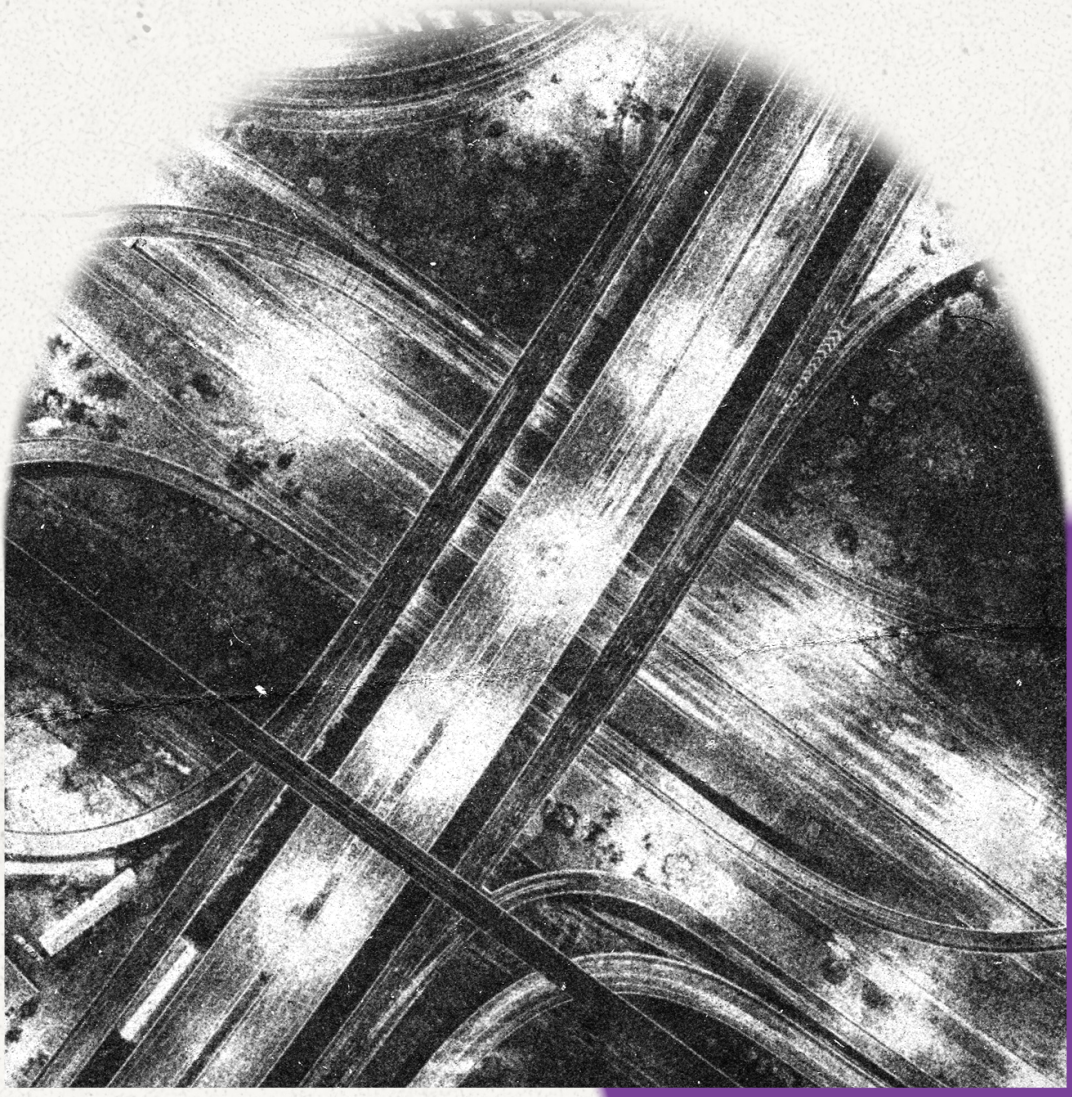
mondoo

AUFBAU EINES DORA-KONFORMEN SCHWACHSTELLENMANAGEMENT-PROGRAMMS

VON PERIODISCHEN SCANS ZU KONTINUIERLICHER RESILIENZ



EINLEITUNG

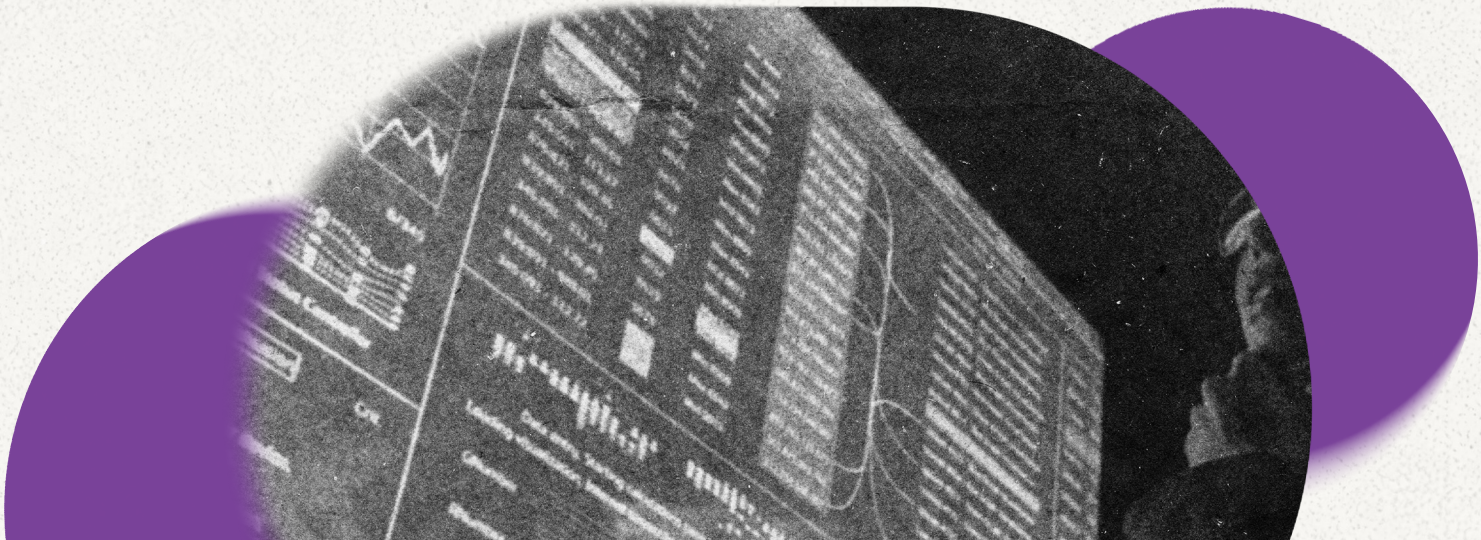
Seit DORA im Januar 2025 verbindlich gilt, bietet der Digital Operational Resilience Act (DORA) Finanzinstituten einen Rahmen, um ihre Cybersicherheit und operationale Resilienz zu stärken.

Anstatt sich auf jährliche Audits oder punktuelle Compliance-Übungen zu verlassen, verlangt DORA von Organisationen, kontinuierlich Nachweise ihrer Resilienz vorzuhalten. Das bedeutet: Sicherheitsteams müssen die Wirksamkeit ihrer Kontrollen jederzeit belegen können und Prüfern auf Abruf präzise, aktuelle Nachweise liefern – statt kurz vor einer Prüfung hektisch die Dokumentation zusammenzustellen.

Im Kern hat DORA kein neues Compliance-Problem geschaffen, sondern eine Herausforderung im Exposure-Management, die Organisationen bewältigen müssen. Der Schwerpunkt hat sich verlagert: weg vom Nachweis, dass Kontrollen existieren, hin zum Nachweis, dass sie dauerhaft wirksam sind und das Risiko in zunehmend komplexen Umgebungen tatsächlich senken.

Eine der größten Veränderungen ist der Übergang vom periodischen Schwachstellen-Scanning zum kontinuierlichen Schwachstellenmanagement. Daten von Mondoo zeigen, dass Organisationen mit kontinuierlichen Ansätzen die mittlere Behebungszeit (MTTR) auf unter 16 Tage senken können. Im Vergleich dazu führt herkömmliches periodisches Scanning häufig zu deutlich längeren Behebungszyklen – bedingt durch manuelle Ticketerstellung, Kontextwechsel und Verzögerungen im Reporting.

Die meisten Sicherheitsprogramme waren nie darauf ausgelegt, kontinuierliche Nachweise zu erzeugen. Dieser Leitfaden zeigt Schritt für Schritt, wie sich ein Programm aufbauen lässt, das den Erwartungen von DORA gerecht wird und zugleich die gesamte Cyber-Resilienz verbessert.



WAS DORA TATSÄCHLICH VERLANGT

Werfen wir zunächst einen Blick darauf, was DORA beinhaltet. Beschrieben als „Verordnung der Europäischen Union zur Stärkung der digitalen Resilienz von Finanzunternehmen“, soll sie diese Finanzdienstleister vor IKT-bezogenen Vorfällen schützen – einschließlich Maßnahmen zu Schutz, Erkennung, Eindämmung, Wiederherstellung und Behebung.

DORA gibt ausdrücklich vor: IKT-Risikomanagement, die Meldung von Vorfällen und Resilienztests. Seine fünf Säulen lauten:

IKT-RISIKOMANAGEMENT **TESTS DER DIGITALEN OPERATIONALEN RESILIENZ**

MANAGEMENT VON IKT-VORFÄLLEN **MANAGEMENT VON IKT-DRITTPARTEIENRISIKEN**

VEREINBARUNGEN ZUM INFORMATIONSAUSTAUSCH

Unter den 64 Artikeln finden sich zwei mit zentralen Anforderungen zu Erkennung sowie Schutz und Prävention. Artikel 9 verlangt von Finanzunternehmen, über periodische Sicherheitsbewertungen hinauszugehen und ihre IKT-Systeme stattdessen kontinuierlich zu überwachen, zu verwalten und zu schützen.

Er verlagert die IKT-Sicherheit von einer reaktiven, punktuellen Tätigkeit hin zu einer fortlaufenden operativen Disziplin, die Cyberrisiken reduzieren und die operationale Resilienz jederzeit aufrechterhalten soll.

Der Artikel schreibt die Umsetzung von Sicherheitsrichtlinien, -verfahren, -tools und -kontrollen vor, um die Resilienz, Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von Systemen und Daten sicherzustellen – insbesondere jener, die kritische Geschäftsfunktionen unterstützen.

Ebenso verlangt dieser Artikel die Einrichtung robuster Zugriffskontrollen, starker Authentifizierung, netzwerkbezogener Sicherheitsmaßnahmen, Verschlüsselung, Prozesse für das Patch- und Schwachstellenmanagement sowie formaler Verfahren für das Änderungsmanagement.

Artikel 10 wiederum legt fest, dass Finanzunternehmen über Mechanismen verfügen müssen, um anomale Aktivitäten umgehend zu erkennen – einschließlich Leistungsproblemen im IKT-Netzwerk und IKT-bezogener Vorfälle. Zudem sind sie verpflichtet, ausreichende Ressourcen und Fähigkeiten bereitzustellen, um Nutzeraktivitäten, das Auftreten von IKT-Anomalien und IKT-bezogene Vorfälle zu überwachen.

Darüber hinaus schreibt Artikel 10 vor, dass Finanzunternehmen formale Verfahren für das Schwachstellen- und Patch-Management entwickeln und dokumentieren müssen. Dazu gehört die Einrichtung von Verfahren, die die Identifizierung, das Testen und die Bereitstellung von

Software- und Hardware-Fixes erleichtern. Diese Verfahren müssen festlegen, wie Patches und andere risikomindernde Maßnahmen priorisiert werden, um identifizierte Schwachstellen zu beheben.

Zudem verpflichtet er Organisationen, erkannte Schwachstellen in ihren IKT-Systemen formell zu dokumentieren sowie deren Behebung zu überwachen und zu verifizieren.

> Der entscheidende Unterschied bei DORA ist, dass es Ergebnisse misst, keine Aktivitäten: Einen Scan durchzuführen ist beispielsweise eine Aktivität, die Schwachstelle zu schließen ist ein Ergebnis. Aufsichtsbehörden wie die BaFin wollen den Nachweis des Letzteren sehen – und dass es korrekt erfolgt ist.

WO DIE MEISTEN PROGRAMME ZU KURZ GREIFEN

Das Problem ist, dass viele periodische Scans auf den Zeitpunkt des Audits ausgerichtet sind und nicht auf den DORA-Rahmen. Im jüngsten Fall einer europäischen Bank existierte – bevor sie Mondoo auf ihrem Weg zur DORA-Konformität einsetzte – zwar ein risikoorientierter Schwachstellenmanagement-Prozess, ebenso jedoch eine manuelle Erfassung von Key-Risk-Indikatoren und Excel-Tabellen, um den Überblick zu behalten.

Es gab zu viele Medienbrüche zwischen Systemen, manuelle, Excel-basierte Workflows, wo Automatisierung hätte bestehen sollen, und eine Methodik, die eine Aufsichtsbehörde nicht von einem Schritt zum nächsten nachvollziehen konnte.

Die Bank verfügte jedoch über keinerlei Härtungs-Baselines: Die Kennzahlen in ihrem Informationssicherheits-Managementsystem waren schwach und rudimentär, und Key-Risk-Indikatoren wurden von Hand zusammengestellt. Nichts davon würde einer DORA-Prüfung standhalten. Mit Mondoo konnte die Bank kontinuierliche Nachweise erbringen und die Anforderungen des Exposure-Managements erfüllen.

Die Ergebnisse stammen aus Mondoo und gelten als verbindliche Grundlage. Sie bieten eine nachvollziehbare Orientierung darüber, wo das Unternehmen im Gesamtbild steht. Dies schuf einen methodisch robusten Nachweisprozess, der für das Unternehmen funktionierte.

Mit einer korrekten Methodik können Unternehmen einem DORA-Prüfer zeigen, was sie gefunden haben. Nur wenige können jedoch tatsächlich belegen, welche Maßnahmen sie ergriffen haben – und die Lücke zwischen „Finden und Beheben“ wird umso größer, je weniger Maßnahmen ergriffen werden.

Zu berücksichtigen sind außerdem blinde Flecken durch die Abhängigkeit von Open-Source- und SaaS-Tools, die jeweils eigene Probleme mit sich bringen. Open-Source-Tools erfordern Patching und Pflege, die häufig von Freiwilligen und gemeinnützigen Organisationen geleistet werden, welche keine dauerhaften Ressourcen dafür bereitstellen. Bei SaaS-Tools und jeder Form geteilter Infrastruktur sollten Sie eine mangelnde Verfügbarkeit bedenken oder wie sich ein Ausfall auf Ihren Betrieb auswirken könnte.

Schließlich veröffentlichte die BaFin zu Beginn dieses Jahres eine Orientierungshilfe zum Einsatz von KI in Finanzunternehmen, um Organisationen dabei zu unterstützen, IKT-Risiken im Einklang mit den DORA-Anforderungen zu steuern. Sie erkannte an, dass Implementierung und Betrieb von KI-Systemen erhebliche Risiken bergen können – insbesondere aus regulatorischer Sicht in Bezug auf Informations- und Kommunikationstechnologie.

Zusätzlich zu spezifischen Schutzmaßnahmen für IKT-Assets ist es entscheidend, KI-Systeme in das bestehende IKT-Risikomanagement-Rahmenwerk einzubeziehen: Aufgrund der oft hohen Komplexität der mathematischen Modelle, der zu verarbeitenden Datenmengen und der Integration von Software externer IKT-Drittanbieter müssen intern wie extern entwickelte KI-Systeme nach denselben Standards analysiert und getestet werden.

FÜNF DINGE, DIE EIN DORA-KONFORMES VM-PROGRAMM HABEN MUSS

Nachdem Sie nun wissen, wie entscheidend ein Schwachstellenmanagement-Programm ist – und zwar eines, das DORA-konform ist –, besteht der nächste Schritt darin, sicherzustellen, dass Inhalte und Abdeckung den Anforderungen entsprechen.

Betrachten wir die fünf Elemente eines DORA-konformen Schwachstellenmanagement-Programms.

Erster Faktor: Vollständige Abdeckung der Umgebung

Das Programm muss die gesamte IKT-Landschaft umfassen – einschließlich Cloud, On-Premise, Endpoints, SaaS, Netzwerkgeräten und CI/CD-Pipelines –, denn DORA gilt für all das. Das erfordert Asset-Erkennung und -Dokumentation, die Fähigkeit, die gesamte internet-exponierte Infrastruktur zu erfassen, damit Angriffsflächen gefunden werden, bevor es ein Angreifer tut, sowie eine Abkehr von punktuellen, periodischen Scans hin zu kontinuierlicher Echtzeitbewertung und agentenlosem Workload Scanning. Ziel ist die kontinuierliche Überwachung aller Assets, ohne dass etwas unentdeckt bleibt.

Zweiter Faktor: Risikobasierte Priorisierung

Diese muss über CVSS-Scores hinausgehen – deren Entstehung und Zuordnung fragwürdig sein können – und die reale Ausnutzbarkeit sowie die Internet-Exposition berücksichtigen. Berücksichtigen Sie außerdem die Kritikalität der Assets und welche Ihrer Assets für Ihre Umgebung am wichtigsten sind und die meisten Probleme verursachen würden, falls sie ausgenutzt würden.

Ebenso, welche Schwachstellen bei einer Ausnutzung das größte Risiko darstellen. Erfordert eine Schwachstelle physischen Zugang zu einem Endpoint oder Server, fragen Sie sich, wie wahrscheinlich das ist. Betrifft ein Exploit eine Komponente, die Sie kaum nutzen, oder liegt er auf einem nicht exponierten Server, wie kritisch ist dann das Einspielen des Patches – und würde das Einspielen den Betrieb überhaupt stören?

Dritter Faktor: Behebung, nachverfolgt bis zum Abschluss

Gemeint ist hier der Lebenszyklus-Prozess des Identifizierens, Priorisierens, Zuweisens und Verifizierens der Behebung von Sicherheitsschwachstellen. Die Nachverfolgung der Behebung stellt sicher, dass Lücken weder offen bleiben noch ohne unabhängige Validierung geschlossen werden – und liefert dem Prüfer auf Anfrage den Beleg, was gefunden und behoben wurde.

Jede gefundene Schwachstelle benötigt einen „Verantwortlichen“ (Owner), jemanden, der dafür rechenschaftspflichtig ist, wie sie gefunden und behandelt wurde. Ebenso braucht es eine Behebungsmaßnahme – was beim Auffinden des Fehlers unternommen und wie er behandelt und an den Eigentümer der Software gemeldet wurde. Zudem ist ein nachverfolgtes Abschlussdatum erforderlich, um zu belegen, wie der Fehler behandelt und letztlich behoben wurde.

Bei der Übergabe an das Engineering geraten die meisten Programme ins Stocken; eine umsetzbare Behebungsanleitung zu jedem Fund beseitigt jegliche Reibung im Prozess.

Vierter Faktor: Kontinuierliche Compliance-Nachweise

Der Audit-Trail muss von selbst entstehen: mit kontinuierlichen, aktuellen Daten und Befunden, die auf Anfrage vorliegen – statt erst als Reaktion auf eine Prüfung zusammengetragen zu werden.

Fünfter Faktor: Reporting auf Vorstandsebene

Das Programm braucht Rückhalt auf Vorstandsebene – und es muss Schwachstellen in

Geschäftsrisiken übersetzen, damit sie dort ernst genommen werden. Besteht eine technische Exposition, muss sie in Geschäftsrisiko übersetzt werden – und zwar in einer Sprache, mit der ein Vorstandsmitglied etwas anfangen kann. Eine rohe CVE-Zahl lässt sich hier daher nicht verwenden; es braucht klare, verständliche und jargonfreie Sprache.

VIERSTUFIGE UMSETZUNGS-ROADMAP

Nachdem die vier Bestandteile, die Ihr Schwachstellenmanagement-Programm enthalten sollte, beschrieben sind, geht es im nächsten Schritt darum, wie es umgesetzt wird und in Betrieb geht. Die vier Phasen bauen aufeinander auf. Planen Sie für jede ausreichend Zeit ein.

PHASE 1 • MONAT 1 - 2

Bestandsaufnahme und Gap-Analyse: In dieser ersten Phase geht es darum, das aktuelle Programm den zuvor genannten fünf Anforderungen gegenüberzustellen. Wie übersetzt sich das, was Sie tun, in die Sprache und das Verständnis der Vorstandsebene? Verfügt es über eine vollständige Abdeckung der Umgebung und kann es Nachweise kontinuierlicher Compliance erbringen?

Nutzen Sie das erste Scan-Ergebnis als Baseline und dokumentieren Sie die Lücken als Nachweis. Bauen Sie in dieser Phase noch keine komplexe Zuordnungsübung auf.

PHASE 2 • MONAT 2 - 4

Erweiterung der Abdeckung: Nutzen Sie diesen Zeitraum, um Abdeckungslücken zu identifizieren und zu schließen, die in der ersten Phase entdeckt wurden. Der Fokus sollte zunächst auf internet-exponierten Systemen liegen und anschließend auf Cloud-Workloads, On-Premise, SaaS- und KI-Assets sowie etwaigen Legacy-Servern oder -Netzwerken.

PHASE 3 • MONAT 3 - 5

Behebungs-Workflow: Nutzen Sie diese Zeit, um die Übergabe identifizierter Schwachstellen an die Entwicklungsteams zu verbessern. Das gelingt mit weniger Reibung, wenn die Daten mit Angaben zu Risikokontext und Zuständigkeit für die Schwachstelle in die Entwickler-Workflows eingespeist werden, um die Behebungszeit zu verkürzen.

Definieren Sie außerdem Service-Level-Agreements nach der Kritikalität der Assets und wissen Sie, welches Asset die meiste Aufmerksamkeit erfordert. Verfolgen Sie schließlich alle Befunde bis zum Abschluss, damit in der Pipeline nichts verloren geht.

PHASE 4 • MONAT 4 - 6

Kontinuierliche Compliance und Reporting: Wohl der kritischste Teil des Prozesses: Hier geht es darum, Nachweise für den Prüfer vorzubereiten, indem eine durchgehend konforme Infrastruktur bereitsteht, die liefert, wonach ein Prüfer sucht.

In dieser Phase liegt der Nachweis auf Knopfdruck vor. Spätestens jetzt sollten Sie die Nachweiserstellung automatisieren und ein vorstandsgerechtes Reporting aufbauen können. Ist das erledigt, sind Sie besser aufgestellt, um ein Programm umzusetzen, eine plötzliche Audit-Anfrage zu bewältigen und sicher zu sein, dass Sie bestmöglich für alle Probleme gerüstet sind.

WIE DAS IN DER PRAXIS AUSSIEHT

Die europäische Bank aus unserem Beispiel entschied sich auf dem Weg zur DORA-Konformität für Mondoo.

Zuvor arbeitete das Unternehmen mit manuell erhobenen Key-Risk-Indikatoren und Excel-basierten Workflows — und kassierte dafür interne Auditbefunde. Ein Audit des IKT-Risikomanagement-Prozesses stellte zu viele Medienbrüche zwischen Systemen fest, manuelle, Excel-basierte Workflows, wo Automatisierung hätte bestehen sollen, und eine Methodik, die eine Aufsichtsbehörde nicht von einem Schritt zum nächsten nachvollziehen konnte.

Sie verfügte zuvor über keinerlei Härtungs-Baselines, die Kennzahlen in ihrem Informationssicherheits-Managementsystem waren rudimentär, und Key-Risk-Indikatoren wurden von Hand zusammengestellt. Nichts davon würde einer DORA-Prüfung standhalten. Mit Mondoo konnte die Bank kontinuierliche Nachweise erbringen und die Anforderungen des Exposure-Managements erfüllen.

Mondoo versorgt das IKT-Governance-Rahmenwerk mit aktuellen Informationen aus der Infrastruktur und gibt dem operativen Team eine risikogewichtete Möglichkeit, Patch- und Schwachstellenmanagement zu priorisieren.

Zudem fließen KRIs und KPIs nun automatisch aus Mondoo in den IKT-Risikomanagement-Prozess und das IKT-Risikoregister; jede Kennzahl hat ein definiertes Profil: wie sie sich zusammensetzt, welchen Zielwert sie hat und wie sie erhoben wird.

Die Bank hatte zudem keine Härtungs-Baselines. Also hat sie die Mondoo-Scan-Ergebnisse zur Vorgabe erklärt: Was Mondoo als Abweichung meldet, definiert im Umkehrschluss den Soll-Zustand. Auf dieser Grundlage kann sie eine nachvollziehbare Orientierung dafür geben, wo sie mit den verschiedenen Systemen im Gesamtbild steht.

Die heutige Situation: ein kontinuierlicher, jederzeit prüfbarer Nachweispfad – und Compliance-Nachweise sind ein Nebenprodukt des täglichen Betriebs.

FAZIT

Was wir hier gelernt haben: DORA hat nicht verändert, was Finanzinstitute gegen Schwachstellen tun müssen – sondern wie konsequent sie es tun, wie breit sie Exposure Management anwenden und wie klar sie es belegen müssen.

Die Schritte werden in diesem Whitepaper ausführlich beschrieben, damit Sie ein konformes Schwachstellenmanagement umsetzen und und jederzeit belastbare Nachweise für den Prüfer vorlegen können.

Mit Mondoo konnte die europäische Bank kontinuierlich über Cloud, On-Premise, Endpoints, SaaS und Netzwerkgeräte hinweg scannen, sich von manuellen Prozessen lösen und einen kontinuierlichen, jederzeit prüfbaren Nachweispfad vorhalten.

Mit einem automatisierten Audit-Trail war sie jederzeit bereit für ein Audit und zur Vorlage von Nachweisen.

Mit risikobasierter Priorisierung und bis zum Abschluss nachverfolgter Behebung sind Sie auf gutem Weg, den Vorgaben von DORA zu entsprechen und den Anforderungen eines Prüfers gerecht zu werden – ohne größere Umwälzung Ihrer Arbeitsweise.