



Trainingsmodul

Präventive Informationssicherheitsmassnahmen verstehen

Kernkonzepte präventiver Massnahmen, inklusive Zugriffsmanagement, Kryptografie, sicherer Konfiguration und schützender Systemgestaltung



Wie verhindern präventive Massnahmen Sicherheitsvorfälle tatsächlich?

Überblick

Dieses Modul erklärt, wie Organisationen Sicherheitsvorfälle verhindern, indem sie die Angriffsfläche reduzieren und Angriffsmöglichkeiten begrenzen, bevor ein Schaden entsteht.

Die Teilnehmenden lernen, wie Mechanismen für Authentisierung und Autorisierung, kryptografische Schutzmassnahmen, sichere Konfiguration und schützender Systemaufbau zusammenwirken. Das Modul klärt Ziel und Grenzen dieser präventiven Schutzmassnahmen und zeigt, wie sie zu Vertraulichkeit, Integrität und Verfügbarkeit beitragen.

Die Konzepte sind in ISO/IEC 27001 Anhang A verankert. Der Fokus liegt auf dem strukturellen Verständnis und nicht auf der operativen Umsetzung oder der Konfiguration von Werkzeugen.



Zielgruppe

- Verantwortliche für Informationssicherheit und Personen, die ein Informationssicherheitsmanagementsystem (ISMS) umsetzen
- CIOs, CTOs, CISOs und andere Technologie-Führungskräfte
- Verantwortliche für IT-Services, Plattformen und Applikationen
- Compliance-, Risiko- und Governance-Fachpersonen (ISO/IEC 27001)
- Sicherheitsberater und kundennahe Beratende
- Produkt-, Engineering- und Betriebsleitende

Ist dieses Modul für Sie das Richtige?

Es passt gut für Sie, wenn Sie...

- verstehen wollen, wie präventive Massnahmen Risiken reduzieren.
- Klarheit über Ziel und Grenzen der präventiven Massnahmen aus ISO/IEC 27001 benötigen.
- Zugriffskontrollen, Kryptografie oder sichere Konfiguration umsetzen oder beurteilen.
- eine gemeinsame Sprache zu Steuerungsmassnahmen für Informationssicherheit, IT, Risiko und Audit benötigen.
- Anforderungen an Steuerungsmassnahmen in der Praxis konsistent anwenden wollen.

Es passt möglicherweise weniger gut für Sie, wenn Sie...

- vor allem an Detektions-, Reaktions- oder Wiederherstellungsmassnahmen interessiert sind.
- werkzeugspezifische Konfigurations- oder Härtungsschulungen erwarten.
- eine Durchsicht von Anhang A Abschnitt für Abschnitt erwarten.
- präventive Massnahmen bereits sicher entwerfen und beurteilen.

Lernergebnisse



Zentrale Lernergebnisse

- Ziel und Grenzen präventiver Massnahmen in der Praxis einordnen
- Identitäts-, Kryptografie- und Konfigurationsmassnahmen als ergänzende Schutzmassnahmen beschreiben
- Netzwerk-, Plattform- und Informationshandhabungsmassnahmen als Beitrag zur Reduktion der Angriffsfläche interpretieren

Zusätzliche Fähigkeiten

- Strukturelle Schwachstellen und Abhängigkeitslücken bei präventiven Massnahmen erkennen
- Präventive Massnahmen mit ISO/IEC 27001 Anhang A verknüpfen
- Die Logik präventiver Massnahmen über technische Aufgaben und Aufgaben der Governance hinweg vermitteln

Agenda

Was Prävention tatsächlich bedeutet

Wie sich definieren lässt, was präventive Massnahmen verhindern sollen, wie ihre Grenzen klar werden und warum Prävention scheitert, wenn Abhängigkeiten und menschliches Verhalten ignoriert werden

Grundlagen von Identitäts- und Zugriffsmanagement

Wie sich Authentisierung, Autorisierung und Sitzungssteuerung als präventive Mechanismen strukturieren lassen und wie Minimalprinzip und Funktionstrennung die Angriffsfläche reduzieren

Muster für Zugriffssteuerung ohne Prozessballast

Wie sich die Logik für Eintritt, Wechsel und Austritt als Frage des Massnahmendesigns behandeln lässt, wie sich Risiken aus Dienst- und geteilten Zugängen adressieren lassen und wie Notfallzugriffe ohne unnötige Komplexität gesteuert werden

Kryptografie als präventive Massnahme

Wie kryptografische Mechanismen Vertraulichkeit, Integrität und Authentizität schützen und wie typische Schwachstellen im Schlüsselmanagement und in der Umsetzung vermieden werden

Schutzkonfiguration und sichere Aufbaukonzepte

Wie sichere Voreinstellungen, Basiskonfigurationen und Härtingspraktiken aufgebaut werden und wie Schwachstellen- und Patchmanagement den präventiven Aufbau ergänzen

Grundlagen von Netzwerk- und Plattformschutz

Wie Segmentierung, Grenzkontrollen und sicherer Fernzugriff die Angriffsfläche reduzieren und wo präventiver Schutz endet und Detektion nötig wird

Grundlagen der Informationshandhabung und Verlustvermeidung

Wie Klassifizierungs- und Handhabungsregeln mit klarer präventiver Absicht definiert werden und wie Minimierung und Aufbewahrungssteuerung die Angriffsfläche verringern

Praxisworkshop

Anwendung der erlernten Konzepte, Methoden und Ansätze in einem realistischen Praxisfall

Enthaltene Unterlagen

Lernunterlagen

- Foliensatz
- Workbook für Teilnehmende

Vorlagen & Werkzeuge

- IAM-Politik, Konzept für Identitätsgovernance und Prozess für Zugriffsmanagement
- Kryptografiepolitik und Prozess für Schlüssel- und Zertifikatsmanagement
- Konzept für sichere Konfiguration und Baselines
- Konzept für Segmentierung und Grenzkontrolle
- Politik zur Klassifizierung und Handhabung von Informationen
- KI-Prompt-Sammlung für die Anpassung von Artefakten

Bestätigung

- Teilnahmebestätigung

Vorbereitungshinweise

Vorausgesetzter Hintergrund

Dieses Modul setzt allgemeine Berufserfahrung mit der IT und der Informationshandhabung in Organisationen voraus. Vorkenntnisse zu einzelnen Abschnitten von ISO/IEC 27001 sind nicht erforderlich.

Hilfreich sind:

- Grundverständnis für Benutzer, Systeme, Netzwerke und gängige Unternehmenswerkzeuge
- Vertrautheit mit operativen Realitäten wie Zugriffsanträgen, Administrationsrollen und Konfigurationsänderungen
- Sicherheit im Lesen einfacher technischer Diagramme oder Beschreibungen von Steuerungsmassnahmen

Vorbereitungsmodule

Es sind keine Vorbereitungsmodule erforderlich.

Organisatorisches



Verfügbare Sprachen

- Englisch
- Deutsch

Durchführung - Standard

- Virtueller Live-Unterricht
- Blended Learning (E-Learning + Live)

Durchführung - individuell

- Vor-Ort-Durchführung bei Ihnen
- Inhalte angepasst an Ihre Organisation



Halderstone

Halderstone by Langer & Co

Zürcherstrasse 2
CH-8852 Altendorf
Schweiz

info@halderstone.com
www.halderstone.com