Diese Forschungsarbeit wurde durch die Agentur für Innovation in der Cybersicherheit GmbH beauftragt und finanziert. Eine Einflussnahme der Agentur für Innovation in der Cybersicherheit GmbH auf die Ergebnisse fand nicht statt.

Personas erstellt im Rahmen des MANTRA Projektes (Graphen-basierte Informationsaggregation zur Verbesserung des Cybersicherheitsmanagements in kritischen Infrastrukturen)

Ersteller: Michael Kubach und Andrea Horch
Auf Basis von Interviews und Workshops mit Stakeholdern

Kontakt:
Fraunhofer IAO
www.hci.iao.fraunhofer.de
michael.kubach@iao.fraunhofer.de

2024

Dr. Martina Sicher

»Ich treffe möglichst fundierte Entscheidungen zum Einsatz von Sicherheitslösungen und balanciere dabei zwischen dem Schutz des Unternehmens und der Kostenkontrolle.«

Übersicht

Alter: 52 Jahre

Position: Chief Information Security Officer (CISO) in einem großen Industrieunternehmen

Hauptaufgaben: Strategische Planung der Cybersecurity-Maßnahmen, Budgetverantwortung, Risikomanagement, Business Continuity

Kurzbeschreibung

Dr. Martina Sicher ist eine erfahrene CISO in einem führenden Industrieunternehmen. Sie hat einen Doktortitel in Informationssicherheit und über 15 Jahre Erfahrung im Bereich Cybersecurity. Sie ist eine respektierte Führungskraft, die sich für die Weiterbildung ihres Teams und die Stärkung der Unternehmensresilienz einsetzt.

Motivationen

- Erhalt und Verbesserung der Sicherheitslage des Unternehmens
- effektive Prävention gegen Cyberangriffe
- Karriereoption im Top Management

Frustrationen

- Komplexe Entscheidungsfindung bei Sicherheitsinvestitionen
- Abwägung zwischen Sicherheitsbedürfnis und operativer Effizienz
- Reifegrad IT-Sicherheitsniveau in der Supply Chain

Ziele

- Sicherung der Unternehmensdaten und -systeme
- Kostenoptimierung
- Einhaltung von Compliance-Anforderungen

Herausforderungen

- Balance zwischen Sicherheit u. Kosten
- Auswahl effektiver und effizienter Sicherheitslösungen
- Management der Unternehmenssicherheit in einer komplexen Supply-Chain
- IT-Fachkräftemangel

Technologische Fähigkeiten

- Tiefes Verständnis von Sicherheitsarchitekturen
- Kenntnisse in aktuellen Cybersecurity-Trends
- Erfahrung mit Threat Intelligence Plattformen

Kommunikationskanäle

- Geschäftsberichte
- Fachkonferenzen
- Netzwerktreffen mit anderen CISOs
- Meetings im Top Management

Felix Fleißig

»Eine Sicherheitslandkarte von Deutschland oder der ganzen Welt als Übersicht über aktuelle Bedrohungen in einem Dashboard wäre mein Traum.«

Übersicht

Alter: 35 Jahre

Position: Sicherheitsanalyst in der IT-Abteilung eines Industrieunternehmens

Hauptaufgaben: Analyse von Sicherheitswarnungen, Reporting von Vorfällen, Prävention und schnelle Behebung von Sicherheitsvorfällen

Kurzbeschreibung

Felix Fleißig ist ein engagierter Sicherheitsanalyst, der mit Leidenschaft und Präzision arbeitet. Er ist bekannt für seine Fähigkeit, auch unter Druck effizient zu bleiben und komplexe Informationen schnell zu verarbeiten. Felix ist stets motiviert, zur Sicherheit des Unternehmens beizutragen, obwohl seine Zeit durch eine Vielzahl von Aufgaben stark begrenzt ist.

Motivationen

- Beitrag zur Sicherheit des Unternehmens
- Wunsch nach effektiver Nutzung von Sicherheitsplattformen
- Karriere im Sicherheitsbereich

Ziele

- Effizienter Umgang mit Informationen zur Cybersicherheit
- Verbesserung des Incident-Response-Prozesses
- Vermeidung von Sicherheitsvorfällen

Technologische Fähigkeiten

- Versiert im Umgang mit Sicherheitstools
- Analysefähigkeiten
- Verständnis für Incident Management
- Tiefes Verständnis von Sicherheitsarchitekturen

Frustrationen

- Zeitmangel
- Balance zwischen täglichen Aufgaben und Sicherheitsanforderungen
- Druck, keine Fehler zu machen
- Vielzahl Tools u. Sicherheitsmeldungen
- Compliance beschränkt teilweise Möglichkeit zum Austausch mit Peers aus anderen Unternehmen

Herausforderungen

- Hohe Arbeitsbelastung, Management einer Vielzahl von Aufgaben
- Zeitdruck bei der Informationsverarbeitung
- Identifizierung und Priorisierung von Sicherheitsvorfällen
- Balance zwischen Sicherheit und Verfügbarkeit der IT-Infrastruktur

Kommunikationskanäle

- Interne IT-Systeme
- E-Mails
- Kurzmeldungen über Sicherheitsplattformen
- persönliche Kontakte zu Peers

Laura Linse

»Ich möchte Sicherheitsbedrohungen stets proaktiv begegnen und weiß benutzerfreundliche Sicherheitssoftware zu schätzen.«

Übersicht

Alter: 39 Jahre

Position: IT-Sicherheitsbeauftragte in einer kleineren öffentlichen Behörde

Hauptaufgaben: Überwachung und Management der IT-Sicherheit, Einsatz und Pflege von Sicherheitssoftware, Koordination mit höheren Behörden

Kurzbeschreibung

Laura Linse ist die IT-Sicherheitsbeauftragte einer kleineren Behörde und übernimmt dort eine zentrale Rolle in der IT-Sicherheit. Trotz ihrer chronischen Überlastung bleibt sie stets aufmerksam. Laura setzt sich für klare Kommunikationswege und die Verbesserung von Sicherheitsprozessen ein und hat ein besonderes Auge für die Datensicherheit.

Motivationen

- Schutz sensibler Daten der Bürger und der Behörde
- Kontinuierliche Verbesserung der Sicherheitsprozesse
- Arbeit im öffentlichen Interesse

Ziele

- Gewährleistung eines hohen Sicherheitsniveaus
- Effiziente Nutzung begrenzter Ressourcen
- Einhaltung rechtlicher Vorgaben

Technologische Fähigkeiten

- Praktische Erfahrung mit verschiedenen Sicherheitstools
- Gute Kenntnisse der behördlichen Sicherheitsvorschriften
- Verständnis für die Wichtigkeit des Schutzes von sensiblen Daten

Frustrationen

- Permanente Überlastung
- Komplizierte Prozesse und bürokratische Hürden
- Druck, immer auf dem neuesten Stand der Technik zu sein
- Mangel an präzisen Informationen

Herausforderungen

- Umfangreiche Verantwortung bei begrenzten Ressourcen
- Notwendigkeit zur Multitasking-Fähigkeit
- Einhaltung strenger Datenschutzvorgaben

Kommunikationskanäle

- Behördliche Kommunikationswege
- Fachseminare
- Geschützte Online-Plattformen

Carsten Müller

»Bei einem Sicherheitsvorfall kommt es auf umgehendes Handeln an. Je mehr Informationen man zur aktuellen Situation hat, desto schneller kann man die Bedrohung beseitigen und schlimme Folgen verhindern.«

Übersicht

Alter: 42 Jahre

Position: IT-Sicherheitsleiter eines mittelständischen Unternehmens in der Pharma-Branche

Hauptaufgaben: Implementierung und Überwachung von Cybersecurity-Maßnahmen, Risikobewertung und Reaktion auf Sicherheitsvorfälle

Kurzbeschreibung

Carsten Müller ist seit vielen Jahren in der IT-Sicherheit beschäftigt und seit drei Jahren der Leiter der IT-Sicherheit bei einem großen Pharmaunternehmen. Er ist sehr erfahren und konnte schon einige Sicherheitsvorfälle erfolgreich verhindern und auch einen größeren Vorfall gemeinsam mit seinem Team beheben und dabei Schlimmeres verhindern.

Motivationen

- Prävention von Angriffen und Minimierung von Schäden
- Aufbau einer resilienten Sicherheitsinfrastruktur

Frustrationen

- Komplexe und unübersichtliche Zuständigkeiten im Bereich der Cybersicherheit
- Mangel an klaren Rückmeldungen von staatlichen Stellen

Ziele

- Schutz der Unternehmensdaten und -systeme vor Cyberangriffen, insbesondere vor APT-Angriffen und Supply Chain Angriffen

Herausforderungen

- Erkennung und Abwehr fortgeschrittener, u.a. lang andauernder Bedrohungen
- Zusammenarbeit mit Behörden und Austausch von Informationen ohne Verletzung des Geheimschutzes

Technologische Fähigkeiten

- Sehr erfahren im Umgang mit Sicherheitstechnologien
- Analyse von Indicators of Compromise (IoCs)
- Einrichtung und Verwaltung von verschlüsselten Kommunikationskanälen

Kommunikationskanäle

- Direkter Austausch via Telefon oder E-Mail
- Vertrauliche Kommunikation über gesicherte Kanäle

Bernd Brücke

»In der IT-Sicherheit sollte man den Willen haben, täglich Neues zu lernen und ebenso kreativ zu werden wie die Angreifer.«

Übersicht

Alter: 47 Jahre

Position: Leiter des Computer Emergency Response Teams (CERT) eines großen Industrieunternehmens

Hauptaufgaben: Koordination der Reaktion auf Sicherheitsvorfälle, Entwicklung von Empfehlungen für präventive wie auch reaktive Maßnahmen bei sicherheitsrelevanten Vorfällen in IT-Systemen.

Kurzbeschreibung

Bernd Brücke ist Experte für Prävention und Reaktion bei IT-sicherheitsrelevanten Vorfällen. Er hält sich technologisch und methodisch immer auf dem Laufenden, um auch die neusten Angriffsmethoden im Detail zu kennen und hierdurch Gefahren schneller zu erkennen und Lösungsansätze für den Ernstfall zu entwickeln.

Motivationen

- Gewährleistung eines effektiven und sicheren Informationsaustauschs
- Förderung der Resilienz gegenüber Cyberbedrohungen

Frustrationen

- Datenschutzbeschränkungen, die den Austausch von Informationen behindern
- Herausforderungen bei der Skalierbarkeit des Informationssharing

Ziele

- Aufbau und Pflege eines Netzwerks für den Austausch von Cyberthreat Intelligence
- Verbesserung der Anonymisierung von Daten

Herausforderungen

- Mangel an verlässlichen IoCs
- Schwierigkeiten bei der Qualitätssicherung von Daten
- Aufbau von Vertrauensbeziehungen (intern/extern)

Technologische Fähigkeiten

- Expertenwissen im Bereich Threat Intelligence Sharing und Analyseplattformen wie MISP
- Erfahrung in der Handhabung von IT Security Tools

Kommunikationskanäle

- CERT-Netzwerke
- Vertrauliche Foren
- Spezialisierte Sicherheitsplattformen

Karin Schulz

»Für die IT-Sicherheit unseres Unternehmens wünsche ich mir klare und konkrete Handlungsempfehlungen, die auf unsere Bedürfnisse zugeschnitten sind.«

Übersicht

Alter: 38 Jahre

Position: Geschäftsführerin eines mittelständischen Produktionsunternehmens

Hauptaufgaben: Strategische Unternehmensführung, Gewährleistung der Betriebssicherheit, Einhaltung von Compliance-Richtlinien

Kurzbeschreibung

Karin Schulz führt ein mittelständisches Produktionsunternehmen, das sich in einer komplexen und oft bedrohlichen Sicherheitsumgebung zurechtfinden muss, aber nicht über die Ressourcen großer Konzerne verfügt. Sie ist fleißig, ehrgeizig und zielstrebig. In Sachen IT-Sicherheit wünscht sie sich kostengünstige und übersichtlichere Informationen und Werkzeuge.

Motivationen

- Schutz des Unternehmens vor Cyberangriffen
- Vermeidung von Betriebsunterbrechungen
- Sicherung der Wettbewerbsfähigkeit

Frustrationen

- Komplexität der Cybersecurity-Landschaft
- Unsicherheit über den Umgang mit IT-Systemen
- Überforderung durch Masse an Informationen

Ziele

- Erreichen eines hohen IT-Sicherheitsniveaus ohne übermäßige Investitionen
- Effektive Nutzung von Ressourcen für maximalen Schutz

Herausforderungen

- Fehlendes Wissen über aktuelle Bedrohungslagen
- Begrenzte Ressourcen für IT-Sicherheit
- Vertrauen in externe Datenquellen
- Abhängigkeit von externen Dienstleistern für tiefgehendes technisches Wissen

Technologische Fähigkeiten

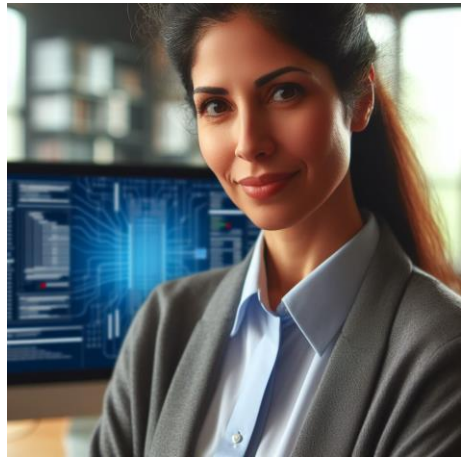
- Grundkenntnisse in IT und Cybersecurity
- Analytisches Verständnis

Kommunikationskanäle

- Direkter Kontakt mit vertrauenswürdigen Sicherheitspartnern
- Branchenspezifische Informationsveranstaltungen

Sarah Baumgartner

KRITIS



»Mein Ziel ist es, dass unsere Systeme immer laufen - sicher, effizient und ohne Ausfallzeiten.«

Übersicht

Alter: 32 Jahre

Position: IT-Systemadministratorin

Hauptaufgaben: Betreuung der IT- und OT-Systeme, Durchführung von Updates und Patches, Reaktion auf Sicherheitswarnungen

Kurzbeschreibung

Sarah Baumgartner ist IT-Systemadministratorin bei den Stadtwerken Energetik GmbH. Sie ist zuständig für die operative Aufrechterhaltung und Sicherheit der IT- und OT-Systeme des Energieversorgers. Trotz ihrer tiefgreifenden technischen Kenntnisse, hat sie viele Aufgaben und steht unter ständigem Zeitdruck.

Motivationen

- Sicherstellung der Systemintegrität
- Effiziente Problemlösung
- Beitrag zur Unternehmenssicherheit

Frustrationen

- Hoher Arbeitsdruck
- Begrenzte Ressourcen
- Fehlen von automatisierten Prozessen

Ziele

- Aufrechterhaltung eines störungsfreien Betriebs der IT-Infrastruktur

Herausforderungen

- Zeitmanagement angesichts vieler Aufgaben
- Priorisierung und Identifikation relevanter Meldungen
- Schnelle Reaktion auf Sicherheitswarnungen ohne Betriebsunterbrechung

Technologische Fähigkeiten

- Tiefgehendes Verständnis von IT- und OT-Systemen
- Praktische Erfahrungen mit Incident Management

Kommunikationskanäle

- Technische Dokumentationen
- Konzern-interne Plattformen
- E-Mails
- Fachworkshops

Michael Vogt

KRITIS

»Wir müssen unser Unternehmen sicher und zukunftsorientiert aufstellen, ohne dabei die Kosten aus den Augen zu verlieren.«

Übersicht

Alter: 45 Jahre

Position: Geschäftsführer

Hauptaufgaben: Strategische Unternehmensführung, Budgetverantwortung, Stakeholder-Management

Kurzbeschreibung

Michael Vogt ist Geschäftsführer einem regionalen Wasserversorger. Er überblickt das Gesamtgeschehen des Unternehmens und ist für strategische Entscheidungen verantwortlich. Als Nicht-Techniker hat er keine spezifische Security-Expertise, muss jedoch sicherstellen, dass das Unternehmen sowohl sicher als auch wirtschaftlich effektiv betrieben wird.

Motivationen

- Langfristiger Unternehmenserfolg
- Kostenoptimierung
- Risikominimierung

Frustrationen

- Komplexität technischer Entscheidungen
- Schwierigkeiten bei der Bewertung von IT-Sicherheitsrisiken

Ziele

- Gewährleistung der Unternehmensstabilität und Wettbewerbsfähigkeit
- Einfache Lagebeurteilung
- Realisierung von Mehrwerten für das Unternehmen

Herausforderungen

- Abwägung zwischen Investitionen in Sicherheit und anderen Unternehmensbereichen ohne technische Expertise

Technologische Fähigkeiten

- Grundverständnis für IT- und Sicherheitslösungen

Kommunikationskanäle

- Geschäftsberichte
- Präsentationen
- Direkter Austausch mit Abteilungsleitern

Dr. Julia Schneider

KRITIS

»Sicherheit ist keine Kostenfrage, sondern eine Frage der Unternehmenszukunft.«

Übersicht

Alter: 38 Jahre

Position: Leiterin der Informationssicherheit

Hauptaufgaben: Entwicklung und Implementierung von Sicherheitsstrategien, Risikobewertung, Überwachung von Sicherheitsvorfällen

Kurzbeschreibung

Dr. Julia Schneider ist die Leiterin der Informationssicherheit bei einem großen deutschen Energiekonzern. Sie hat einen starken Hintergrund in der Cybersecurity und ist verantwortlich für die Implementierung und Aufrechterhaltung von Sicherheitsstrategien. Sie ist überzeugt von der Wichtigkeit eines robusten Sicherheitskonzepts.

Motivationen

- Stärkung der Unternehmensresilienz gegen Cyberangriffe
- Förderung einer starken Sicherheitskultur

Frustrationen

- Begrenzte Entscheidungsmacht bei Budgetfragen
- Begrenzte Ressourcen, insb. auch Fachkräfte

Ziele

- Sicherstellung der Unternehmenssicherheit
- Implementierung effektiver Sicherheitslösungen
- Schnelle Erkennung auch neuester Angriffsmethoden

Herausforderungen

- Überzeugung der Geschäftsführung von Sicherheitsinvestitionen ohne direkte Budgetverantwortung
- Screening hoher Anzahl von sicherheitsrelevanten Meldungen
- Heterogenität und Alter der Systeme

Technologische Fähigkeiten

- Expertin in Cybersecurity
- Erfahrung mit SIEM-Systemen und Incident Response

Kommunikationskanäle

- Direkter Austausch mit Branchenkolleg*innen
- Direkte Kommunikation mit anderen Sicherheitsexperten
- Konzern-interne Plattformen
- E-Mail

Lukas Weber

»Fallen unsere IT-Systeme aus, können wir unseren Bürgerinnen und Bürgern nur sehr begrenzte Dienstleistungen anbieten.«

Übersicht

Alter: 53 Jahre

Position: Bürgermeister einer kleinen Gemeinde

Hauptaufgaben: Leiter der Gemeindeverwaltung, Vorsitzender des Gemeinderats, Repräsentant der Gemeinde.

Kurzbeschreibung

Lukas Weber ist in seiner zweiten Amtszeit als Bürgermeister der Gemeinde Stronzberg mit insgesamt ca. 8.000 Einwohnern. Er leitet die Verwaltung und vertritt die Gemeinde repräsentativ und manchmal auch vor Gericht. Zudem steht er dem Rat vor. Die Gemeinde teilt sich einen IT-Dienstleister, der sich auf kommunale IT spezialisiert hat, zusammen mit den Nachbargemeinden.

Motivationen

- Schnellstmögliche Bearbeitung der Dienstleistungen für die Bürgerinnen und Bürger.
- Sichere Übertragung der (personenbezogenen) Daten der Bürgerinnen und Bürger.

Frustrationen

- Abhängigkeit von einem IT-Dienstleister.
- Fehlende Digitalisierung in verschiedenen Bereichen bzw. digitaler Bruch innerhalb von Prozessketten.

Ziele

- Erweiterung der (digitalen) Angebote für Bürgerinnen und Bürger.
- Schnellere Bearbeitung von Anträgen und Formularen.
- Erfolgreichen Ransomware-Angriff auf die Gemeinde vermeiden.

Herausforderungen

- Keine IT-Expertise in der Verwaltung.
- Ältere Bürgerinnen und Bürger benötigen persönliche Assistenz bei der Nutzung digitaler Angebote.

Technologische Fähigkeiten

- Nutzung der kommunalen Anwendungen.
- Microsoft Word + Excel.
- HTML-Einsteigerkurs an der Volkshochschule Mitte der 90er Jahre .

Kommunikationskanäle

- Kontakt mit IT-Dienstleister per E-Mail und Telefon.
- Treffen mit anderen Bürgermeistern zum Thema IT-Sicherheit.
- Informationsveranstaltungen für Gemeinden zum Thema IT-Sicherheit.