Information Security in Healthcare

KUDELSKI SECURITY

Insider Threat im Spital: Wie Sie interne Bedrohungen und Cyber Risiken effizient managen können

Johannes Schaetz, Director & Sanda Haas Würmli, Manager – Advisory Services

Agenda

- Insider Threats und Bedrohungslage
- Frameworks und Massnahmen
- Erfahrungen und Erfolgsmodelle
- Key Takeaways

Insider Threats und Bedrohungslage

Warum gerade der Gesundheitssektor?

Healthcare Cyberattacks Cost $1.4 Million on Average in Recovery

The cost is directly tied to a loss of productivity, reputation damage, and service disruption, among other business impacts.

KUDELSKI SECURITY

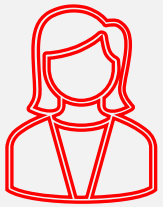
Information Security in Healthcare

Definition eines Insiders

- **Eine Person, der die Organisation vertraut**, einschliesslich der Mitarbeiter, denen die Organisation vertrauliche Informationen und Zugang gewährt hat
- **Eine Person, der ein Ausweis oder ein Zugangsgerät ausgestellt wurde**, welches sie als Person mit regelmässigem oder ständigem Zugriff identifiziert (z.B. ein Mitarbeiter oder Mitglied einer Organisation, Auftragnehmer, Verkäufer, Hausmeister, Mechaniker)
- Eine Person, der man **einen Computer mit Netzwerkzugriff** zur Verfügung gestellt hat
- **Eine Person, die Produkte und Dienstleistungen der Organisation entwickelt**, einschliesslich denjenigen, die Geheimnisse der Produkte und deren Mehrwerte kennen
- **Eine Person, die sich mit den Grundlagen der Organisation auskennt**, einschliesslich Preisgestaltung, Kosten sowie Stärken und Schwächen
- **Eine Person, der Geschäftsstrategie und Organisationsziele bekannt sind** und die mit Zukunftsplänen und Massnahmen der Organisation und der Sorge seiner Leute betraut ist
- Im Rahmen staatlicher Aufgaben **eine Person mit Zugriff auf geschützte Informationen**, die im Falle einer Kompromittierung der nationalen und öffentlichen Sicherheit schaden könnte

Bedrohung durch Insider – eine kurze Übersicht

ca. 15% der Insider



- böswillig
- absichtlich

Datenbank-Administrator verkauft Daten auf dem Darkweb.

Ein Sicherheitsmitarbeiter verschafft sich Zugang und installiert Malware auf PCs.

Eine ehemalige Mitarbeiterin hat weiterhin Systemzugriff und bleibt unbemerkt.

ca. 85% der Insider

- unwissentlich
- unabsichtlich

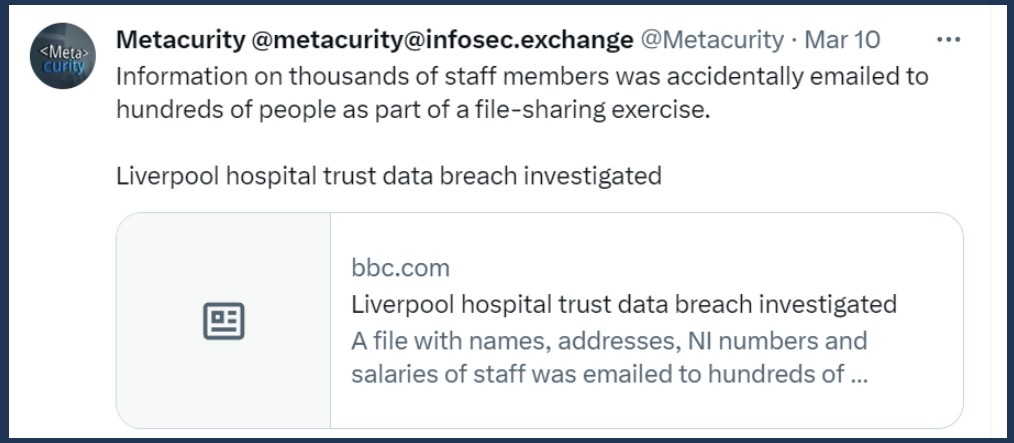
Praktikant installiert unbewilligte Software

Ein Mitarbeiter lässt einen ungesicherten Laptop für 2 Minuten in der Cafeteria stehen.

Eine Mitarbeiterin verliert den Zugangsbadge und bemerkt es nicht sofort

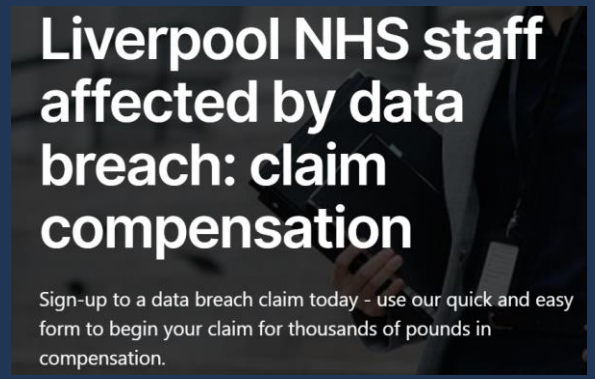
Datenleck beim Liverpool Hospital Trust

- Der Liverpool Hospital Trust betreibt die Spitäler Aintree, Royal Liverpool University Hospital, Broadgreen und Liverpool University Dental Hospital
- Dezember 2022: grosse Datenleck auf Grund von Nachlässigkeit
- Was ist passiert:
  - Persönliche Daten von 14.000 Angestellten wurden aus Versehen an eine unautorisierte Partei via Email geschickt
  - Details enthielten Name, Adresse, Salär, Geschlecht, Ethnizität, Versicherungsangaben
  - Die Informationen waren in einer Exceltabelle enthalten die and hunderte Trust Manager verschickt wurden

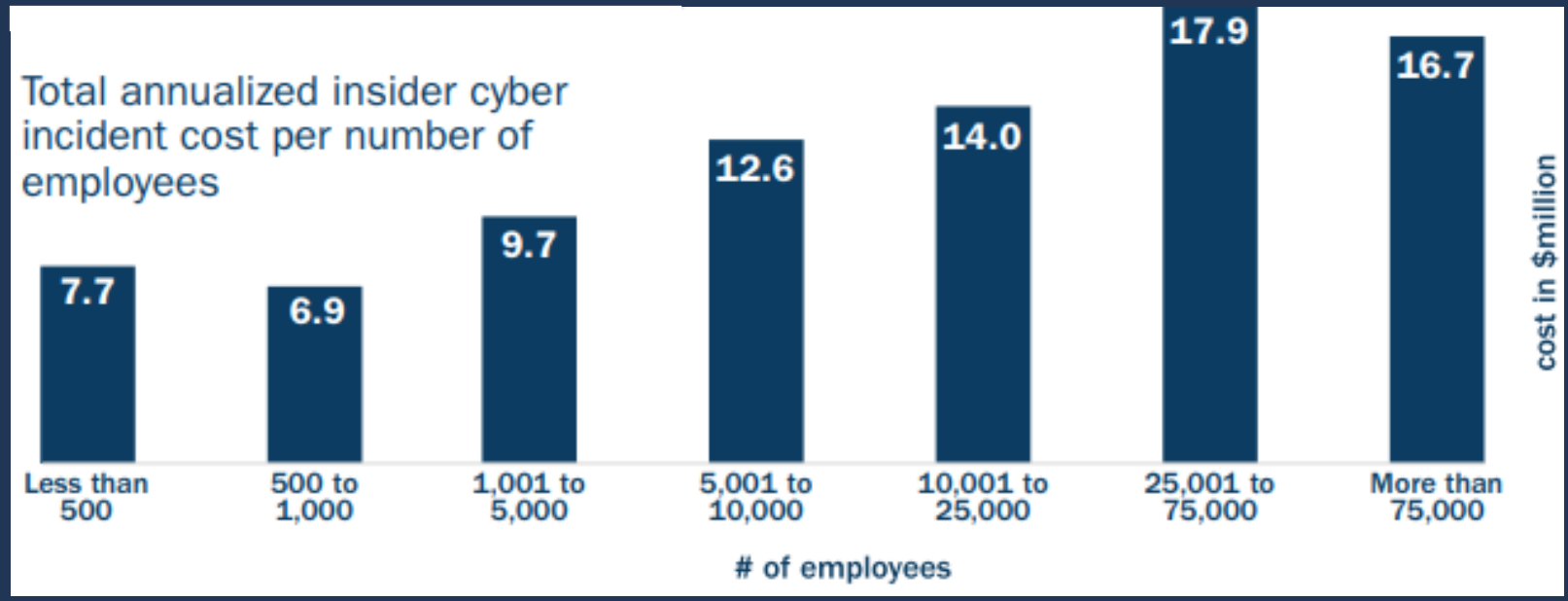


Datenleck beim Liverpool Hospital Trust II

- Liverpool Hospital Trust hat die Datenpanne erst im Februar bekannt gegeben
- Später hat sich heraus gestellt, dass das Email insgesamt an 24 externe Empfänger ging
- Der Trust musste sich einem kompletten Email Recovery- und Löschungsprozess unterziehen
- Bis heute kann nicht eindeutig ausgeschlossen welche Personen Einsicht in die Exceltabelle hatte
- Die Trust Angestellten wurden informiert und eine Entschuldigung ausgesprochen
- Das Datenleck wurde der britischen Regulierungsbehörde ICO gemeldet
- Klagen mit Anspruch auf Entschädigungszahlungen sind in Vorbereitung



Kosten von Insider Threats



Potenzielle Kosten, die in einer Organisation je nach Art des Insider-Vorfalls entstehen können.

- Insider Threats sind ein glaubwürdiges Risiko und stellen potenziell unerschwingliche Kosten für jedes Unternehmen unabhängig ihrer Grösse dar
- Die finanziellen Auswirkungen für Organisationen sind verheerend, insbesondere für Unternehmen mit weniger als 500 Mitarbeitern

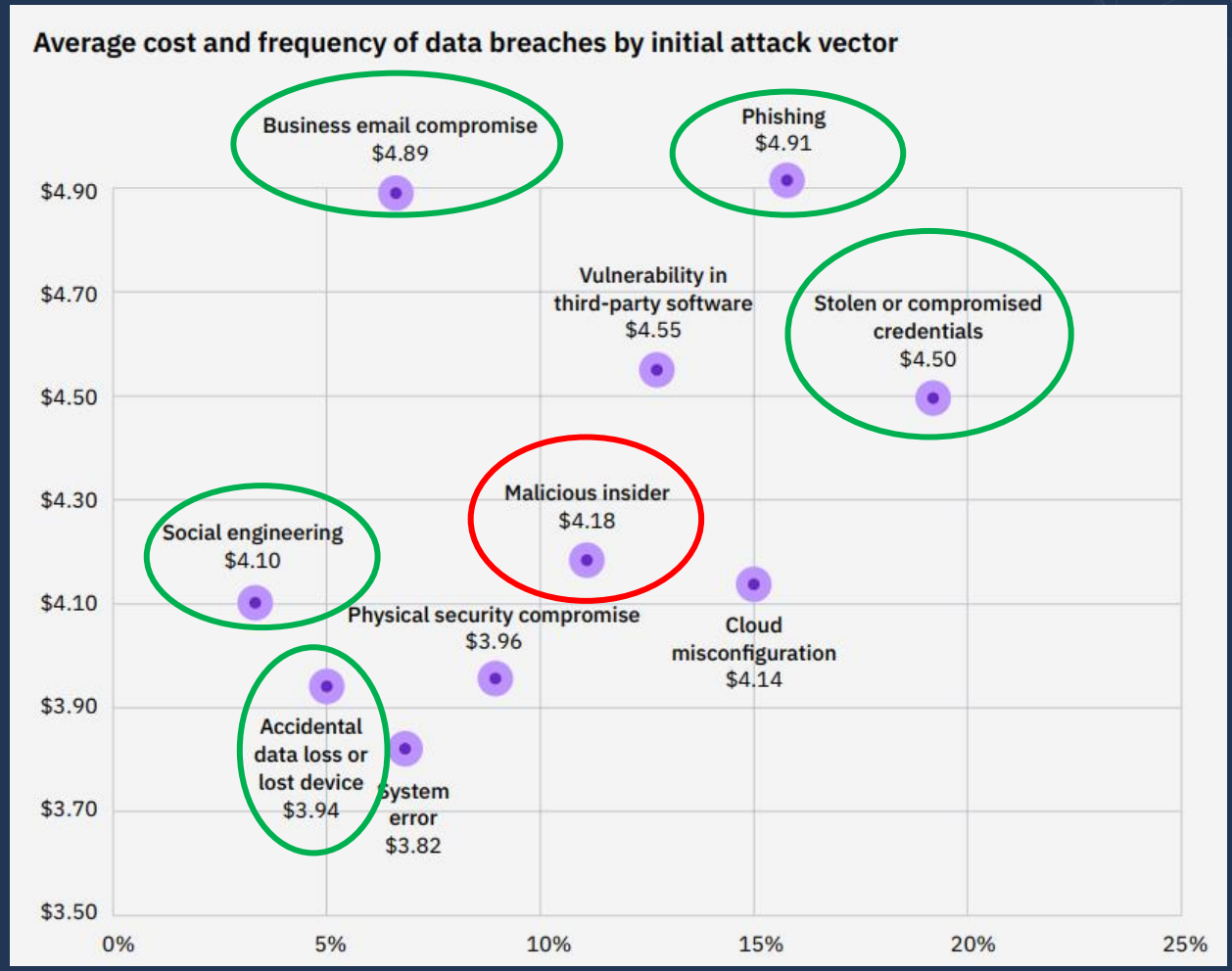
Verbreitung von Insider Threat Vorfällen

- Insider-Threats nehmen stetig zu, insbesondere Technologiediebstähle
- Mögliche Verluste: Schäden an der Infrastruktur, Unterbrechung der Produktivität, Diebstahl geistigen Eigentums, Verlust sensibler Daten und Reputationsschaden
- Jeder dieser Faktoren kann zum Verlust von Wettbewerbsvorteilen führen

Böswillige Insider – das kleinere Problem

Typische Auswirkungen von Insider Threat Fällen

- Kritischer Datenverlust: 40%
- Betriebsausfall / -störungen: 33%
- Reputation / Markenschaden: 26%
- Kosten für Behebung von Sicherheitslücken: 19%
- Wettbewerbsverlust: 17%



Source: IBM Security – Cost of Data Breach Report 2022

Measured in USD millions

Frameworks und Massnahmen

Fragestellung

Welche **Bedrohungen** bestehen?

Wie finden die **Angriffe** statt?

Welche **Auswirkungen** haben die Angriffe?

Können **Standardszenarien** abgedeckt werden?

Welche **Massnahmen** sind zu treffen?

Return on Investment für Mitigationsprogramme

Die Kosten für die Bewältigung eines Insider-Vorfalls und die anschliessende Wiederherstellung sind erheblich höher als die Kosten für die Einrichtung und Aufrechterhaltung eines Insider Threat-Programmes

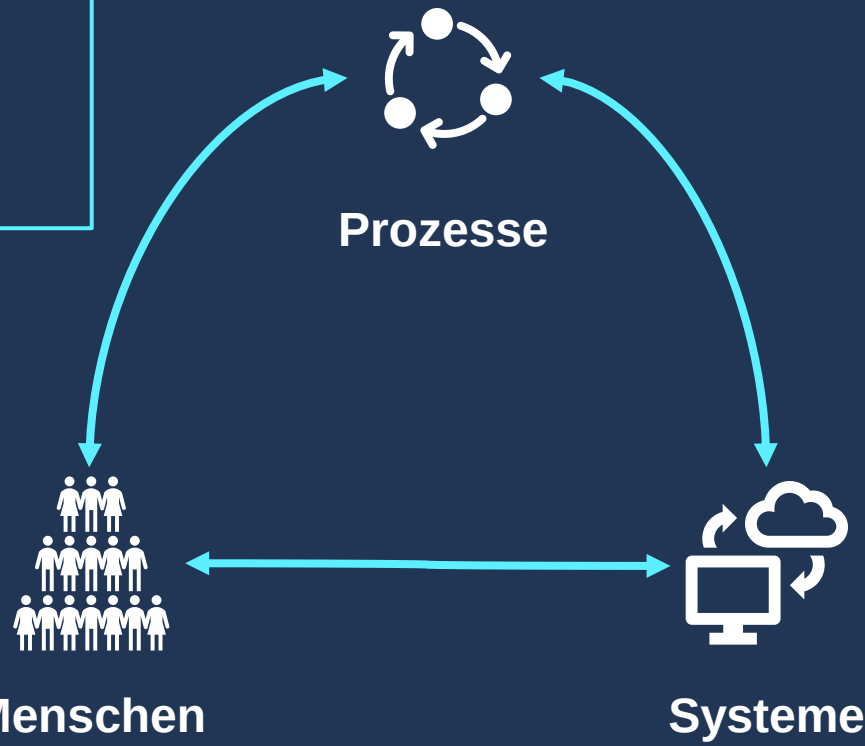
Unternehmen, die ein Programm zur Abwehr von Insider Threats erstellen oder verbessern, erzielen ein Return of Investment, sowohl immateriell als auch materiell. Der ROI wird in folgenden Bereichen angezeigt:

- ☑ Verstärkung der bestehenden Sicherheitsmassnahmen
- ☑ Erhöhte Anzahl sicherheitsbewusster Mitarbeiter oder Mitglieder
- ☑ Verbesserte Kultur des Teilens der Sicherheitsverantwortung und des Vermögensschutzes
- ☑ Frühzeitige Erkennung von Bedrohungen
- ☑ Kürzere Zeit für die Erkennung von Bedrohungen
- ☑ Schutz des organisatorischen Rufes
- ☑ Erhöhte Kundenakzeptanz

Was nun?

Governance:

- Weisungen und Richtlinien
- Onboarding und Offboarding Prozesse
- Background Checks
- Passwort Management
- Überwachung und Audits
- Datenklassifizierung



Awareness Training:

- Phishing Simulationen
- Cyber Security Awareness
- Passwort Hygiene

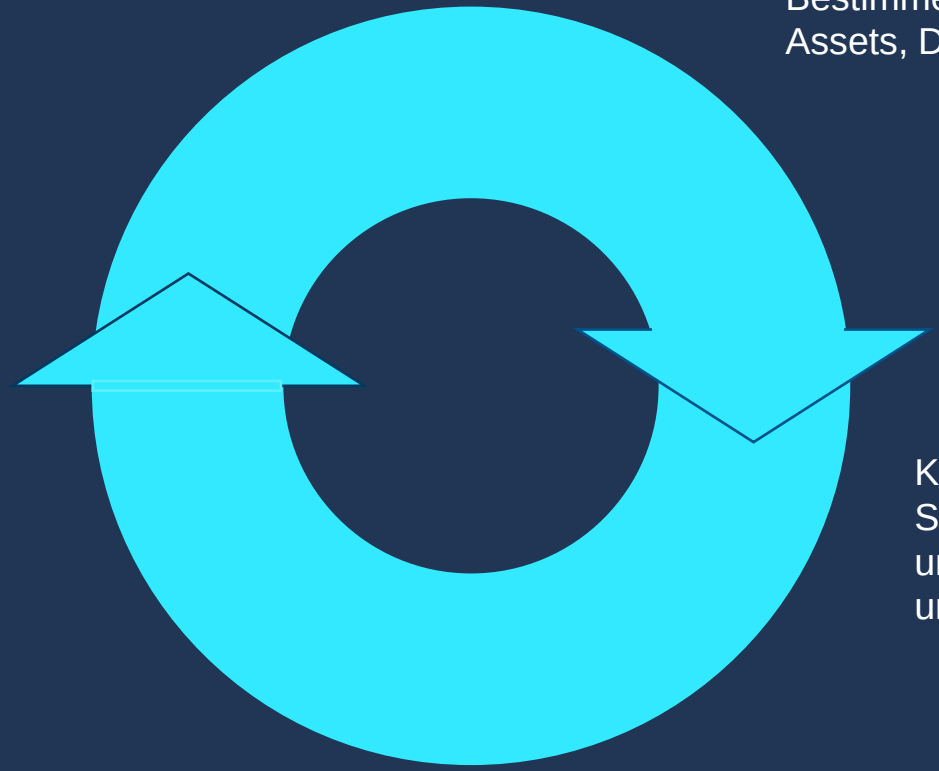
IT Security Massnahmen:

- Passwort Management
- Anti-spam / Anti-Malware Lösungen
- Zero-trust und MFA
- Incident Detection & Response Lösungen
- Backup Management
- Data Loss Prevention Lösungen
- Device Management
- User Activity Monitoring
- Logging und Auditing

Mitigation von Insider Threats

Threats definieren

Das Definieren von Insider Threats ist der Start eines jeden Mitigationsprogrammes. Dazu gehört das Bestimmen von Verhaltensmustern und kritische Assets, Daten und Services.



Threats monitoren und identifizieren

Kontinuierliches Überwachen von Systemen und Benutzerverhalten, um ungewöhnliches Verhalten von Systemen und Benutzern frühzeitig zu entdecken.

Threats bewerten

Bewertung identifizierter Bedrohungen, um entsprechende Massnahmen zu ergreifen.

Threats managen

Multidisziplinäres, kontinuierliches Managen von Insider Threats mittels aktiver und passiver Massnahmen, welche organisatorische, prozessbasierte und technische Mittel umfassen.

Erfahrungen und Erfolgsmodelle

Etablieren eines Insider Threat Mitigationsprogramms

PLANEN

- Sichern des Executive-Engagements
- Bestimmen des Best Fit
- Bestimmen der Programm-Ownership
- Einrichten einer multidisziplinären Governance-Gruppe
- Festlegen von Leitprinzipien
- Richtlinien entwickeln
- Auf rechtliche Verpflichtungen eingehen
- Identifizieren der Kronjuwelen

ORGANISIEREN & AUSRÜSTEN

- Integrieren Sie Informationen, Analyse und Reaktion
- Entwickeln Sie einen Reaktionsplan für Vorfälle
- Richten Sie Berichtswege ein
- Setzen Sie Technologien und Tools ein, um besorgniserregendes Verhalten zu identifizieren
- Erstellen Sie eine Risikorubrik und eine Methodik zur Bedrohungsbewertung
- Richten Sie ein multidisziplinäres Bedrohungsmanagement-team ein

TRAINIEREN & AUSFÜHREN

- Internes Vermarkten des Programms
- Fördern einer Kultur der Berichterstattung
- Implementieren eines formelles Schulungs- und Sensibilisierungsprogramms

EVALUIEREN & VERBESSERN

- Durchführen von Übungen
- Pflegen des Programms
- Sorgen für Aufsicht und Einhaltung

Effiziente Insider Threat Mitigationsprogramme

Massschneidern des Programms und Risikobereitschaft an die Mission, Kultur, kritische Ressourcen und Bedrohungen der Unternehmenslandschaft an

Entwickeln eine Melde- und Präventionskultur, welche eine positive Aussage über die Investition des Unternehmens in das Wohlergehen der Mitarbeiter macht, sowie über ihre allgemeine Belastbarkeit und operationelle Wirksamkeit.

Nutzen multidisziplinäre Fähigkeiten, die durch Technologien ermöglicht werden sowie dediziertes Personal je nach Art, Grösse, Kultur, Natur, Geschäftswert und Risikotoleranz gegenüber böswilligen, fahrlässigen oder unbeabsichtigten Insidern.

Verwenden eines Frameworks zum Erkennen und Identifizieren, Bewerten und Verwalten, zur Verhinderung, dem Schutz und der Minderung von Insider Threats.

Etablieren eine schützende und unterstützende Kultur, sichern den Schutz der bürgerlichen Freiheiten und wahren die Vertraulichkeit.

Unterstützen von Unternehmen bei der Bereitstellung einer sicheren, nicht bedrohlichen Umgebung, wo Personen, die eine Bedrohung darstellen könnten, identifiziert und geholfen wird, bevor ihre Handlungen Schaden anrichten können.

Komponenten eines erfolgreichen Mitigationsprogramms

1. **Grundsätze und Normen, welche das Programm an die Kultur und das Geschäft einer Organisation anpassen** und die dessen Zweck, Ziele und Zielsetzungen beschreiben
2. **Eine nach Prioritäten geordnete Liste kritischer Assets**, **physisch als auch IP bezogen**, die für den Betrieb oder das Geschäft einer Organisation unerlässlich sind und deren Kompromittierung, Schaden, oder Verlust sich nachteilig auf ihre Mission auswirken kann
3. **Definitionen der signifikantesten und vorherrschenden Bedrohungen** und wie sie sich auf die kritischen Assets des Unternehmens auswirken können
4. **Mittel zum Erkennen und Identifizieren von Indikatoren** für potenzielle Risiken
5. Ein **Incident Response (IR) Plan** im Falle eines Insider Threat Vorfalls
6. Ein **Gremium von Interessenvertretern** für Programm-Governance und Führung
7. Eine **Organisationskultur, die ermutigt und die Mittel zum Reporting zur Verfügung stellt**; wo das Melden von potenziellen Bedrohungen, Indikatoren oder Bedenken an einen Verantwortlichen eine vernünftige Erwartung ist und wo Vertraulichkeit gewahrt wird
8. Ein **zentraler Informations-Hub** für die Sammlung, Integration, Analyse und Speicherung aller Elemente in Bezug auf Insider Threats
9. Ein **Threat Management Team** für Bewertung, Reaktion und Management potenzieller Insider Threats

Key Takeaways

Erfolgsfaktoren für das Management von Insider Threat

- Organisationskultur, die auf proaktives Handeln und Kooperation auf allen Ebenen fördert
- Balance zwischen Schutz der Unternehmenswerte (Assets) einerseits und Schutz von Daten, Rechten und Freiheiten andererseits
- Regelmässige Überprüfung und Anpassung der Rahmenbedingungen, Massnahmen und Kontrollen
- Fokus auf Risikoprävention – es ist besser und einfacher alle Angestellten im Boot zu haben und ihnen zu helfen, als Fehler zu suchen und aufzudecken.
- Klare Vorgaben und Richtlinien betreffend erwartetem Verhalten der Mitarbeiter, sowie ein gesunder Mix zwischen positiven Anreizen und klaren Sanktionierungsmassnahmen.

Ein wirksames Insider Threat Mitigationsprogramm…

- **Identifiziert und konzentriert sich auf die kritischen Vermögenswerte, Daten und Dienste**, die das Unternehmen als wertvoll definiert.
- **Überwacht das Verhalten**, um vertrauenswürdige Insider zu erkennen und zu identifizieren, die das Vertrauen der Organisation missbrauchen.
- **Bewertet Bedrohungen**, um das individuelle Risikoniveau identifizierter Personen zu bestimmen.
- **Verwaltet das gesamte Spektrum von Insider Threats**, einschliesslich der Umsetzung von Strategien, die sich auf die betroffene Person, potenzielle Opfer und/oder Teile der Organisation konzentrieren, die für einen Insider Threats anfällig sind oder von ihm angegriffen werden.
- **Bezieht einzelne Insider mit ein**, die möglicherweise auf dem Weg zu einer feindseligen, fahrlässigen oder schädlichen Handlung sind, zur Abschreckung, Erkennung und Schadensbegrenzung.

Diskussions- & Fragerunde

Kudelski Security

Advisory

Security Programs & Assessments
Cloud Security Services
Incident Preparedness

We help security leaders to be successful, partnering with them to develop strategies that minimize exposure & strengthen security posture.

Managed Security

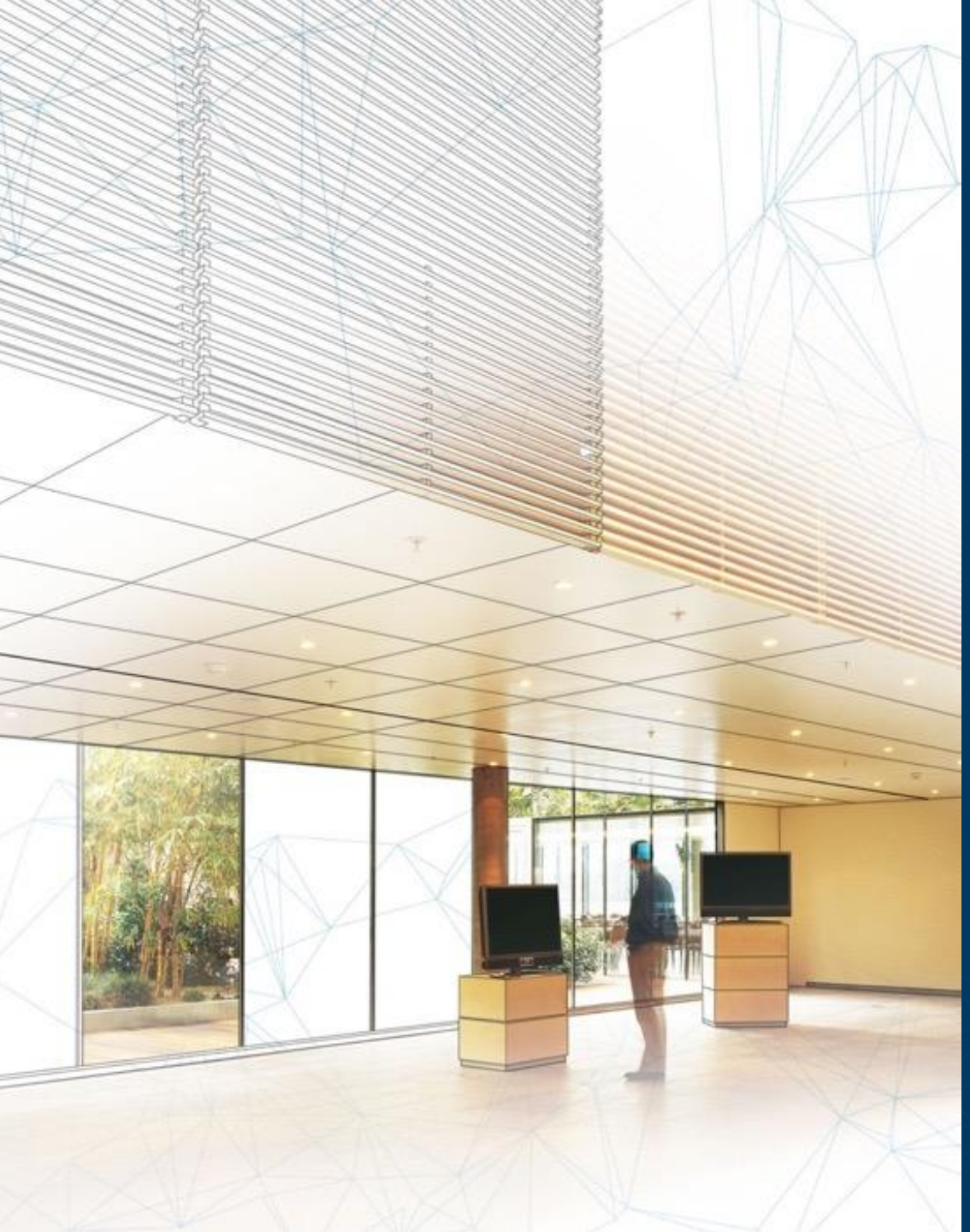
Cyber Fusion Center
24x7x365
Managed Detection & Response

We use advanced fusion capabilities to detect & respond to real threats faster, and safeguard client data – wherever it resides.

Technology Optimization

Technology Assessments
Cybersecurity Architectures & Design
Automation & Orchestration

We help organizations build, deploy and manage IT security to best match their business & operation needs.



KUDELSKI SECURITY

Thank you!

Johannes Schaetz
johannes.schaetz@kudelskisecurity.com
+41 79 698 2987

Sanda Haas Würmli
sanda.haaswuermli@kudelskisecurity.com
+41 79 441 9694