Wie entwickeln Sie einen Aktionsplan zur Verbesserung der IT-Sicherheit?

Einen wirksamen Aktionsplan für die Verbesserung der IT-Sicherheit zu entwickeln, ist anspruchsvoll.

Wo beginnen Sie? Welche Themen haben Priorität? Welche Schwachstellen bestehen tatsächlich? Und welche Massnahmen bringen den grössten Nutzen?

Moderne IT-Infrastrukturen sind komplex. Technische Systeme, Cloud-Dienste, Benutzerverhalten, Berechtigungen und organisatorische Abläufe greifen ineinander. Oft besteht das Gefühl, dass Verbesserungen notwendig sind. Belastbare Fakten zu schaffen, die dieses Gefühl bestätigen und eine klare Priorisierung ermöglichen, ist jedoch zeitaufwendig.

Ein Aktionsplan auf Basis von Fakten

Ein wirksamer Aktionsplan sollte nicht auf Annahmen, sondern auf nachvollziehbaren Fakten basieren. Dazu gehört mehr als die technische Infrastruktur. Auch Benutzerverhalten, Verantwortlichkeiten, Berechtigungen und bestehende Sicherheitsprozesse sollten berücksichtigt werden.

Entscheidend ist anschliessend die Priorisierung:

- Welche Risiken sind relevant?
- Welche Massnahmen sind dringend?
- Und wo erzielt eine Investition den grössten Nutzen?

Genau hier liegt häufig die Herausforderung. Unternehmen sollten deshalb nicht einfach neue Sicherheitsprodukte beschaffen, nur weil diese technisch leistungsfähig sind. Ebenso wenig sollten Projekte gestartet werden, bevor klar ist, welches Problem tatsächlich gelöst werden soll.

Nach dem Prinzip: -> Zuerst verstehen. Dann priorisieren. Erst danach investieren.

Ein Blick auf Schwachstellen innerhalb kurzer Zeit

Das Cyber Security Assessment Tool, kurz CSAT, unterstützt dabei, innerhalb kurzer Zeit einen strukturierten Überblick über die bestehende Sicherheitslage zu erhalten.

Dabei werden technische Informationen aus der IT-Infrastruktur ausgewertet und mit weiteren Erkenntnissen aus dem Assessment kombiniert. Das Ziel ist nicht nur, mögliche Schwachstellen aufzuzeigen. Ebenso wichtig ist die Frage, welche Sicherheitsmassnahmen bereits wirksam umgesetzt sind.

So entsteht ein Gesamtbild:

- Wo bestehen erkennbare Risiken?
- Welche Kontrollen funktionieren bereits?
- Wo bestehen Lücken?
- Welche Themen sollten zuerst behandelt werden?

Auf dieser Grundlage lassen sich Schwachstellen analysieren und Massnahmen sinnvoll priorisieren.

Von der Analyse zum Aktionsplan

Die eigentliche Stärke eines Assessments liegt nicht im einzelnen technischen Befund. Entscheidend ist die Übersetzung in einen umsetzbaren Aktionsplan. Dabei werden technische und organisatorische Erkenntnisse zusammengeführt, bewertet und nach Relevanz priorisiert.

Das Ergebnis ist eine strukturierte Grundlage für die nächsten Schritte:

- kurzfristig notwendige Massnahmen
- mittelfristige Verbesserungen
- organisatorische Anpassungen
- notwendige Investitionen
- Themen mit geringerer Priorität

So entsteht keine lose Sammlung von Empfehlungen, sondern eine nachvollziehbare Security Roadmap.

Orientierung an etablierten Sicherheitsstandards

Die Bewertung orientiert sich an etablierten Sicherheitsrahmenwerken wie CIS, NIST und ISO 27001. Diese Standards helfen dabei, zentrale Sicherheitsthemen systematisch zu berücksichtigen und die Ergebnisse nachvollziehbar zu strukturieren. Das bedeutet nicht automatisch eine Zertifizierung oder vollständige Konformität mit einem bestimmten Standard. Vielmehr dienen die Frameworks als belastbare Orientierung, um Risiken einzuordnen und Prioritäten abzuleiten.

Klare Entscheidungsgrundlagen für das Management

Ein guter Aktionsplan richtet sich nicht nur an die IT.

Auch Geschäftsleitung und Verwaltungsrat benötigen eine verständliche Entscheidungsgrundlage:

- Wo stehen wir heute?
- Welche Risiken sind relevant?
- Welche Massnahmen haben Priorität?
- Wo ist eine Investition sinnvoll?

Ein strukturiertes Cybersecurity Assessment schafft dafür Transparenz. Statt einzelne Sicherheitsprodukte isoliert zu betrachten, entsteht ein Gesamtbild der tatsächlichen Sicherheitslage. Das erleichtert nicht nur die technische Umsetzung, sondern auch Budgetentscheide und die Kommunikation gegenüber dem Management.

Fazit

IT-Sicherheit verbessert sich nicht automatisch durch mehr Produkte oder mehr Projekte. Entscheidend ist zuerst zu verstehen, wo die relevanten Risiken liegen. Ein faktenbasierter Aktionsplan schafft Klarheit, setzt Prioritäten und bildet die Grundlage für gezielte Investitionen.

Nicht mehr Massnahmen. Sondern die richtigen Massnahmen in der richtigen Reihenfolge.