

Der 30-Sekunden-Kickstart für CISOs

„Verschlüsselt“ bedeutet nicht automatisch „sicher“ – insbesondere dann nicht, wenn kryptografische Risiken nicht verwaltet werden. Beispiele: abgelaufene Zertifikate, veraltete Algorithmen, fest codierte Schlüssel, schwache Verschlüsselung.

Niemand fühlt sich wirklich für Kryptografie verantwortlich – deshalb bleiben Risiken oft unsichtbar, bis es zu spät ist.

Als CISO können Sie nicht jedes versteckte Risiko persönlich aufspüren. Aber Sie können sicherstellen, dass Ihr Team weiß, wo es suchen muss – und wonach.

/// DIE HERAUSFORDERUNG



Stellen Sie sich vor, Sie wachen eines Morgens auf und entdecken, dass die verschlüsselten Daten Ihres Unternehmens ...

offengelegt wurden.

/// SCHNELLSTART-CHECKLISTE:

Kryptografische Transparenz



Erkennung



Inventarisierung



Risikoreduktion



Demokratisierung

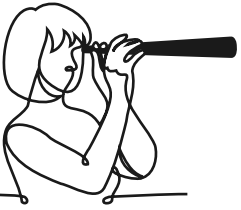


Resilienz

Obwohl diese Schritte nacheinander dargestellt werden, erfolgen Fortschritte häufig parallel – insbesondere bei der Reduzierung kritischer Risiken.

Resilienz ist kein Endzustand, sondern ein fortlaufender Prozess aktiver Verwaltung und Anpassung an Veränderungen.

Erkennung



Scannen Sie Code, Infrastruktur und Netzwerkverkehr nach kryptografischer Nutzung:

- Schlüssel, Zertifikate, Protokolle, Algorithmen, Bibliotheken
- Unverschlüsselte Datenflüsse, schwache Protokolle
- Quellcode, CI/CD-Umgebungen, Endpunkte, Server, Drittanbieter

Kryptografie ist überall – aber oft unsichtbar

Inventarisierung



Zentralisieren Sie Erkenntnisse in einem lebenden Inventar:

- Assets Anwendungen, Systemen und Verantwortlichen zuordnen
- Nutzung, Compliance-Status und Risikostufe verfolgen

Man kann nicht verwalten, was man nicht sehen kann

Risikoreduktion



Identifizieren und priorisieren Sie Risiken mit hohem Gefährdungspotenzial:

- Fest codierte, wiederverwendete oder offengelegte Schlüssel
- Abgelaufene oder langlebige Zertifikate
- Veraltete Algorithmen und Cipher Suites
- Unverschlüsselter oder schwach verschlüsselter Datenverkehr
- Nicht konforme oder proprietäre Kryptografie

Wechseln Sie von der Erkennung zu nachvollziehbaren Maßnahmen

Demokratisierung

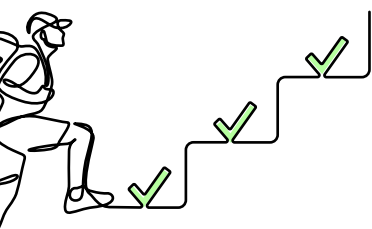


Verankern Sie Verantwortlichkeiten für Kryptographie in Arbeitsabläufen:

- Zertifikats- und Schlüsselmanagement automatisieren
- Klare Richtlinien und Warnmeldungen bereitstellen
- Verantwortlichkeiten teamübergreifend zuweisen

Sicherheit verbessert sich, wenn Kryptografie kein isoliertes Spezialgebiet bleibt

Resilienz



Bauen Sie langfristige Kryptografie-Agilität auf:

- Erneuerungen und Schlüsselrotation automatisieren
- Bereitschaft für Post-Quanten-Kryptografie überwachen
- Richtlinien und Zuständigkeiten regelmäßig überprüfen
- Verantwortliche benennen und über ITSM-/GRC-/CMDB-Tools nachverfolgen

Kryptografische Standards entwickeln sich weiter – Ihre Reaktion muss das ebenfalls tun

"Was haben wir?"

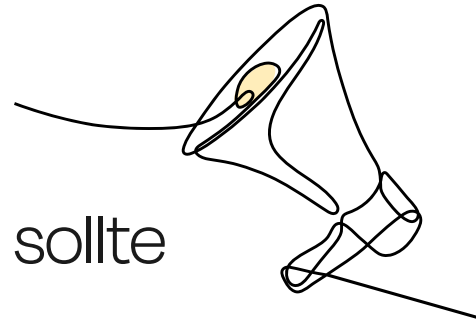
"Was verbirgt sich?"

"Ist es sicher und compliant?"

/// SCHWIERIGE FRAGEN:

Was CISOs interessieren sollte

Diese Fragen sind keine technischen Detailfragen, sondern strategische Fragen. Wenn Ihr Team sie nicht beantworten kann, sind Sie operationellen, regulatorischen und finanziellen Risiken ausgesetzt.



An Security Architecture & Engineering Leads

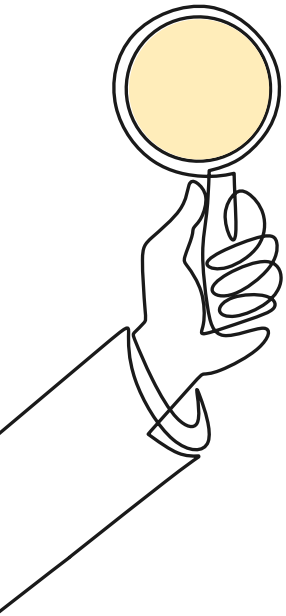
- Können wir ein aktuelles Inventar aller kryptografischen Assets und ihrer Verantwortlichen erstellen?
- Wo verlassen wir uns noch auf unsichere Protokolle oder schwache Chiffren?
- Können wir heute bereits quantenanfällige Algorithmen identifizieren?

An PKI- / Kryptografie-Verantwortliche

- Werden Zertifikatsabläufe, Schlüsselrotationen und Algorithmusnutzung aktiv überwacht und durchgesetzt?
- Wie bewerten wir unsere Gefährdung durch Post-Quanten-Bedrohungen?
- Könnten wir bei einem Audit morgen ein vollständiges kryptografisches Inventar vorlegen?

An AppSec- / DevSecOps-Leads

- Werden geheime Dokumente, Zertifikate und kryptografische Bibliotheken im gesamten SDLC korrekt verwaltet?
- Verstehen Entwicklungsteams klar, was erlaubt ist – und was nicht?
- Können wir kryptografische Abhängigkeiten in Drittanbieter- oder Open-Source-Komponenten identifizieren?



Abschließendes Wort an den CISO

Sie müssen kein Kryptografie-Experte sein – aber Sie müssen die Initiative ergreifen. Stellen Sie schwierige Fragen. Fordern Sie Antworten ein. Teilen Sie dieses Dokument mit Ihrem Team. Starten Sie die Diskussion. Verstehen Sie die Risiken.