

NIS2 Compliance

Mit NIS2 und Mimecast zu einer stärkeren digitalen Resilienz

Problem

Mit der Umsetzung der NIS2-Richtlinie stehen viele Unternehmen in der Europäischen Union heute vor einer außergewöhnlichen Herausforderung. Das erweiterte Cybersecurity-Framework von NIS2 wirkt sich nicht nur auf eine größere Anzahl von Unternehmen aus, sondern es diktiert auch umfangreichere Compliance-Anforderungen als je zuvor. Mit NIS2 gelten nun strengere Aufsichtsmaßnahmen und Durchsetzungsanforderungen sowie härtere Sanktionen, sodass die betroffenen Unternehmen dringend entsprechende operative und strategische Änderungen vornehmen müssen.

Diese Unternehmen befassen sich nun mit den komplexen neuen Verpflichtungen der NIS2 in den Bereichen Risikomanagement, Vorfallmeldung, Lieferkettensicherheit, Governance und Informationsaustausch. Dabei haben viele von ihnen Schwierigkeiten, ihren Klassifizierungsstatus zu verstehen, ihre aktuelle Sicherheitslage im Kontext der neuen Anforderungen zu bewerten oder festzustellen, welche Änderungen an ihren bestehenden Cybersicherheitsprogrammen erforderlich sind. Die Ausweitung des Geltungsbereichs der Compliance-Anforderungen bedeutet, dass nun Tausende zusätzlicher

Geldstrafe von **2%** des weltweiten Jahresumsatzes bei Nichtkonformität¹

67% Persönliche Haftbarmachung bei grober Fahrlässigkeit²

¹ <https://nis2directive.eu/nis2-fines/>

² <https://www.dlapiper.com/en-us/insights/publications/derisk-newsletter/2024/nis2-directors-personal-liability-for-lack-of-compliance-is-a-warning-message>

Wichtigste Vorteile

- **Transparenz über Sicherheitsrisiken.**
Sie erhalten einen beispiellosen Einblick in das Human Risk innerhalb Ihres Unternehmens – basierend auf dem Verhalten Ihrer Benutzer und realen Bedrohungen.
- **Adaptive Maßnahmen**
Um unsicherem Verhalten vorzubeugen, können Sie Nutzern punktuell entsprechende Rückmeldungen geben und ergänzend dazu ein ansprechendes Schulungsangebot bereitstellen.
- **Proaktive Kontrollmaßnahmen.**
Um das Human Risk über Ihre gesamte Sicherheitslandschaft hinweg zu minimieren, helfen wir Ihnen, Ihre Nutzer durch angepasste Kontrollmaßnahmen besser zu schützen.

Unternehmen Cybersicherheitsvorschriften einhalten müssen, darunter viele, die mit derart umfassenden Anweisungen noch nie zuvor konfrontiert waren. Besonders komplex ist diese Herausforderung dadurch, dass die erforderlichen Anpassungen gleich über mehrere interne Interessengruppen und externe Lieferanten hinweg koordiniert werden müssen. Das verlangt den betroffenen Unternehmen erhebliche operative und technische Fähigkeiten ab. Ohne die richtige Vorbereitung und fachkundige Beratung riskieren sie beträchtliche Strafen, Reputationsschäden und Betriebsunterbrechungen.

Lösung

Viele Unternehmen leiden zunehmend unter einer dreifachen Belastung: Sie müssen die Anforderungen der NIS2-Richtlinie erfüllen, ihre betriebliche Effizienz aufrechterhalten und ihre Sicherheitslage verbessern. Diesen Unternehmen bietet Mimecast eine integrierte Sicherheitsplattform, damit sie ihre Compliance mit den sieben kritischen Bereichen der NIS2 durch einen einheitlichen, leicht zu koordinierenden Ansatz gewährleisten können. In unserem umfassenden Lösungsangebot kombinieren wir effektive Richtlinienkontrollmaßnahmen mit fortschrittlichen Funktionen zum Vorfallmanagement, damit Sie Bedrohungen schnell erkennen und abwehren können. Wir stellen Ihnen zuverlässige E-Mail-Sicherheitslösungen zur Gewährleistung Ihrer Geschäftskontinuität zur Verfügung ebenso wie Kontrollmaßnahmen für Ihre Lieferkette, damit Sie Risiken durch die Zusammenarbeit mit Drittanbietern effektiv handhaben können. Durch ansprechende Sicherheitsbewusstseins Schulungen helfen wir Ihnen, Ihre Belegschaft von einer potenziellen Schwachstelle in eine starke Verteidigungslinie zu verwandeln. Des Weiteren ermöglicht Ihnen unsere Plattform die kontinuierliche Durchführung von Sicherheitstests und -audits, mit denen Sie die Wirksamkeit Ihrer Kontrollmaßnahmen validieren können, während wir mit unseren modernen Verschlüsselungsverfahren sensible Daten zuverlässig schützen. Dieser integrierte Ansatz vereinfacht Unternehmen nicht nur die Einhaltung der NIS2-Vorschriften, sondern bietet ihnen auch einen messbaren Mehrwert, da sie damit ihre Risiken reduzieren, ihre Sicherheit erhöhen und einen sicheren, unterbrechungsfreien Geschäftsbetrieb erzielen. Durch die Partnerschaft mit Mimecast erhalten Unternehmen mehr als nur eine Technologielösung: Sie gewinnen einen vertrauenswürdigen Berater, der sich dem Schutz ihrer Kommunikation, Daten und Abläufe vor immer ausgeklügelteren Cyberbedrohungen verschrieben hat und sie gleichzeitig bei der Einhaltung ihrer NIS2-Anforderungen unterstützt.

NIS2-Compliance leicht gemacht: Der Vorteil von Mimecast

Die NIS2-Richtlinie schreibt sieben Grundsäulen zur Stärkung der EU-Cybersicherheitslandschaft vor, die zusammengenommen eine effektive Verteidigungslinie gegen moderne Cyberbedrohungen bilden. Diese sieben miteinander verbundenen Säulen schaffen ein robustes Sicherheitsrahmenwerk durch: Risikoanalysen und Systemsicherheitsrichtlinien, Protokolle für das Vorfallmanagement, Maßnahmen zur Gewährleistung der Geschäftskontinuität, Kontrollmaßnahmen für Lieferketten, umfassende Sensibilisierungsschulungen, regelmäßige Sicherheitstests und -audits sowie starke kryptografische Schutzmaßnahmen. Indem sie sich an diesem Rahmenwerk orientieren, können Unternehmen dauerhaft eine starke Cyber Resilience aufbauen und gleichzeitig die erweiterten Compliance-Anforderungen der NIS2 erfüllen. Im Endeffekt schützen sie dadurch ihre wichtigsten Assets und Abläufe vor immer raffinierteren digitalen Bedrohungen.

Über unsere integrierte Sicherheitsplattform bieten wir Ihnen einen umfassenden Schutz für alle sieben NIS2-Säulen, sodass Ihre regulatorischen Anforderungen zu praktischen Sicherheitsvorteilen werden, mit denen Sie Ihre Unternehmenskommunikation schützen, Ihre Compliance stärken und eine dauerhafte Cyber Resilience aufbauen.

Richtlinien

NIS2 schreibt umfassende Kontrollmaßnahmen für die Sicherheit von E-Mail-Systemen vor: Unternehmen müssen eine starke Verschlüsselung durchsetzen, sichere Authentifizierungsmechanismen anwenden und Schutzmaßnahmen gegen fortschrittliche Bedrohungen umsetzen. Besonders wichtig sind diese Sicherheitsvorkehrungen für kritische Systeme, die durch E-Mail-Angriffe infiltriert werden könnten. Unternehmen benötigen demnach ein mehrschichtiges E-Mail-Sicherheitskonzept mit einer kontinuierlichen Evaluierung ihrer Sicherheitslage, um sich vor fortschrittlichen E-Mail-Bedrohungen wie Phishing und Business Email Compromise zu schützen.

Incydr stellt Unternehmen umfassende Datenschutz- und Risikomanagementfunktionen bereit, die auch den Anforderungen von NIS2 gerecht werden. Durch eine Echtzeitüberwachung und fortschrittliche Bedrohungserkennung bietet Incydr Ihnen eine kontinuierliche Einsicht in die Datenbewegungen in Ihrer digitalen Umgebung, damit Sie potenzielle Risiken identifizieren und abwehren können, bevor diese sich zu ernsthaften Vorfällen entwickeln.

Reaktion auf Vorfälle

Unsere Lösungen für die Vorfalleaktion geben Ihrem Unternehmen wirksame Sicherheits- und Compliance-Funktionen an die Hand, die Sie zur Erfüllung der neuen NIS2-Vorgaben benötigen. Die integrierte Mimecast-Lösungssuite umfasst Analysis and Response, Internal Email Protect und Mimecast Email Incident Response (MEIR). Sie profitieren damit von einer kontinuierlichen Überwachung der jeweils aktuellen Bedrohungslage Ihrer E-Mail-Kanäle und einer schnellen Beseitigung von E-Mail-basierten Bedrohungen. MEIR rationalisiert Ihre Sicherheitsabläufe, indem es eine automatisierte Triage mit einer Validierung durch (menschliche) Experten kombiniert, um die Arbeitsbelastung Ihrer Sicherheitsteams erheblich zu reduzieren, ohne Abstriche bei der Erkennungsgenauigkeit zu machen. Durch die nahtlose Integration mit Orchestrierungsplattformen automatisieren wir Reaktions-Workflows, um Bedrohungen zu beseitigen, Richtlinien zu aktualisieren und eine entsprechende Dokumentation zu generieren. Dadurch wird ein einheitliches und effizientes Bedrohungsmanagement gewährleistet.

Incydr bietet Ihnen umfassende Einblicke in die Bewegungen Ihrer Daten sowie in potenzielle Bedrohungen und unterstützt Sie dadurch dabei, die strengen Meldeanforderungen von NIS2 zu erfüllen. Auch unser integriertes Fall-Management-System vereinfacht Ihnen die Compliance mit der Richtlinie, indem es Sicherheitsfunktionen, die traditionell von mehreren Tools ausgeführt werden, auf einer Plattform konsolidiert. Dadurch kann sich Ihr Sicherheitsteam auf seine strategischen Initiativen konzentrieren, anstatt komplexe Berichtsprozesse verwalten zu müssen.

Kontinuität

Continuity garantiert Ihnen einen unterbrechungsfreien Zugriff auf Ihre Kommunikationssysteme während geplanter und ungeplanter Ausfallzeiten – unterstützt durch geografisch verteilte Rechenzentren und abgesichert durch ein SLA mit 100 % Serviceverfügbarkeit –, während Sync and Recover eine schnelle Wiederaufnahme des Betriebs nach versehentlichem Datenverlust oder Angriffen ermöglicht. Diese Lösung ist besonders nützlich bei E-Mail-basierten Bedrohungen wie Ransomware, denn sie bietet dank konfigurierbarer Aufbewahrungsrichtlinien eine schnelle, detaillierte Wiederherstellung von Postfächern, Kalendern und Aufgaben.

Lieferkette

Advanced Business Email Compromise (BEC) ist Ihre Verteidigungslinie gegen ausgeklügelte Angriffe auf die Lieferkette. Diese Lösung verwendet maschinelles Lernen und die Verarbeitung natürlicher Sprache, um Kommunikationsmuster zu analysieren und betrügerische Aktivitäten zu blockieren, bevor sie Ihren Geschäftsbetrieb beeinträchtigen. Um diese Verteidigungslinie weiter zu stärken, nutzen wir die Transport-Layer-Security(TLS)-Verschlüsselung und DNS-based Authentication of Named Entities (DANE) für eine durchgängige Absicherung und Authentifizierung Ihres E-Mail-Verkehrs.

Schulung

Durch gezielte Schulungen und Risikobewertungen verwandelt Mimecast Engage potenzielle Sicherheitslücken in organisatorische Stärken. Unsere Lösung für den Umgang mit Human Risk bietet Ihnen detaillierte Einblicke in das Verhalten und die Risikoprofile Ihrer Mitarbeiter und nutzt Ihre Sicherheitstools, um mit maßgeschneiderten Schulungen – die kontinuierlich an neue Bedrohungen angepasst werden – das Sicherheitsbewusstsein Ihrer Belegschaft zu schärfen.

Kryptographie

Mit Transport Layer Security (TLS 1.2 und 1.3) wird Ihre Kommunikation während der Übertragung automatisch verschlüsselt. Ergänzend dazu wenden wir das Protokoll DNS-based Authentication of Named Entities (DANE) an, das anhand von DNSSEC die Authentizität von E-Mail-Servern überprüft und Man-in-the-Middle-Angriffe verhindert. Für Unternehmen mit sehr hohen Sicherheitsanforderungen unterstützen wir außerdem die PGP- und OpenPGP-Standards mit intuitiver Schlüsselverwaltung, damit Sie von einer echten End-to-End-Verschlüsselung profitieren, ohne Ihr IT-Team unnötig zu belasten.

Darüber hinaus sind unsere Tools darauf ausgelegt, Ihre Anforderungen bezüglich des Auditings, der integrierten Protokollierung und des Bedrohungsaustauschs zu unterstützen, damit Ihr Unternehmen jetzt und in Zukunft regelkonform agiert. Durch eine Partnerschaft mit Mimecast können Unternehmen ihre Compliance mit der NIS2-Richtlinie sicherstellen und gleichzeitig die digitale Resilienz ihres Betriebs stärken.

ÜBER MIMICAST

Mimecast ist eine KI-gestützte, API-fähige und vernetzte Human Risk Management-Plattform. Sie wurde entwickelt, um Unternehmen vor dem gesamten Spektrum von Cyberbedrohungen zu schützen. Dafür integriert sie moderne, benutzerfreundliche Technologie mit Strategien für das Erkennen von Risiken und den Aufbau von Sicherheitskompetenz, die immer den Nutzer im Fokus behalten. Darauf ausgelegt, unsichtbare Risiken sichtbar zu machen und Dateneinblicke so aufzubereiten, dass sie als Entscheidungsgrundlage dienen können, eröffnet sie Unternehmen proaktive Handlungsmöglichkeiten. Sie hilft, Kommunikations- und Kollaborationslandschaften zu schützen, kritische Daten zu sichern, Mitarbeiter aktiv in das Risikomanagement einzubeziehen und eine Sicherheitskultur zu fördern, die mit Unternehmenszielen wie Geschäftskontinuität und Steigerung der Produktivität in Einklang steht. Über 42.000 Unternehmen weltweit vertrauen Mimecast, um der sich dynamisch entwickelnden Bedrohungslandschaft einen Schritt voraus zu sein. Von internen Risiken bis hin zu externen Gefahren – Mimecast bietet Kunden mehr. Mehr Sichtbarkeit. Mehr Einblicke. Mehr Agilität. Mehr Sicherheit.