforma (móvil, web, Mac), con funcionalidades completas de correo electrónico y notificaciones SMS • Monitoreo avanzado de correos electrónicos con umbrales definidos por el administrador y alertas automáticas • Gestión dirigida de eventos de continuidad para individuos o grupos, manteniendo la seguridad y habilitando la sincronización automática del buzón para una rápida recuperación
12 - Políticas de respaldo y procedimientos, proced imientos de restauración y métodos de recuperación	• Monitoreo de correos entrantes y salientes utilizando umbrales definidos por el administrador • Recepción de alertas automatizadas que proporcionan una consola específica del evento con información clave y activación con un solo clic de un camino alternativo de correo • Activación rápida de eventos de continuidad cuando los sistemas de correo primarios están fuera de línea • Activación de eventos de continuidad para individuos o grupos sin activar un evento a nivel organizacional • Mantenimiento de la protección total de seguridad de los correos electrónicos durante eventos de continuidad • Reducción del tiempo de limpieza mediante la sincronización automática del buzón
13 - Aprendizaje y evolución	• Puntuación completa de riesgos basada en datos de phishing reales/simulados para identificar amenazas organizacionales y empleados de alto riesgo • Entrenamiento conductual en tiempo real mediante módulos de microaprendizaje y sugerencias, reforzando las mejores prácticas de seguridad • Programa automatizado de concienciación en seguridad con simulación de phishing y capacidades de cumplimiento normativo

Acerca de Mimecast

Asegure el riesgo humano con una plataforma unificada. La plataforma conectada de gestión del riesgo humano de Mimecast previene amenazas sofisticadas que apuntan al error humano. Al obtener visibilidad del riesgo humano en sus paisajes de colaboración, puede proteger su organización, salvaguardar datos críticos y comprometer activamente a los empleados para reducir el riesgo y mejorar la productividad.