mondoo

CASE STUDY

REISEZIEL RESILIENZ

Wie ein führender europäischer Reisekonzern 1.000 Assets von AIX bis AWS unter kontinuierliche Prüfung brachte und heute mit dem bestehenden Team am selben Tag den Überblick erhält.

Ein Sicherheitsprogramm fällt nicht zurück, weil ihm der Standard fehlt. Es fällt zurück, wenn der Nachweis Handarbeit bleibt: stichprobenhaft erhoben, exportiert und schon veraltet, bevor ihn jemand liest.

Teams, die das Problem richtig erkannt haben, bauen etwas anderes. Bei ihnen entstehen die Nachweise als Nebenprodukt guter Sicherheitsarbeit und nicht als eigenes Projekt.

Genau das tat der Reisekonzern in dieser Case Study; Mondoo ist die Plattform, auf der diese Nachweise entstehen.

Sechs Personen prüfen heute rund 1.000 Assets, von den geschäftskritischen AIX-Systemen bis zu mehreren AWS-Konten. Die sieben Tage Blindflug zwischen zwei Scans gibt es nicht mehr, die technischen Nachweise für Audits entstehen in Tagen statt in Monaten und jedes AWS-Konto im Rahmen der Prüfung ist heute abgedeckt. Die IT-Landschaft ist gewachsen. Das Team nicht.

AUF EINEN BLICK

ORGANISATION: Führender europäischer Reisekonzern mit mehreren Betriebsgesellschaften

BRANCHE: Reise und Tourismus

GRÖSSE: Sieben Länder, Millionen Reisende pro Jahr, über 2.000 Mitarbeiter

REGION: Europa

UMGEBUNG: Hybrid: On-Premises-Linux, Windows und geschäftskritische AIX-Systeme, dazu mehrere AWS-Konten

SECURITY-TEAM: Sechs Personen für Security Engineering und Security Operations

FRAMEWORKS & RECHTSVORSCHRIFTEN: CIS, PCI DSS, ISO 27001, NIS2, GDPR

ROLLE VON MONDOO: Kontinuierliche Prüfung von Schwachstellen, Konfigurationen und Compliance über die gesamte Infrastruktur

Diese Case Study wurde durch den Kunden geprüft und freigegeben. Der Kunde möchte nicht namentlich genannt werden.

01
DER KONZERN

VERFÜGBARKEIT UND VERTRAUEN SIND DASSELBE PROBLEM

Der Konzern gehört zu den führenden Reiseanbietern Europas, befördert jedes Jahr Millionen Reisende, ist in sieben Ländern aktiv und beschäftigt über ein Portfolio von Gesellschaften über 2.000 Menschen. Seine IT trägt die gesamte Reise des Kunden: am Anfang die Buchungssysteme, dahinter die Koordination, die Reisende ans Ziel bringt und unterwegs betreut.

Sicherheit hat hier zwei Aufträge zugleich. Verfügbarkeit: Ein Ausfall oder ein Angriff kann Buchungen stoppen, die Abwicklung vor Ort stören oder Reisende ohne rechtzeitige Information zurücklassen. Vertrauen: Der Konzern verarbeitet sensible personenbezogene Daten, darunter Namen, Passdaten, Geburtsdaten und Buchungsdaten. Fünf Frameworks und Rechtsvorschriften prägen das Programm, nämlich CIS, PCI DSS, ISO 27001, NIS2 und die DSGVO. Die DSGVO stellt dabei die höchsten Anforderungen, weil die Branche Kundendaten mit Partnern in Drittländern austauschen muss.

Die Vorgabe der Geschäftsführung an das sechsköpfige Security-Team ist klar: das Unternehmen so sicher wie möglich machen, ohne den Betrieb auszubremsen.

02
THE CHALLENGE

EIN SCAN PRO WOCHE, EIN PDF UND SIEBEN TAGE BLINDFLUG

Der alte Prozess bestand aus einzelnen Tools und manueller Nacharbeit. Ein wöchentlicher Scan mit Tenable Nessus erzeugte ein PDF. Jemand sichtete es, übersetzte die Befunde in Tickets, telefonierte den Verantwortlichen hinterher und scannte irgendwann erneut, um zu sehen, ob sich etwas verändert hatte. Für das Remote-Scanning mit Zugangsdaten musste außerdem auf jeder Maschine im Bestand ein hochprivilegiertes Konto eingerichtet und abgesichert werden.

Zwei Probleme verstärkten sich gegenseitig. Verzögerung: Weil der Scan nur wöchentlich lief, konnte eine Schwachstelle bis zu sieben Tage bestehen, bevor sie überhaupt auffiel, und danach

brauchte die Behebung eines kritischen Befunds noch ein bis drei Arbeitstage. Abdeckung: Am größten waren die Lücken bei den geschäftskritischen AIX-Systemen, wo eine tiefe Prüfung externe Spezialisten mehrere Tage pro Stichprobe beschäftigte und der native CIS-Scanner keine brauchbaren Hinweise zur Behebung lieferte. Das Team stützte sich also auf Stichproben und Erfahrung statt auf laufend verifizierte Nachweise.

Auslöser war weder ein Sicherheitsvorfall noch ein gescheitertes Audit. Stattdessen kamen drei Dinge zusammen: ein neu aufgestelltes, bereichsübergreifendes Security-Team, der Auftrag, das Sicherheitsniveau über bisher getrennt arbeitende Teams hinwegzuheben, und die Entscheidung für CIS als praktischen Standard des Konzerns. Diese letzte Entscheidung gab den Ausschlag; sie brauchte einen Weg, der ohne manuelle Erhebung und Stichproben auskommt. Ohne skalierbare Plattform wäre die Wahl gewesen: lückenhafte Abdeckung akzeptieren oder schätzungsweise vier Personen zusätzlich einstellen.

> “Mondoo hat das CIS-Ziel nicht erfunden. Mondoo hat es operativ erreichbar gemacht.”
>
> TEAMLEITER IT-SECURITY

03
DIE ERGEBNISSE

WAS SICH VERÄNDERT HAT, IN ZAHLEN

~1.000 Assets unter kontinuierlicher Prüfung, vorher unter 200	**6** Personen betreiben ein Programm, für das sonst rund vier zusätzliche Stellen nötig gewesen wären	**3** bis **4** Tage für die technischen Nachweise, vorher ein Aufwand von Monaten

	VORHER	MIT MONDOO
Geprüfte Assets	Weniger als 200	Rund 1.000
AWS-Konten	Keine Abdeckung	Alle einbezogenen Konten abgedeckt
Prüfrhythmus	Ein Scan pro Woche, bis zu sieben Tage Blindflug	Kontinuierlich, Reaktion am selben Tag möglich
Technische Nachweise für Audits	Monate, eine frühe Runde fast sieben Monate	rei bis vier Tage für ein- en definierten Prüfumfang
Nötiges Team für diesen Umfang	Geschätzt zehn Personen	Die bestehenden sechs Personen
Grundlage der Nachweise	PDF-Exporte, Tabellen und Stichproben	Aktuelle technische Belege für die gesamte Infrastruktur

Ein Teil des Wachstums bei den geprüften Assets geht auf das Wachstum des Geschäfts zurück. Das klarste geschäftliche Ergebnis ist das Verhältnis: Die Abdeckung ist gewachsen, das Team nicht mit ihr.

04
DIE LÖSUNG

EINE PLATTFORM, EIN AKTUELLES BILD DER GESAMTEN INFRASTRUKTUR

Mondoo prüft die gesamte hybride Infrastruktur: On-Premises-Linux, Windows und AIX über den lokal installierten Mondoo Client, dazu mehrere AWS-Konten. Schwachstellen und Compliance bleiben dabei in einer Plattform statt in getrennten Tools und Abläufen. Drei Dinge entschieden die Wahl.

Open Source im Kern. Die Scan-Komponente cnspec ist Open Source. Das Team kann also nachvollziehen, was in der eigenen

Umgebung tatsächlich läuft, und die Community kann das ebenfalls. Auch die offene Dokumentation half, Deployment und Produktqualität vorab zu bewerten, ohne vorher mit dem Vertrieb sprechen zu müssen.

Ein Deployment, das sich nativ anfühlt. Der Mondoo Client installiert sich über die üblichen Paketmanager wie apt und dnf. Der Rollout fühlte sich dadurch an wie ein Teil der eigenen Linux-Umgebung, nicht wie ein Fremdkörper. Gegenüber Remote-Scannern liefert der lokal installierte Client zudem ein aktuelleres Bild, ohne ein hochprivilegiertes Konto mit Zugangsdaten über den gesamten Bestand zu verteilen.

Eine Plattform für beide Aufgaben. Schwachstellen und Compliance liegen auf denselben Daten; mit wachsender Abdeckung tragen diese Daten inzwischen auch das Reporting, die Asset-Übersicht und neue Automatisierungen.

Ein Anbieter, den das Team erreichen konnte. Der kommerzielle Vergleich war wichtig, die Beziehung wog aber genauso schwer. Das Team konnte direkt mit Engineers sprechen, die wissen, wovon sie reden und ebenfalls mit der Geschäftsführung von Mondoo. Feature-Wünsche konnte es einbringen und wurde damit auch gehört

> “Wir konnten direkt mit Leuten sprechen, die sich auskennen, und Feature-Wünsche loswerden. Man fühlt sich gehört und eben nicht wie einer von Zehntausenden Kunden.”
>
> TEAM LEAD IT SECURITY

DIE CVE-FRAGE, AN EINER STELLE BEANTWORTET

Beim alten Scanner sah die Frage „Sind wir betroffen?“ so aus: das passende Plugin finden, Ziele und Zugangsdaten konfigurieren, scannen, warten, Ergebnisse exportieren und nach dem Patchen alles noch einmal, um zu belegen, dass der Fix sitzt. Mit Mondoo liegt das aktuelle Ergebnis für den gesamten Bestand schon im Tenant. Das Team filtert es, weist Verantwortliche zu und erzeugt die Tickets direkt aus der Plattform. Die Verantwortlichen für die AIX-Systeme arbeiten mit denselben Daten an Härtung und Compliance-Scores. Zwei Dinge überraschten das Team positiv: wie schnell MQL-Abfragen antworten und wie viel operative Arbeit inzwischen an dieser einen Stelle stattfindet.

05
DAS VORGEHEN

MIT DEM ZIEL ANFANGEN, NICHT MIT DEM TOOL

Das Team verglich Rapid7, Tenable Nessus und Qualys sowie agentenbasierte Alternativen, anhand klarer Kriterien: breite Ökosystem- und AIX-Abdeckung, CIS-Fähigkeit, ein schlankes Deployment-Modell, aktuelle Nachweise, brauchbare Hinweise zur Behebung, Transparenz und Kosten. Der Teamleiter IT-Security und der Leiter der IT entschieden gemeinsam, dass ein lokal installierter Client das richtige Modell ist, wohl wissend, dass auch ein solcher Client selbst Teil der Angriffsfläche ist und entsprechend bewertet werden muss.

Den Rest erledigte ein sorgfältig vorbereiteter Proof of Concept. Mondoo fragte, was das Team sehen muss, setzte konkrete Arbeitssitzungen von einer bis anderthalb Stunden an und führte genau diese Abläufe dann auch vor. So passte das Onboarding im Produktivbetrieb zu den Erwartungen aus dem PoC. Die Systeme einzubinden war ungewöhnlich schmerzfrei, weil die Spaces in Mondoo jedem Team den passenden Installationsbefehl geben und die Assets automatisch im richtigen Kontext landen. Der schwierigste Teil war organisatorisch: zu definieren, was 100 % Abdeckung überhaupt heißt, wenn man nicht sicher sein kann, dass die CMDB jedes Asset kennt.

WAS DAS TEAM EINEM KOLLEGEN MITGEBEN WÜRDE

- Mit dem Ziel anfangen, nicht mit dem Tool.
- Damit rechnen, dass das Deployment Schwächen in der CMDB offenlegt. Das ist eine nützliche Information, kein Rückschlag.
- Die Risiko- und Compliance-Scores in den ersten Wochen für Schwung nutzen, wenn Teams ihre eigenen Fortschritte sofort sehen.
- Sich bei der Härtung Zeit lassen. Einen Score über 90 % zu treiben, ohne die betrieblichen Folgen zu verstehen, kann ein System auf dem Papier sicher und in der Praxis unbenutzbar machen.
- Ausnahmen richtig nutzen: dokumentiert, befristet und überprüfbar.

Beim Rückhalt in der Organisation half, dass das Vertrauen der Geschäftsführung schon da war. Das Team stellte Mondoo als Mittel dar, um die CIS- und Sicherheitsziele rechtzeitig und zu vertretbaren Kosten zu erreichen, und wählte den Horizont von drei Jahren bewusst, um genug Anlauf für ein sauberes Deployment zu haben und mit der Plattform zu wachsen.

> “Der Business Case war keine Feature-Liste für ein Jahr. Es ging um tragfähige Abdeckung und um Hebel für das Sicherheitsprogramm.”
>
> TEAM LEAD IT SECURITY

06
THE TAKEAWAY

mondoo.com

email

linkedin

ABDECKUNG LÄSST SICH NICHT PER STICHPROBE BELEGEN. SIE MUSS GEMESSEN WERDEN.

Die ehrliche Einordnung zählt hier genauso viel wie die großen Zahlen. Die Nachweise beruhen heute auf aktuellen technischen Belegen statt auf selbst ausgefüllten Tabellen: Das gibt Security und GRC deutlich mehr Vertrauen in die Ergebnisse. Bei der Behebung ist der Vergleich noch nicht sauber. Die MTTR für kritische Befunde lag zum Zeitpunkt des Interviews bei rund acht Tagen, gerechnet von der Veröffentlichung der CVE bis zur Behebung. Der frühere Prozess kombinierte einen wöchentlichen Scan mit ein bis drei Arbeitstagen für die Behebung, sodass derselbe kritische Befund rund acht bis zehn Tage bis zum Abschluss brauchte. Und das unter der Annahme, dass der Scan ihn überhaupt gefunden hat. Strukturell hat sich vor allem eines geändert: Die sieben Tage Blindflug sind verschwunden. Die Zahlen zur Behebung dürften nachziehen, je reifer das Programm wird.

Mondoo wird außerdem zur führenden Quelle für eine verlässlichere Software- und Security-CMDB; Stakeholder greifen inzwischen selbst auf die Auswertungen zu, statt einen weiteren Scan-Bericht anzufragen, der beim Lesen schon veraltet sein kann. Am meisten zählt für das Team allerdings ein Ergebnis, das keine Zahl ist: der sichere Überblick über fast die gesamte IT-Landschaft, on premises und in der Cloud, aktuell genug, um danach zu handeln. Die technische Grundlage jedes Befunds ist dabei sichtbar, statt aus einem veralteten Bericht oder einer Selbstauskunft abgeleitet zu sein.

DIE IT-LANDSCHAFT IST GEWACHSEN.
DIE REAKTION IST SCHNELLER GEWORDEN.
DIE ARBEITSLAST NICHT.