ISMS pragmatisch
Von Säulen zu Brücken

Handout zum Vortrag · Karlsruher Tag der IT-Sicherheit 2026

Holger Mack
Chief Information Security Officer
Everest Systems GmbH
holger.mack@everest-erp.com
linkedin.com/in/holger-mack-1476b51a

Kai Jendrian
ISO-27001-Auditor & ISMS-Consultant
Secorvo Security Consulting GmbH
kai.jendrian@secorvo.de
linkedin.com/in/0x2e6b6169

Der Aufbau eines ISMS gilt vielerorts als bürokratisch und wenig wirksam – Compliance-Theater mit viel Aufwand und wenig Mehrwert. Wirksam wird ein ISMS erst, wenn es an den Zielen der Organisation ausgerichtet ist, wenn die Intention hinter den Standards verstanden und nicht nur formal abgehakt wird, und wenn die Umsetzung auf die eigenen Gegebenheiten zugeschnitten ist. Zentraler Hebel ist das Überwinden isolierter Verantwortungsbereiche: Solange die Disziplinen der IT-Sicherheit als getrennte Säulen nebeneinanderstehen, bleibt das ISMS fragmentiert. Erst Brücken – abgestimmte Prozesse und echte Zusammenarbeit – machen aus einem Dokumentensystem ein Steuerungsinstrument.

Die fünf Sätze zum Mitnehmen

1. Für wen machen Sie das ISMS – für die Ablage oder für die Menschen?
2. Erst die Ziele. Dann die Controls.
3. Wer schätzt ab, wer entscheidet – und welche Wette gehen Sie ein?
4. Jede Anforderung ist eine Frage, kein Befehl.
5. Security an dem orientieren, was schon funktioniert.

1. Compliance-Theater kostet, ohne zu schützen

Wo Informationssicherheit im Konjunktiv verhandelt wird – „man sollte„, „man müsste“, „man muss„ –, entsteht viel Aufwand, mit dem am Ende niemand zufrieden ist: Die Verantwortlichen schalten ab, die Betroffenen auch. Ein ISMS ist kein Selbstzweck. Sein Maßstab ist der Beitrag zum Erfolg der Organisation, nicht der Umfang des Ordners. Stellen Sie die Frage deshalb laut: Wie stellen wir sicher, dass Sicherheitsaktivitäten auf den Erfolg der Organisation einzahlen?

> *Noch nie hat ein Ordner einen Angriff bemerkt.*



2. Erst die Ziele, dann die Controls

Securitas kommt von *sine cura* – „ohne Sorge„, nicht „maximal sicher“. Der ausgeschaltete Server ist maximal sicher und komplett nutzlos. Und Risiko ist die Abweichung von Zielen, nicht nur der Angreifer: Auch das Backup, das nie zurückgespielt wurde, bringt Sie vom Ziel ab – ganz ohne Gegner. Wer Risiken managen will, muss also zuerst die Ziele der Organisation kennen, nicht die Norm.

Ziele haben ein Verfallsdatum. Markt, Kunden, Technik und Bedrohungslage ändern sich laufend. Wer Ziele einmal festschreibt und danach nur noch Controls pflegt, schützt bald ein Unternehmen von gestern. Zielfindung ist keine jährliche Alibi-Veranstaltung, sondern ständiger Austausch darüber, wohin sich das Unternehmen entwickelt. Das Ergebnis ist eine Geschäftsführung, die alle relevanten Risiken kennt – und trotzdem gut schläft. Oder zumindest weiß, warum sie schlecht schläft.

AUS DER PRAXIS · EVEREST SYSTEMS
Das Sicherheitssystem passt auf eine Seite. Der gesamte Security-Ansatz steht bei Everest auf einem einzigen Übersichtsbild. Was die Ziele bewegt, läuft dort als ständiger Zufluss hinein: Unternehmensstrategie und -status, Kunden und Markt, Bedrohungslage, Verträge, regulatorisches Umfeld. In der Mitte steht das Risikomanagement mit einem monatlichen Security Checkpoint, außen liegen Nachweise und Auditoren. Die Ziele werden damit nicht einmal jährlich erhoben, sondern sind fest verdrahtet – und der Austausch läuft in beide Richtungen.

Anhang A kennt Ihre Ziele nicht.

3. Risikomanagement heißt: informiert entscheiden

Risikomanagement ist das Herzstück eines ISMS, und es lässt sich in einem Satz fassen: Die richtigen Leute treffen informierte Entscheidungen und sorgen für deren Umsetzung. Eine Risikoentscheidung ist dabei eine begründete Wette unter Unsicherheit – subjektiv, aber nicht beliebig. Zwei Fachleute kommen zu zwei Einschätzungen, beide ehrlich; mit jeder zusätzlichen Evidenz rücken sie zusammen. Und jede Maßnahme hat Nebenwirkungen: Sie kostet und erzeugt selbst neue Risiken.

Entscheidend ist die saubere Trennung zweier Schritte:

Abschätzen – wie schwer wiegt das Risiko?
Security- und Fachleute ermitteln die Signifikanz: wie wahrscheinlich, wie schädlich für unsere Ziele.

Bewerten – wie gehen wir damit um?
Die zuständige Ebene wägt ab – gegen Kosten, Zeit und Chancen – und entscheidet, was angemessen ist.

Die Signifikanz bestimmt, wer bewertet und entscheidet: operativ, taktisch oder strategisch. Beide Fehler sind teuer – alles nach oben tragen, bis niemand mehr mitliest, und Großes unten hängen lassen, bis der Falsche mit fremdem Einsatz wettet. Akzeptieren ist auf jeder Ebene eine bewusste Option und keine Niederlage; vollständig eliminieren lässt sich fast nie etwas. Halten Sie deshalb fest, worauf Sie setzen, wer entschieden hat und was Sie deshalb tun.

AUS DER PRAXIS · EVEREST SYSTEMS
Wer entscheidet, hängt an der Tragweite. Der Ansatz bei Everest trennt drei Ebenen sauber: Alle setzen Sicherheit in den Standardprozessen des Tagesgeschäfts um; die Führungsebene beobachtet, erkennt und priorisiert; die Geschäftsführung verantwortet die geschäftskritischen offenen Risiken und entscheidet über Minderung oder Akzeptanz. Jedes Risiko wird dabei in zwei Sprachen beschrieben – als Security-Konsequenz (Verlust, Ausfall, Offenlegung, Manipulation von Daten, Systemen, Compliance) und als Business-Konsequenz (Markt- und Kundenverlust, finanzieller Schaden, Reputationsschaden, Regelverstoß). Im monatlichen Security Checkpoint kommen Konsequenz, Eintrittswahrscheinlichkeit und Behandlungsentscheidung zusammen –

mit Geschäftsführung, Entwicklung, Produkt, Vertrieb, Infrastruktur, Architektur und Datenschutz am Tisch.

AUS DER PRAXIS · EVEREST SYSTEMS

Das Risikoregister ist ein Ticket-Backlog. Risiken entstehen als Tickets im Werkzeug der Teams, nach fester Vorlage: betroffenes Asset und bedrohtes Schutzziel, dann in Freitext die Begründung der Eintrittswahrscheinlichkeit – welche Faktoren, welche Vorbedingungen, welche mindernden Umstände – und ebenso die Begründung der Auswirkung, je mit einer groben Skala von „sehr hoch„ bis „vermieden“. Die Vorlage erzwingt genau das, was eine Zahl allein nicht liefert: die aufgeschriebene Wette. Für wiederkehrende Fälle gibt es eigene Vorlagen, etwa für die Sicherheitsprüfung eines neuen Dienstleisters.

Der Tacho bremst nicht – denn er weiß nicht, ob Sie zu schnell sind.

4. Standards: Intention verstehen statt Zeilen abhaken

ISO 27001, SOC, TISAX, DORA, BSI IT-Grundschutz – die Liste schreckt ab, aber die Standards überschneiden sich stark und beschreiben dieselbe Sache aus unterschiedlichen Sichten. Der Reflex, jede Zeile in einem Requirement Mapping blind abzuhaken, ist meist der falsche Einsatz von Energie. Drei Fragen führen weiter:

1. Welche Intention steht hinter dieser Anforderung?
2. Was davon ergibt bei uns keinen Sinn?
3. Welche Lösung passt zu uns?

Fast jede Anforderung ergibt Sinn. Was oft keinen Sinn ergibt, ist der Standard-Weg ihrer Umsetzung. Risikomanagement gilt auch für die Anforderungen der Standards selbst – und KI ist beim Mapping ein brauchbarer Praktikant, aber kein Autor Ihrer Richtlinien.

AUS DER PRAXIS · EVEREST SYSTEMS

KI füllt den Fragebogen, der Mensch prüft. Für die TISAX-Selbstauskunft nach dem VDA-ISA-Katalog liegt das eigene Sicherheitsmodell samt Zertifikaten und Nachweisen in einem KI-Projekt. Die KI gleicht den Fragenkatalog dagegen ab, liefert eine Zusammenfassung und befüllt die Arbeitsmappe – inklusive Hinweisen, welche Abschnitte gar nicht einschlägig sind, etwa der Prototypenschutz aus der Automobilwelt. Der Merksatz dazu steht im Vortrag rot daneben: Ergebnisse immer prüfen.

Ein Standard ist die gesammelte Erfahrung derer, die es vorher falsch gemacht haben.

5. Von Säulen zu Brücken

Business, Security und Compliance stehen in vielen Organisationen als getrennte Säulen nebeneinander – und werden damit schnell zu Silos, in denen das ISMS fragmentiert. Brücken entstehen dort, wo Sicherheit sich an dem orientiert, was ohnehin schon funktioniert, statt etwas Neues danebenzustellen. Drei Brücken aus dem Alltag bei Everest Systems:

Security Leadership Team
Gemeinsam entscheiden; technische Entscheidungen bleiben lokal in den Dev-Teams.

Tooling = GitHub
Kein eigenes Security-Tool. Risiken als Tickets, dort wo die Teams ohnehin arbeiten.

Doku als Grafik
Controls im Ende-zu-Ende-Bild der Systemlandschaft statt im Word-Dokument.

Dazu gehört auch, den Takt zu ändern: Ein Risiko-Review alle sechs Monate ist Norm-Kalender, nicht Geschäftsrhythmus. In einer schnellen Umgebung wird kontinuierlich bewertet, wenn es etwas zu bewerten gibt.

AUS DER PRAXIS · EVEREST SYSTEMS
Die Architekturbilder sind die Sicherheitsdokumentation. Controls werden direkt in die Bilder eingezeichnet, die Entwicklung und Betrieb ohnehin pflegen: in die Infrastrukturübersicht und in den Software-Entwicklungs- und Betriebslebenszyklus. Die Markierung steht dort, wo die Maßnahme wirkt – verschlüsselte Datenbanken und unveränderliche Backups an der Speicherschicht, Vier-Augen-Review und automatisierte Tests in der Build-Pipeline. Dieselben Bilder nutzen auch andere Funktionen im Haus. Ein zusätzliches Dokument, das all das noch einmal in Prosa beschreibt, gibt es nicht.

Zweimal im Jahr zum Zahnarzt ersetzt kein Zähneputzen.

6. Vom Dokumentensystem zum Steuerungsinstrument

Am Ende steht der Wechsel des Modus: weg von „sollte„ und „müsste“, hin zu „wir wollen„ und bewussten Entscheidungen. Sicherheit ist dann keine eigene Säule, die alles anders macht, sondern ein Qualitätsmerkmal aller organisatorischen Tätigkeiten. Und Kennzahlen sind keine Pflichtübung, sondern Antworten auf die Frage, wie gut Sicherheit tatsächlich funktioniert – messen heißt, Unsicherheit zu vermindern.

Ein wirksames ISMS erkennt man nicht am Aktenordner, sondern daran, dass die richtigen Leute ruhig schlafen. Oder zumindest wissen, warum sie schlecht schlafen.

Gespenster gibt es nur im Konjunktiv.