mondoo

CASE STUDY

KONTINUIERLICHE SICHERHEIT, KONTINUIERLICHE COMPLIANCE

Wie eine etablierte europäische Bank DORA-Nachweise zum Nebenprodukt ihrer täglichen Sicherheitsarbeit gemacht hat – jederzeit auf Knopfdruck belegbar.

DORA hat für Europas Banken kein Compliance-Problem geschaffen, sondern eine Herausforderung im Exposure Management. Institute, die die Verordnung als reine Dokumentationsübung verstanden haben, bauten Frameworks, Richtlinien und Register, die auf das Bestehen einer Prüfung ausgelegt waren.

Wer sie richtig gelesen hat, baute etwas anderes: ein kontinuierliches Betriebsmodell, das Compliance-Nachweise als Nebenprodukt guter Sicherheitsarbeit hervorbringt. Die Bank in dieser Case Study gehört zur zweiten Gruppe – und Mondoo liefert einen zentralen Baustein dieses Modells.

UF EINEN BLICK

ORGANISATION: Eine etablierte europäische Bank

SEKTOR: Regulierte Universalbank für Privat-und Firmenkunden in der EU

GRÖSSE: Europäische Bank mit einer Bilanzsumme im Milliardenbereich und einem weitverzweigten Filialnetz

REGION: Europäische Union

ENVIRONMENT: Rund 70 bis 75 Prozent on-premises. VMware, Windows- und Linux-Server, Windows- und Mac-Endgeräte. Das Kernbankensystem läuft über einen gemeinsamen IT-Dienstleister der Gruppe.

SICHERHEITSFUNKTION: Im Kern ein Head of Security, ein kleines Team und externe Berater

MONDOO'S ROLLE: Zentrale Plattform für DORA-konforme Nachweise zur IKT-Governance und für Continuous Threat Exposure Management (CTEM)

01
DIE BANK

EINE REGULIERTE BANK, DIE IHRE IT SELBST BETREIBT

Diese Case Study beschreibt eine etablierte europäische Bank: ein reguliertes Institut mit einer Bilanzsumme im Milliardenbereich und einem weitverzweigten Filialnetz. Sie betreut Privat- und Firmenkunden und gehört zu einer größeren Bankengruppe, deren Mitglieder zentrale Dienste und Infrastruktur gemeinsam nutzen.

Anders als viele kleinere Institute, die den Großteil ihrer IT vom gemeinsamen Dienstleister der Gruppe beziehen, betreibt diese Bank einen großen Teil ihrer Infrastruktur selbst: das gesamte LAN, WAN und SD-WAN, den kompletten Security-Stack vom Endgerät bis zum Perimeter, den Rechenzentrumsbetrieb, die Storage-Virtualisierung und die Telekommunikation. Rund 70 bis 75 Prozent davon liegen nach wie vor on-premises – auf Basis von VMware, mit Windows- und Linux-Servern sowie Windows-und Mac-Endgeräten. Die Sicherheitsfunktion ist schlank aufgestellt: ein einziger Head of Security, unterstützt von einem kleinen Team und externen Beratern

02
DIE HERAUS-FORDERUNG

DORA HAT DIE FRAGE VERÄNDERT

Für den Head of Security der Bank ist die größte Bedrohung dieselbe geblieben: ein erfolgreicher Angriff – meist Ransomware –, der den Geschäftsbetrieb zum Stillstand bringt, weil die Systeme nicht mehr verfügbar sind. Verändert hat sich der Maßstab, an dem er gemessen wird. Für Banken hat DORA Vorrang: Inhaltlich überschneidet sie sich weitgehend mit der breiter angelegten NIS2.

Richtlinie, doch als finanzsektorspezifische Regelung ist sie für Banken maßgeblich. Ihre Artikel zum IKT-Risikomanagement legen konkret fest, was zu tun ist und in welcher Qualität – mit der impliziten Erwartung, dass sich Unternehmen an anerkannten Frameworks wie der ISO-27001-Familie und NIST orientieren,

> “Sie haben vier Excel-Tabellen, und irgendwann fließt daraus etwas ins operationelle Risiko – aber wir können nicht nachvollziehen, wie Sie von A nach B kommen. Bitte erklären Sie das.”

DIE PRÜFUNGSFES STELLUNG, SO WIE DER HEAD OF SECURITY DIE POSITION DER AUFSICHT BESCHREIB

ergänzt um die technischen Vorgaben der nationalen Cybersicherheitsbehörde.

Konkret wurde der Druck durch die verpflichtende Jahresprüfung der Bank. Diese wird nicht von einer Big-Four-Gesellschaft durchgeführt, sondern von ihrem externen Prüfungsverband – und sie schließt die IT-Prüfung ein. Die Prüfungsfeststellung bemängelte die fehlende Transparenz und Nachvollziehbarkeit des IKT-Risikomanagementprozesses und seiner Übergabe an das operationelle Risiko. Zu viele Medienbrüche zwischen den Systemen, manuelle, Excel-basierte Abläufe, wo Automatisierung längst hätte greifen müssen, und eine Methodik, die die Aufsicht nicht Schritt für Schritt nachvollziehen konnte.

Hinter der Feststellung steckte eine unbequemere Wahrheit über den Ausgangspunkt. Die Bank hatte überhaupt keine Härtungs-Baselines. Die Kennzahlen in ihrem Informationssicherheits-Managementsystem waren, in den Worten des Head of Security, schwach, rudimentär und spärlich. Key Risk Indicators (KRI) wurden von Hand zusammengetragen. Nichts davon hätte einer DORA-Prüfung standgehalten – und allen Beteiligten war das klar.

03
DIE LÖSUNG

EINE PLATTFORM ALS DREHSCHEIBE

Der Head of Security der Bank beschreibt Mondoo als die zentrale Drehscheibe, an der alles andere zusammenläuft. Seinen Nutzen sieht er in zwei Hälften, die beide aus einer einzigen Single Source of Truth gespeist werden. Zum einen versorgt die Plattform das IKT-Governance-Framework mit konkreten, aktuellen Informationen aus der Infrastruktur. Zum anderen gibt sie dem operativen Team eine risikogewichtete Grundlage, um Patch-und Schwachstellenmanagement zu priorisieren – wobei eine Jira-Integration die Behebung direkt in den bestehenden Workflow überführt. Entscheidend dabei: Die Frameworks und ihre Kontrollen sind als nachvollziehbarer Code in der Plattform hinterlegt. Es gibt also keine Mapping-Tabellen zu erstellen und keine Herleitungen von Hand zu dokumentieren.

HÄRTUNG, UMGEKEHRT GEDACHT

Am deutlichsten zeigt sich das bei der Härtung. Ohne Baselines als Ausgangspunkt drehte das Team die übliche Reihenfolge um: Man nimmt, was die Plattform prüft, erklärt das zur Anforderung und validiert anschließend jede Prüfung an der realen Umgebung. Lässt sich eine Kontrolle tatsächlich nicht erfüllen, weil ein Dienstleister der Gruppe eine Einstellung fest vorgegeben hat, auf die die Bank keinen Einfluss hat – etwa eine auf 10 Zeichen fixierte Mindestpasswortlänge gegenüber dem CIS-Level-2-Benchmark von 13 –, wird die Prüfung mit dokumentierter Begründung entfernt. So bleibt die Bank aufsichtsrechtlich konform – und das Bild ihrer Sicherheitslage zugleich ehrlich. Aus der Lücke heraus kann das Team seine Position risikogewichtet einordnen, Maßnahmen zur Behebung ableiten und regelmäßig sowie nachvollziehbar darüber berichten.

ENNZAHLEN ALS NEBENPRODUKT

Dieselbe Disziplin zieht sich durch die Kennzahlen. KRIs und KPIs fließen heute automatisch aus Mondoo in den IKT-Risikomanagementprozess und das IKT-Risikoregister. Jede Kennzahl hat ein definiertes Profil: wie sie sich zusammensetzt, welcher Zielwert gilt und wie sie erhoben wird – jedes Mal auf dieselbe automatisierte, standardisierte und nachvollziehbare Weise. Was früher Handarbeit war, ist heute ein Nebenprodukt davon, dass die Plattform einfach ihre Arbeit tut.

Agentische Automatisierung ist es, die dies in dem Umfang und Tempo möglich macht, das DORA voraussetzt. Zugleich sagt er offen: Urteilsvermögen lässt sich nicht wegautomatisieren. Zu entscheiden, welche Prüfungen für eine bestimmte Umgebung gelten, Ergebnisse zu validieren und über Ausnahmen zu urteilen – das ist Arbeit, die weder ein Tool noch eine KI abnehmen kann. Das ist keine Schwäche des Modells. Das ist die Kontrolle. Die Plattform liefert Nachweise in großem Umfang, und ein Mensch bleibt verantwortlich dafür, was sie bedeuten und welche operativen Änderungen daraus folgen – genau die Nachvollziehbarkeit, die die Aufsicht verlangt.

04
ONBOARDING & ERKENNTNISSE

MIT EINEM ASSET-TYP BEGINNEN

Systeme und Infrastruktur in die Plattform zu bekommen, war – in seinen Worten – ein Kinderspiel. Der eigentliche Aufwand liegt, wie bei jedem ernstzunehmenden Werkzeug im Cyber- und Compliance-Umfeld, im Feintuning: zu entscheiden, welche Benchmarks für welche Systeme gelten, einzelne Prüfungen zu validieren und die Ergebnisse auf die Umgebung zuzuschneiden. Sein Rat an neue Kunden: der Versuchung widerstehen, alles auf einmal zu onboarden. Mit einem Asset-Typ anfangen – Windows-Endgeräte sind ein sinnvoller erster Kandidat. Verstehen, was die Plattform einem sagt, und erst dann erweitern.
Wer gleich zu Beginn alles auf einmal will, verzettelt sich.

Diese Darstellung ist ehrlich, nicht geschönt – deshalb gehören auch die Reibungspunkte hierher. Weil die Agenten ihre Updates aus dem Internet beziehen, hat der Endpoint-Schutz der Gruppe etwas dagegen. Die Bank kann daher kein automatisches Update nahezu in Echtzeit nutzen und spielt Updates stattdessen über die standardmäßige Softwareverteilung in einem langsameren Rhythmus aus. Es funktioniert, aber eben nicht automatisch. Hinzu kam ein einmaliges Reporting-Problem – Berichte wurden nicht erzeugt –, das im Rahmen des normalen Supportprozesses behandelt wurde. Und Mondoo ist keine vollständige End-to-End-GRC-Plattform – und will das auch nicht sein. Positiv hervorgehoben wurden das Entwicklungstempo, die neuen Integrationen und die durchweg kurzen Reaktionszeiten. Zur Kunden-Anbieter-Beziehung äußert sich der Head of Security unmissverständlich: rundum zufrieden.

05
ERGEBNISSE

OM FINDEN ZUM BEHEBEN

Das messbare Ergebnis ist ein deutlich rückläufiger Trend bei den identifizierten Schwachstellen, festgehalten in einem früheren Review – getragen davon, dass das Team auf das reagiert, was die Plattform sichtbar macht. Das ist der Teil des Exposure Managements, auf den es am meisten ankommt: der Schritt vom Finden zum Beheben – die Lücke zwischen Entdeckung und Behebung

> MEINER MEINUNG NACH SOLLTE JEDE BANK DAMIT ARBEITEN.
>
> - HEAD OF SECURITY

schließen, statt nur darüber zu berichten.

Das strukturelle Ergebnis wiegt ebenso schwer: eine einzige Methodik und eine einzige Plattform statt zersplitterter, von Medienbrüchen durchzogener Abläufe – mit einem vollständigen Blick über die gesamte Systemlandschaft und nachvollziehbaren Nachweisen auf Abruf. Die Konsolidierung läuft bereits: Der klassische Schwachstellenscanner steht vor der Ablösung, der Wildwuchs an Tools wird reduziert, ein dediziertes Asset Management läuft parallel mit, und die Nachweise für Compliance und Exposure bündeln sich in Mondoo.

1+	**70–75%**	**1** plattform
Personalstärke im Security-Team – ein Head of Security plus Berater –, die das Modell betreiben	On-premises-Bestand, der kontinuierlich bewertet wird	Eine Methodik ersetzt vier Excel-Tabellen und von Medienbrüchen durchzogene Abläufe

> Wenn der Prüfer kommt, drücke ich auf den Knopf und sage: Hier, so sieht es aus, so sah es letzte Woche aus, so sah es vor vier Wochen aus, das ist der Trend, das tun wir – und so tun wir es."
>
> - HEAD OF SECURITY

06

DORA MAPPING

WIE MONDOO ZUR AUFRECHTERHALTUNG DER DORA-COMPLIANCE BEITRÄGT

Keine einzelne Plattform belegt jede Anforderung von DORA. Bei dieser Bank ist Mondoo die Plattform für die Anforderungen an kontinuierliche Nachweise und Exposure Management, die im Zentrum der Verordnung stehen – und sie liefert Nachweise zu den angrenzenden Anforderungen.

PRIMÄR	
ART. 9	Schutz und Prävention
ART. 10	Erkennung von Exposures, Fehlkonfigurationen und Posture-Drift
ART. 24	Allgemeine Anforderungen an das Testen
ART. 25	Testen von IKT-Tools und -Systemen

UNTERSTÜTZEND	
ART. 5-6	Betriebskennzahlen und KRIs, die in den IKT-Risikomanagementrahmen einfließen
ART. 13	Die Datenbasis hinter Lessons Learned
ART. 28	Sicherheitslage von Drittparteien, soweit erfassbar

ÜBER MONDOO

Führende Branchenanalysten beschreiben Exposure Management heute als Weg von der Sichtbarkeit zur Handlung: die Lücke zwischen dem Entdecken einer Exposure und ihrer tatsächlichen Beseitigung zu schließen, statt bei einem priorisierten Bericht haltzumachen. Sie bezeichnen diesen Wandel als Preemptive Exposure Management – die handlungsorientierte Weiterentwicklung von CTEM. Diese Bank zeigt, wie dieses Modell in einer regulierten, überwiegend on-premises betriebenen EU-Bank aussieht: kontinuierliche Bewertung, Priorisierung nach Geschäftskontext und Behebung – alles auf einer einzigen Plattform nachverfolgt und dokumentiert.

DORA BESTEHT MAN NICHT. MAN MUSS SIE BEWEISEN.

Compliance zu dokumentieren ist das Minimum. Die Fähigkeit, Risiken belastbar zu beheben und zu mindern – kontinuierlich und in großem Maßstab –, schafft operationale Resilienz. Diese Bank ist der Beweis, dass sich das Betriebsmodell des Exposure Managements in einer realen, regulierten Umgebung umsetzen lässt – mit einem Sicherheitsteam von effektiv einer Person plus Beratern. Mondoo schließt die Hälfte der Lücke, die Dokumentation allein nicht schließen kann, und macht aus Nachweisen Resilienz. In genau dieser Reihenfolge.