Probando
We love Studies

Datenintegrität und Cybersicherheit aus der Perspektive eines Health-Startups:

Herausforderungen und Umsetzung aktueller Normen und Richtlinien

Gernot Winkler
17.10.2024

Über Probando

Rekrutierung von Probanden und Auszahlung von Aufwandsentschädigungen über eine Web Plattform

- *Studien, Umfragen, Produkttests etc.*

Kunden

- *Pharma, CRO’s, Universitäten etc.*

–> *Medizinische Daten, Bankdaten, regulierte Unternehmen*

Datenintegrität

Korrektheit, Vollständigkeit und Konsistenz von Daten

- *Input Validierung*
- *Daten Validierung*
- *keine redundanten Daten*
- *Backups*
- *Zugriffskontrollen*
- *Audit Trails*

–> *<u>Datensicherheit ist ein relevanter Teil der Datenintegrität</u>*

Cybersecurity

Schutz von Systemen, Netzwerken und Programmen vor digitalen Angriffen

Angriffe

- *Phishing (Spear-Phishing, Whaling, Vishing, Email Phishing)*
- *Malware (Ransomware, Adware)*
- *Denial-of-Service (DoS)*
- *Password Attacks*
- *SQL Injection, Cross-Site Scripting (XSS)*
- *Man-In-The-Middle-Angriff (MITM)*

  ect…

Cybersecurity

Zahlen & Fakten

2,365

cyberattacks in 2023, with 343.338.964 victims [1]

72%

increase in data breaches since 2021 [1]

$4.88 M

is the global average cost of a data breach in 2024 [2]

35%

of malware delivered via email in 2023 [3]

94%

of organizations have reported email security incidents [4]

$2.9 B

losses in 2023 business email compromises [5]

32%

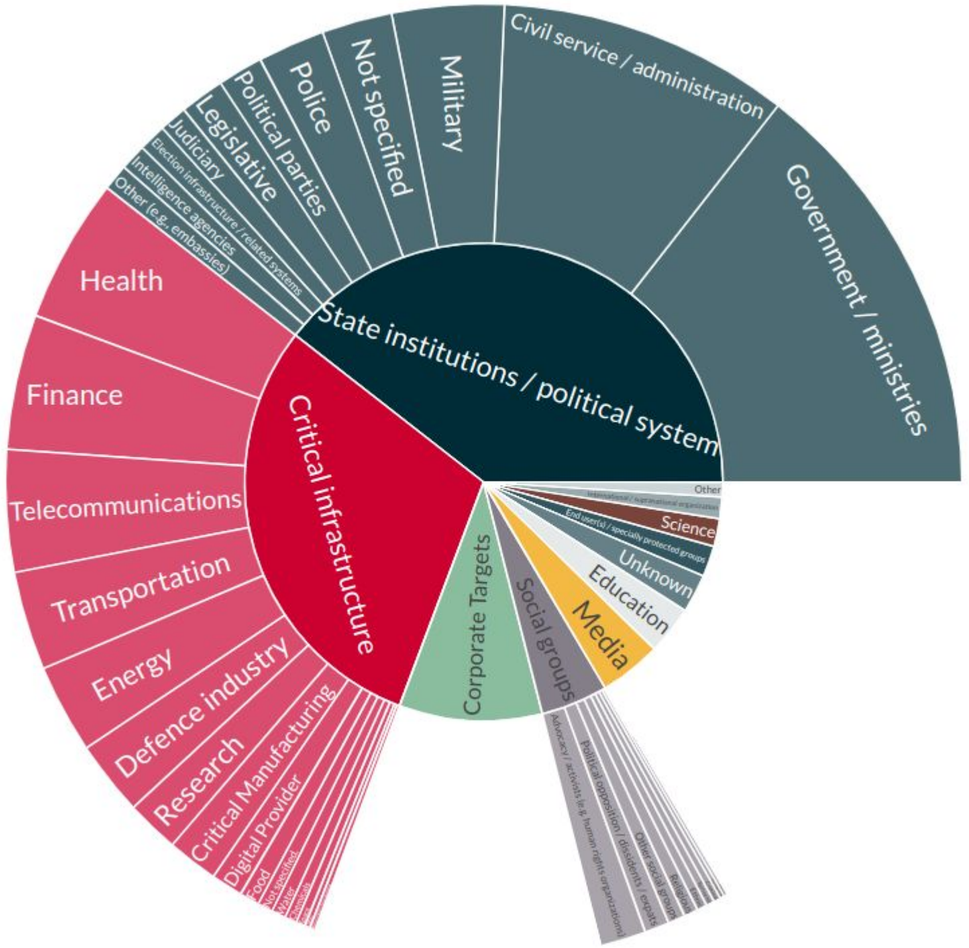
growth of Information security jobs projected [6]

1 Identity Theft Resource Center 2023 Data Breach Report
2 IBM Cost of a Data Breach Report 2024
3 Verizon 2023 Data Breach Investigation Report
4 Egress 2024 Email Risk Security Report
5 FBI Internet Crime Report 2023
6 BLS Occupational Outlook Handbook: Information Security Analyst

Cybersecurity

European Repository of Cyber Incidents (EuRepoC)

01.01.2000 - 10.10.2024



Herausforderungen

Startups

- *Begrenzte Ressourcen, Kosten*
- *Vertrauensbildung mit Kunden (Kundenanforderungen)*
- *QMS Etablierung, Prozess Etablierung*
- *Einhaltung der Regularien, international und speziell im Gesundheitsbereich*
  ISO 27001, NIS2, IEC 81001-5-1, DSGVO, GCP, HIPAA, HITECH Act, CCPA ect.
- *Skalierbaren Lösungen*
- *Agilität vs. Regularien*

ISMS allgemein

Ansatz:

- *Kunden Fokus*
- *Prozess Ansatz*
- *Risikobasiertes Denken*

Ziele:

- *Vertraulichkeit*
- *Verfügbarkeit*
- *Integrität*

ISMS - Cybersecurity

Angriffsflächen

- *Hardware*
- *Software*
- *Passwörter*
- *Arbeitsplatz*
- *Online-Anwendungen*
- *Datenübertragung*
- *Datenspeicherung*

  ect…

–> *<u>Angriffsflächen minimieren</u>*

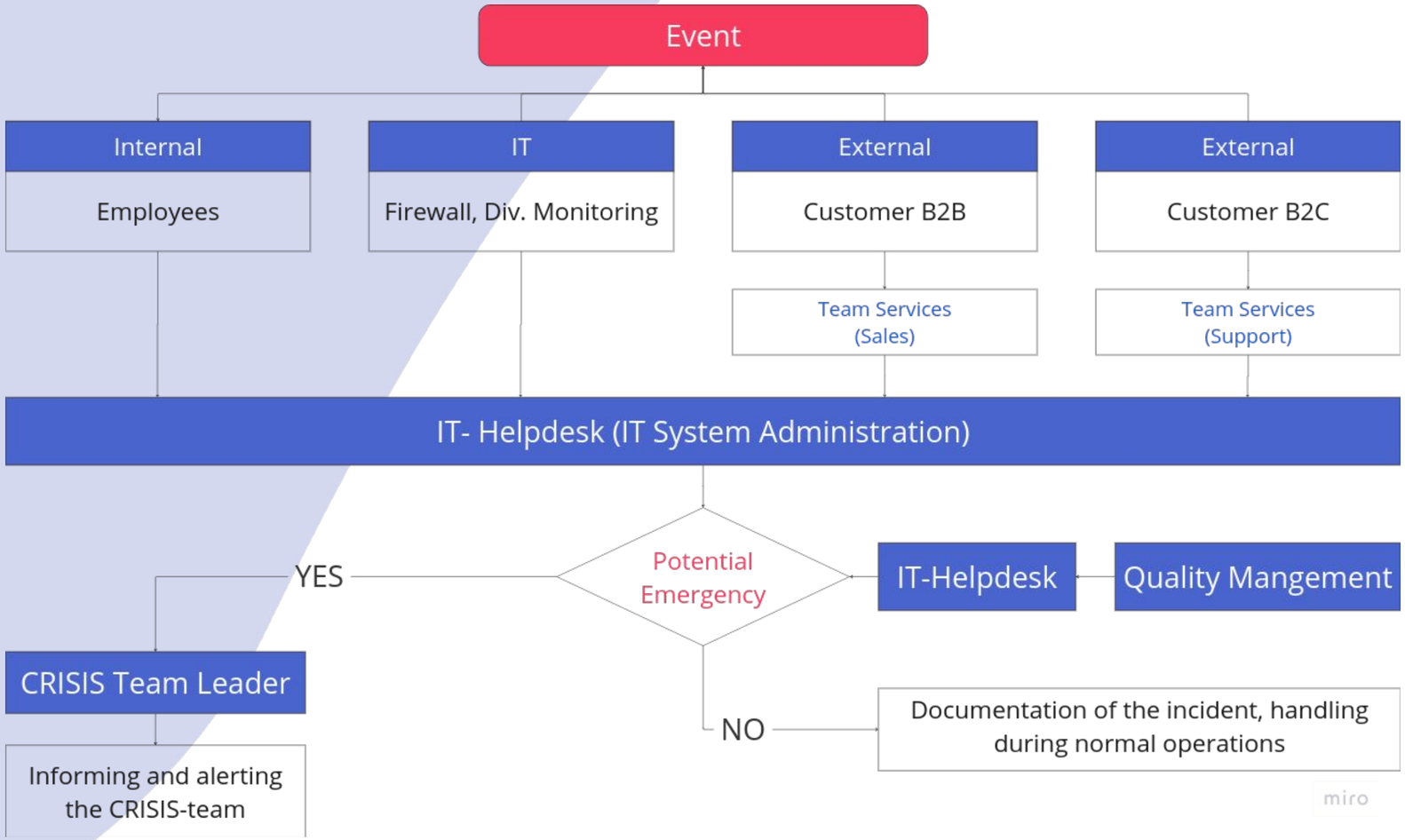
ISMS - Cybersecurity

Monitoring und Evaluierung

- *Technische Kontrollen - Logging, Alarme etc.*
- *Zugriffskontrollen und Rechtemanagement ect…*

–> *<u>Angriffe rechtzeitig erkennen</u>*

Security Incident Response



Bsp.Alarmierung und Kommunikation

Security Incident Response

US-CERT Incident Kategorien:

- *Test Blue Team / Red Team*
- *Unautorisierte Zugriff*
- *Unautorisierte Benutzung*
- *Scans / Zugriffsversuche*
- *Fehlfunktionen*
- *Verdachtsfall / Ermittlungsfall*
- *Phishing*
- *Denial of Service (DoS)*
- *Malware*

Bewertung von sicherheitsrelevanten Vorfällen bezogen auf deren Auswirkungen

- *Störung - Level 1*
  Störungen werden in der Regel im Rahmen des normalen, täglichen Betriebs durch die allgemeine Organisationsstruktur der Organisation behoben.
- *Notfall - Level 2*
  Notfälle sind Unterbrechungen des Geschäftsbetriebs, die mindestens einen zeitkritischen Geschäftsprozess betreffen, der nicht innerhalb der maximal tolerierbaren Ausfallzeit wieder in den Normalbetrieb überführt werden kann.
- *Krise - Level 3*
  Unter einer Krise versteht man ein Schadensereignis, das massive negative Auswirkungen auf das Unternehmen hat und dessen Auswirkungen auf die Organisation im Normalbetrieb nicht bewältigt werden können.

Schlussfolgerungen:

- *Sicherheit ist eine Schlüsselkomponente für den Geschäftserfolg*
- *Maßnahmen zur Cyber Sicherheit und Datenintegrität von Anfang an*
- *Balance zwischen Agilität und notwendigen komplexen Regularien*

Vielen Dank für Ihre Aufmerksamkeit!