sure[secure]
your security operations center

secure mag

SECURITY OVERENGINEERING

Wenn Sicherheitsarchitekturen komplexer werden als die Risiken, die sie lösen sollen

EINLEITUNG

Viele Sicherheitsorganisationen erleben heute eine paradoxe Entwicklung: Die Sicherheitsarchitektur wächst kontinuierlich. Neue Plattformen, spezialisierte Sicherheitslösungen und automatisierte Analyseverfahren liefern immer mehr Transparenz über potenzielle Risiken. Unternehmen sehen mehr Schwachstellen, mehr Angriffsversuche und mehr sicherheitsrelevante Ereignisse als jemals zuvor.

Diese Entwicklung ist längst messbar. Große Organisationen betreiben heute nicht selten 45 bis über 80 Security-Tools parallel. Gleichzeitig zeigt sich ein klares Muster: Mit steigender Tool-Anzahl wächst nicht nur die Komplexität, sondern auch die operative Unsicherheit.

Studien zeigen, dass fragmentierte Sicherheitsarchitekturen zu längeren Reaktionszeiten und höheren Kosten bei Sicherheitsvorfällen führen. Die eigentliche Herausforderung liegt jedoch tiefer: Viele Organisationen verfügen heute über mehr Sicherheitslösungen, als sie operativ wirksam steuern können.

Die unbequeme Realität: Mehr Security führt nicht automatisch zu mehr Sicherheit, sondern oft zu weniger Klarheit.

Security Overengineering entsteht nicht durch falsche Entscheidungen, sondern durch viele richtige Entscheidungen ohne übergeordnete Steuerung. Dieses Whitepaper zeigt, wo diese Dynamik entsteht und wie sie sich gezielt auflösen lässt.

Quellen:
https://www.ibm.com/reports/data-breach
https://www.paloaltonetworks.com/resources/research/state-of-security-operations-report
https://www.verizon.com/business/resources/reports/dbir/

„Irgendwann kommt der Punkt, an dem Security nicht mehr schützt, sondern nur noch beschäftigt. Und genau da beginnt das eigentliche Risiko."

— Andreas Papadaniil, CEO suresecure

HERAUSFORDERUNG:

SICHERHEITSLÖSUNGEN WACHSEN SCHNELLER ALS DIE ORGANISATION, DIE SIE BETREIBT

Security wächst selten strategisch. Sie wächst reaktiv. Ein Vorfall führt zu einem neuen Tool. Ein Audit fordert zusätzliche Kontrollen. Ein Hersteller verspricht bessere Detection. Jede Entscheidung ist für sich sinnvoll, aber kaum eine wird im Gesamtkontext bewertet. So entstehen Architekturen, die nicht geplant, sondern angesammelt sind.

In der Praxis bedeutet das: Viele Organisationen betreiben heute Dutzende Security-Tools, nutzen aber nur einen Bruchteil davon aktiv. Ein Großteil der Funktionen bleibt ungenutzt. Ein Teil der Alerts wird nicht bearbeitet. Und nur wenige Systeme werden wirklich kontinuierlich optimiert. Die Architektur wächst, die Wirksamkeit nicht.

Mit jeder neuen Lösung wächst nicht nur die Schutzwirkung, sondern auch der Betriebsaufwand. Integration, Konfiguration, Updates und Alert-Handling erzeugen eine Komplexität, die nicht linear skaliert.

Die Folge ist eine schleichende Verschiebung: Security wird zum Betriebsproblem.

LÖSUNGSANSATZ

Die zentrale Steuerungsfrage lautet: Welche Komplexität kann die Organisation dauerhaft tragen? Technologieentscheidungen sollten nicht isoliert getroffen werden, sondern im Kontext der bestehenden Architektur und der verfügbaren Kapazität. Der größte Hebel liegt dabei oft nicht im Ausbau, sondern in der Fokussierung.

Dort, wo operative Last dauerhaft hoch bleibt, kann eine gezielte Entkopplung sinnvoll sein. Der Betrieb einzelner Plattformen oder die kontinuierliche Analyse von Security-Events lässt sich in vielen Fällen effizienter außerhalb der eigenen Organisation abbilden, ohne zusätzliche interne Komplexität aufzubauen.

HERAUSFORDERUNG:

MEHR SICHTBARKEIT FÜHRT NICHT AUTOMATISCH ZU MEHR SICHERHEIT

Security hat ein neues Problem: Sie sieht zu viel. Moderne Security-Technologien liefern maximale Transparenz. Doch diese Transparenz erzeugt eine neue Realität. In vielen Security-Teams ist nicht fehlende Sichtbarkeit das Problem, sondern Überlastung.

Analysten priorisieren nicht mehr nach Risiko, sondern nach Dringlichkeit. Alerts werden abgearbeitet, aber nicht bewertet. Das Ergebnis ist paradox: Je mehr gesehen wird, desto weniger wird entschieden. Ein Großteil der Security-Teams leidet unter Alert Fatigue und hat Schwierigkeiten, relevante Ereignisse zuverlässig zu priorisieren.

LÖSUNGSANSATZ

Sicherheit entsteht durch Entscheidung, nicht durch Sichtbarkeit. Der Fokus muss sich verschieben: von mehr Detection zu klarer Priorisierung.

Das erfordert:

- eine klare Definition von geschäftskritischen Risiken
- verbindliche Entscheidungslogiken
- echte Verantwortlichkeiten

Der Engpass liegt selten in der Erkennung, sondern in der Bewertung. Wer diese Lücke schließt, gewinnt unmittelbar an Wirksamkeit.

HERAUSFORDERUNG:

FEHLENDE TRANSPARENZ ÜBER ASSETS VERSTÄRKT SECURITY OVERENGINEERING

Ein zentraler Treiber von Overengineering ist fehlende Klarheit über die eigene Angriffsfläche. In vielen Organisationen ist nicht vollständig bekannt, welche Systeme tatsächlich betrieben werden. Cloud-Ressourcen entstehen dynamisch, Anwendungen entwickeln sich außerhalb zentraler Strukturen, und ältere Systeme bleiben im Betrieb.

Die Folge: Security wird breit ausgerollt, statt gezielt eingesetzt. Das führt zu Doppelabsicherung auf der einen Seite und zu blinden Flecken auf der anderen. Komplexität entsteht hier nicht durch zu wenig Sicherheit, sondern durch fehlendes Verständnis.

LÖSUNGSANSATZ

Jede Sicherheitsstrategie beginnt mit einer einfachen Frage: Was existiert tatsächlich? Organisationen benötigen eine belastbare Sicht auf ihre Assets, ihre Exposition und ihre Verantwortlichkeiten.

Erst auf dieser Grundlage lassen sich Risiken sinnvoll priorisieren und Maßnahmen gezielt einsetzen. Ohne diese Klarheit führt jede zusätzliche Sicherheitsmaßnahme zwangsläufig zu mehr Komplexität.

HERAUSFORDERUNG:

PLATTFORMSTRATEGIEN LÖSEN KOMPLEXITÄT NICHT AUTOMATISCH

Plattformen gelten als Antwort auf wachsende Security-Komplexität. Die Erwartung ist klar: weniger Tools, weniger Schnittstellen, mehr Übersicht. In der Praxis entsteht jedoch häufig ein anderes Bild.

Plattformen ersetzen bestehende Lösungen selten vollständig. Stattdessen werden sie ergänzt. Spezialisierte Tools bleiben bestehen, neue Abhängigkeiten entstehen. Die Komplexität verschwindet nicht, sie wird nur neu verpackt.

LÖSUNGSANSATZ

Plattformen sind dann sinnvoll, wenn sie Komplexität reduzieren. Die entscheidende Frage lautet: Welche Systeme fallen dadurch tatsächlich weg?

Nur wenn Funktionen konsolidiert, Integrationen reduziert und Betriebsaufwände gesenkt werden, entsteht echter Mehrwert. Ansonsten entsteht lediglich eine neue Ebene innerhalb der bestehenden Komplexität.

HERAUSFORDERUNG:

AUTOMATISIERUNG VERSTÄRKT BESTEHENDE PROBLEME

Automatisierung wird häufig als Lösung für steigende Komplexität gesehen. Doch sie wirkt nicht neutral. Automatisierung verstärkt bestehende Strukturen. Gute Prozesse werden effizienter. Unklare Prozesse werden schneller problematisch.

Viele Organisationen automatisieren Unsicherheit. Das Ergebnis sind automatisierte Entscheidungen ohne klare Grundlage. Geschwindigkeit steigt, Qualität nicht.

LÖSUNGSANSATZ

Automatisierung ist kein Ausgangspunkt, sondern ein Reifegradindikator. Sie sollte dort eingesetzt werden, wo Prozesse klar definiert und stabil sind. Der größte Hebel liegt nicht in der Automatisierung selbst, sondern in der Klarheit der zugrunde liegenden Abläufe.

Erst Struktur, dann Geschwindigkeit.

ENTSCHEIDUNGSMODELL

WANN SECURITY ZU OVERENGINEERING WIRD

Security Overengineering entsteht schleichend. Entscheidend ist, den Punkt zu erkennen, an dem Komplexität beginnt, Sicherheit zu verdrängen.

Werden mehr Erkenntnisse erzeugt, als umgesetzt werden können?

Offene Schwachstellen und unbearbeitete Alerts sind kein Zeichen von Reife, sondern von Überlastung.

Gibt es Tools oder Funktionen ohne klare Verantwortung?

Was keinen Owner hat, hat langfristig keinen Wert.

Wird Komplexität durch neue Technologie weiter erhöht?

Wenn neue Tools nichts ersetzen, entsteht Overengineering.

Ist der operative Aufwand höher als der Sicherheitsgewinn?

Wenn mehr Zeit in den Betrieb der Security fließt als in die Reduktion von Risiken, ist der kritische Punkt erreicht.

PODCAST

CYBER SECURITY Basement

In unserem Podcast spricht Michael Döhmen über spannende Themen aus dem Bereich Cybersecurity. Dabei legen wir großen Wert auf Objektivität und verzichten auf übertriebenes Marketing oder „Feature-Fucking“. Stattdessen setzen wir auf einen seriösen, authentischen und ehrlichen Austausch zwischen Theorie und Praxis.

Jetzt reinhören

Spotify

Apple Podcast

YouTube Music

amazon music

und noch mehr...

FAZIT:

Security Overengineering ist kein Zeichen für zu viel Sicherheit. Es ist ein Zeichen dafür, dass Sicherheit nicht mehr steuerbar ist. Die größte Gefahr entsteht nicht durch fehlende Technologien, sondern durch Systeme, die niemand mehr vollständig überblickt.

Sicherheit entsteht nicht durch mehr Tools. Sondern durch Klarheit, Reduktion und konsequente Entscheidungen.

CISO
TAKEAWAYS

- Reduziere aktiv Security-Tools, die keinen klaren operativen Beitrag leisten.
- Stelle sicher, dass jede Lösung einen klaren Owner und messbaren Nutzen hat.
- Ersetze Komplexität, statt sie durch neue Technologie zu erweitern.
- Etabliere klare Entscheidungslogiken, nicht jede Information ist relevant.
- Überdenke dein Betriebsmodell dort, wo operative Last die Wirksamkeit verhindert.

SCHLUSSWORT:

Security Overengineering ist kein Sonderfall, sondern eine typische Entwicklung moderner Sicherheitsarchitekturen. Wer beginnt, Security aktiv zu steuern, gewinnt nicht nur Effizienz, sondern Kontrolle. Und genau diese Kontrolle entscheidet darüber, ob Security im Ernstfall funktioniert.

Weitere Informationen zum Thema:

Podcast-Folge:

In dieser Folge geht es um ein Phänomen, das in vielen Organisationen Realität ist: überladene Security Stacks mit dutzenden Tools, die kaum noch beherrschbar sind.

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60

E-Mail: kontakt@suresecure.de
Web: www.suresecure.de