KANTON AARGAU

Menschen machen Zukunft

DEPARTEMENT
FINANZEN UND RESSOURCEN

Informationssicherheit

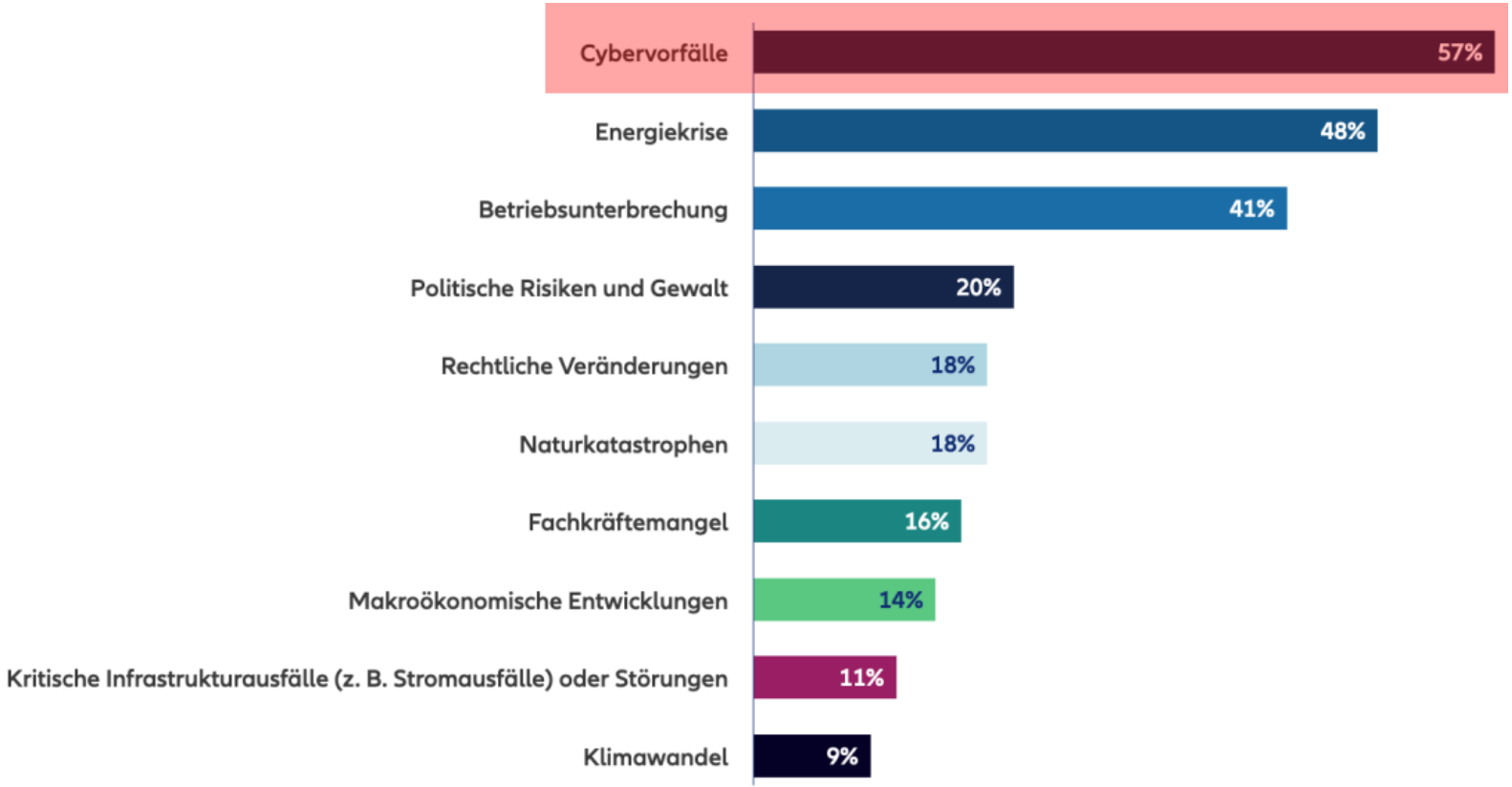
Behörden sind gefordert

7. November 2024

CISO – Öffentlich C1

AUSGANGSLAGE

Allianz Risk Barometer 2023



Die Akteure – Beispiele

- **Devisenbeschaffung**
  - Nord Korea > 4000 Cyber-Angriffsspezialisten

- **Störung öffentlichen Lebens**
  - Russland - hybride Kriegsführung (Fancy Bear, APT28)
  - DDoS und Hacking
    - Angriffe auf zivile und öffentliche Infrastrukturen

- Akteure arbeiten in der Regel nicht alleine
- Weltweiter professioneller Markt für Hacking-as-a-Service
- Exploit as a Service – Verkauf von Schwachstellen

Cybercrime in der CH

- > Aufwand sehr gering
- > Risiko minimal
- > Ertrag gigantisch
  - > Beispiel: 20 Mio Umsatz
    - – 20'000 Investition
    - – 12 Mio Geldwäsche Transfer
    - = ca. 8 Mio Gewinn

- 71% der Cyberangriffe finanziell motiviert
- 30% aller CH Unternehmen hatten bereits einen Ransomware-Vorfall (46% in KMU)
- 40% zahlen Lösegeld (KMU73%)
- 1000 Meldungen pro Woche bei NCSC
- 30'000 kriminelle Handlungen in der CH angezeigt
- 35% Aufklärungsrate für Cyberkriminalität (Ransomware <5%)
- 1,5 bis 7 Billionen Umsatz (höher als weltweiter Drogenhandel)
- Global (Länder / Grenzen / Souveränität existiert im Cyberraum nicht)

Ca 2-3 Cyberangriffe auf Behörden / Monat

- Gov / SmartServices ZH: Badiausweise, Name, Adresse, Telefonnummer und Foto
- Gov: KAPO BE, persönliche, private Telefonnummern
- Gov: Architekturbüro gehackt, Pläne aller Schweizer Botschaften
- Gov: Xplain, höchst sensible Daten bei MA des Dienstleisters
- Bildung: Basel Stadt, Zeugnisse, Krankenakten, Kantonsschulen, Berufsschulen
- Bildung: Kanton Waadt: Sonderschule, sehr sensible Informationen
- Health Care: Psychiatrische Klinik, Verschlüsselung, Gefahr von Veröffentlichung sensitiver Krankenakten
- Gemeinden: Rolle VD, Zollikofen BE, Baden AG
- Lieferanten: Concevis, Xplain, RUAG, Solarwinds, Citrix, Ivanti, Java (Log4j)
- International: https://konbriefing.com/de-topics/cyber-angriffe-oeffentliche-verwaltung.html

Wir sind gefordert

Eintrittswahrscheinlichkeit 100%

Auswirkung ?

Wo stehen wir bei der Verwaltung des Kanton Aargau bei der Cybersicherheit - ein paar Zahlen und Fakten

150'000 Benutzerkonten SmartAargau

13'000 Endpunkte

850 Applikationen

7000 Konten intern / 3000 extern

9'000 Sicherheitsmeldungen / Jahr

10-15 Vorfälle mit Analysen / Woche

1 vertiefte Analyse / Woche

5 Fälle im Monat mit sofortiger Gegenmassnahme

Ca. 100 Fälle mit automatisierten Gegenmassnahmen / Woche

6000 SPAM Mails / Tag

600 Phishing Mails / Tag

Was tun?

Gesetzliche Grundlagen (Gemeinden gehören zur kritischen Infrastruktur)

- Neues Informationssicherheits-Gesetz (InfoSig 2026)
- Datenschutzgesetz IDAG / VIDAG

Konzeptuelle Arbeit

- Risikoanalyse, Cyberrisiken in IKS / Risikomanagement der Gemeinde aufnehmen
- Sicherheitsrichtlinien nach "best practice" implementieren (Passwörter, Zugänge, Rechte, Multi-Factor)
- Notfallmanagement (wie weiter bei mehrtätigen Totalausfall/ BCM)
- Mitarbeiter Schulungen / Awareness
- Lieferantensicherheit
- Organisation (GL trägt Verantwortung)

Technische Massnahmen

- Verschlüsselung Daten
- Updates / Release Management
- Malwareschutz und Kontrollen (Logging, Monitoring)
- Backup Strategie (Ransomware Resistant Backup)

nicht abschliessend

Erhebungsmethodik jährlich / KTAG / BUND

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF
Bundesamt für wirtschaftliche Landesversorgung BWL
Fachbereich IKT

IKT-Minimalstandard - Assessment Tool

Version 1.11 April 2023 – Update NIST SP 800-53 Rev.5 – ISO 27001 2022

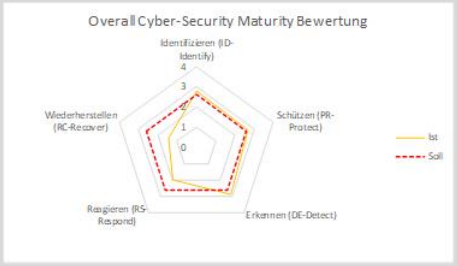
Anleitung und Erklärung zum Assessment-Tools

Das Assessment-Tool besteht aus 4 Registern (Erklärung, Assessment, Resultate und Hilfsfunktionen). Um das eigene Maturitätsniveau einzustufen werden alle 108 Aktivitäten im Reiter "Assessment" eingestuft. Dazu klicken Sie in der Spalte D (Bewertung) auf die entsprechende Zelle und können im Dropdown-Bereich den entsprechenden Wert auswählen:

Die Definition der Werte (Tier 0-4) kann dem Reiter "Hilfsfunktionen" entnommen werden. In der nebenliegenden Spalte "Kommentare" begründen Sie das definierte Maturitätsniveau für alle 108 Aktivitäten.

Darstellung der Resultate

Nachdem alle 108 Aktivitäten bewertet wurden, werden die Resultate im Reiter "Resultate" dargestellt. Die Resultate sind in ein "Overall Cyber Security Maturity Rating" sowie spezifische Resultate zu allen 5 Funktionen des Cyber-Security Frameworks unterteilt. Der IKT-Minimalstandard gilt dann als erfüllt, wenn das "Overall Cyber Security Maturity Rating" den Minimalvorgaben (Soll) entspricht:



Identifizieren
Schützen
Erkennen
Reagieren
Wiederherstellen

https://www.bwl.admin.ch/bwl/de/home/bereiche/ikt/ikt_minimalstandard.html

IKT-Minimalstandard

Identifikation → Schutz → Detektion → Reaktion → Wiederherstellung

GOVERNANCE

VORHER | WÄHREND | DANACH

Melden

KAPO +41 (0)62 835 80 90 / resp. 117

https://www.ag.ch/de/verwaltung/dvi/kantonspolizei/praevention/cybercrime

KTAG: security@ag.ch informieren.

Bund: Meldestelle bei Bund BACS (ehemals NCSC) wird ca. Q2/25 aufgeschaltet.

Kontakt

David Schlaginhaufen
Chief Information Security Officer
Informatik Aargau
Departement Finanzen und Ressourcen

Suhrenmattstrasse 48
5035 Unterentfelden

E-Mail: david.schlaginhaufen@ag.ch