Facharbeitermangel meets Hackerangriff

(ISC)^2 ISACA Konferenz 2023

pwc

Vorstellung

Rudolf Werner

Cybersecurity & Privacy Manager

Wien, Österreich

+43 699 1630 0262

rudolf.werner@pwc.com

Michael Pummer

Cybersecurity & Privacy Manager

Wien, Österreich

+43 699 1630 5639

michael.pummer@pwc.com

Facharbeitermangel meets Hackerangriff

Definition von Facharbeitermangel in der Cybersecurity

- Fehlende Bewerbungen von Cybersecurity Expert:innen
- In Österreich fehlen aktuell doppelt so viele Fachkräfte im Bereich Cybersecurity, wie in Deutschland

Bedeutung des Themas für Unternehmen und Gesellschaft

- Fehlende Qualifikationen führen zu nicht besetzten Stellen
- Kleine Gruppe an top qualifizierte Fachkräfte können sich den Job aussuchen
- Weiter steigendes Gehaltsniveau
- Kleinere Unternehmen können nicht mithalten

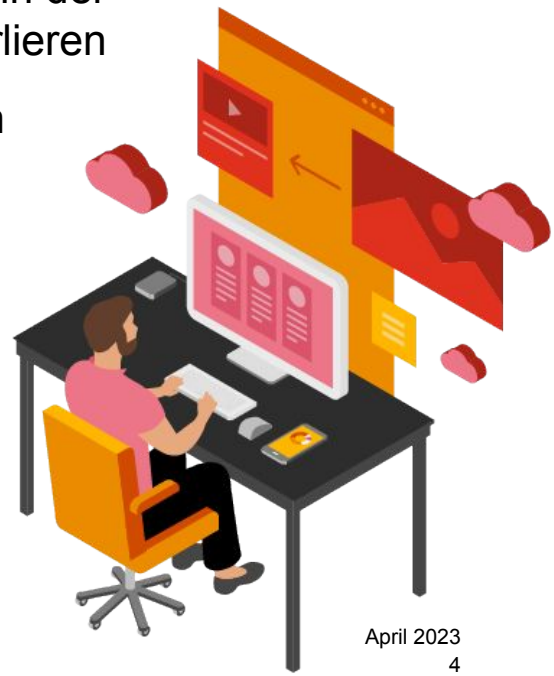
Digitalisierung der Gesellschaft und Wirtschaft als Treiber des Facharbeitermangels

Ursache

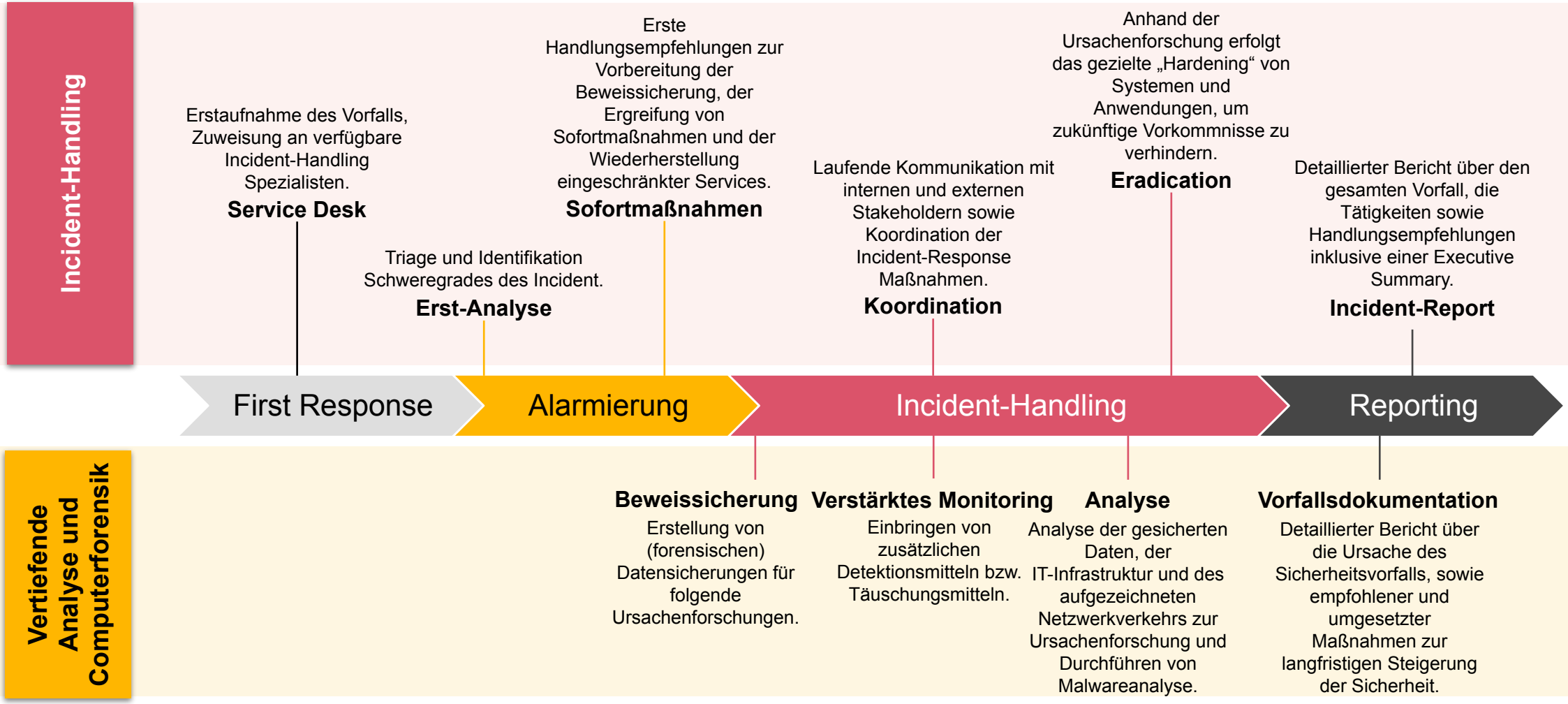
- Steigende **Bedrohungslage** sowie komplexere **Problemstellungen** führen zu **höheren Anforderungen** an die **Bewerber:innen** und dadurch höhere Ausbildungsniveaus
- **Ausbildungsmöglichkeiten** bzw. interessierte Bewerber:innen nur begrenzt verfügbar.
- Rapider **technologischer Fortschritt** auf der Seite der **Unternehmen** (Prävention) aber auch bei den eingesetzt Tools der **Bedrohungsakteure** (Response)
- **Zunahme** der Anzahl erfolgreicher **Hackerangriffe** mit gesteigerten Auswirkungen (**Ransomware aaS**)
- Steigerung der **regulatorischen Anforderungen** sowie der **Komplexität** in der Umsetzung (DORA, NISG,...)

Folgen

- Das **Risiko** für erfolgreiche **Cyberangriffe steigt** seit Jahren kontinuierlich an.
- Der Fachkräftemangel führt dazu dass Unternehmen sowohl in **Prävention** als auch in der **Response** weiter an Boden verlieren
- **Verlust** von hochspezialisierten **Personals** wegen Überlastung
- **Hohe Kosten** für Unternehmen in einer bereits angespannten Budgetsituation
- **Beschleunigter Trend** zu Cloud Lösungen



Hackerangriff aus Unternehmenssicht



Notwendiges Personal für die Reaktion auf Hackerangriffe vs. die jährlichen Kosten

- **Redundanz -** Urlaub, Krankenstand, Bereitschaftsdienste etc.
- **Auslastung -** Sonstige (sinnstiftende) Aufgaben für den Normalbetrieb finden
- **Ausbildung / Praxis -** Schneller Wandel der Bedrohungslage
- **Risiko -** Verlust der Investition durch Austritt, Veränderung intern etc.

Was bedeutet ein IR Einsatz für die Mitarbeiter:innen

Incident Response Einsatz rund um die Uhr!

Auswirkung auf Mitarbeiter

- **Druck -** Wann ist das System wieder verfügbar?
- **Stress -** Einsatz, Schlafen, Einsatz, keine freien Tage, Absage von Urlauben etc.
- **Angst -** Verlust meines Arbeitsplatzes?
- **Kompetenzlosigkeit -** Schaffe ich das?

Gefahr - Was haben wir beobachtet

- **Stressreaktionen**
- **Burnout**
- **Kündigung**
- **Konflikte brechen wieder auf**

Lösung des Problems durch Incident Response Retainer Services

Schnelligkeit

- **Remote Support** für die Einleitung von Sofortmaßnahmen.
- **Onsite Support** direkt beim Unternehmen und gemeinschaftliche Bewältigung des Incidents.
- **International Support** um Mitarbeiter:innen vor Ort zu unterstützen.

Effektivität

- **Kontinuierlicher Aufbau** der Incident **Readiness** für das Unternehmen durch Anpassung von **Prozessen** und **vorbereiteten Unterlagen.**
- Sicherstellen der **Kommunikations- und Kollaborationsfähigkeiten,** um im Incident Handlungsfähig zu bleiben.

Expertise

- **Skalierbare** Anzahl an Incident Response und Digital Forensic **Experten**
- **Spezialthemen** wie Malware-Analyse, Threat Intelligence, OT-Security, Business Continuity & Recovery etc.

Wir machen es Ihnen leicht, es Hackern schwer zu machen

Trust in Transformation: Vertrauen Sie auf einen Partner, der mit Ihnen flexible Strategien für sich schnell wandelnde Bedrohungen entwickelt und Abwehrmechanismen implementiert, mit denen Sie Angreifer in die Verzweiflung treiben:

www.pwc.at/cyber

pwc

(ISC)²/ISACA Konferenz 2023