technote&meet
Cyber Security

Branchentalk CHANCENLAND VORARLBERG

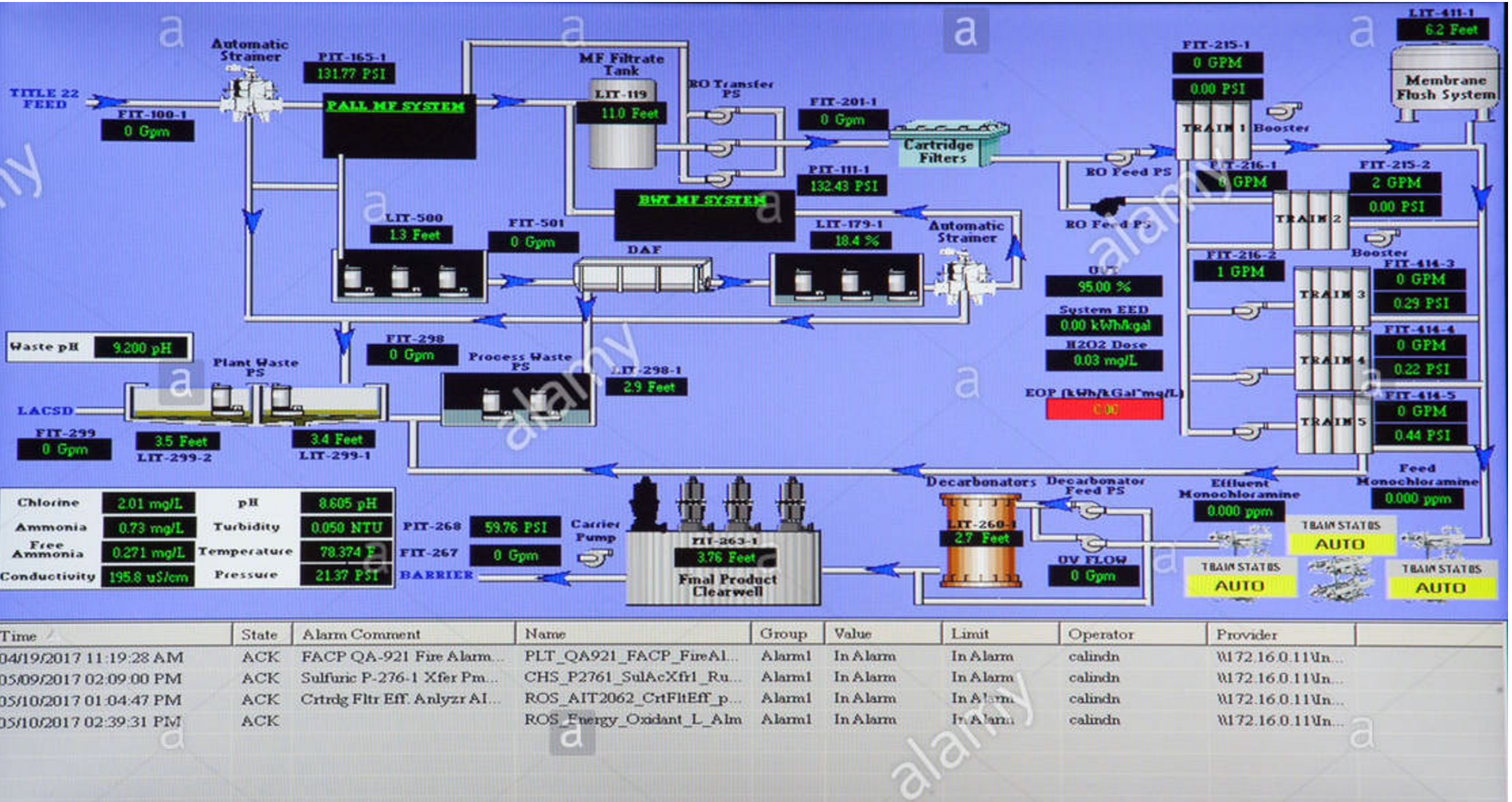
26. April 2021

Armin Simma

Die unheimliche *Maus. Der Film.*

Film-”Trailer” - low cost

Die unheimliche Maus. Der Film



Time	State	Alarm Comment	Name	Group	Value	Limit	Operator	Provider
04/19/2017 11:19:28 AM	ACK	FACP QA-921 Fire Alarm...	PLT_QA921_FACP_FireAl...	Alarm1	In Alarm	In Alarm	calindn	\\172.16.0.11\In...
05/09/2017 02:09:00 PM	ACK	Sulfuric P-276-1 Xfer Pm...	CHS_P2761_SulAcXfr1_Ru...	Alarm1	In Alarm	In Alarm	calindn	\\172.16.0.11\In...
05/10/2017 01:04:47 PM	ACK	Crtrdg Fltr Eff. Anlyzr AI...	ROS_AIT2062_CrtFltEff_p...	Alarm1	In Alarm	In Alarm	calindn	\\172.16.0.11\In...
05/10/2017 02:39:31 PM	ACK		ROS_Energy_Oxidant_L_Alm	Alarm1	In Alarm	In Alarm	calindn	\\172.16.0.11\In...

Die unheimliche Maus. Der Film

- Kein Film (Name/ Ort vorher frei erfunden)
- Aber: **Szenario ist real**
- **Florida Februar 2021**

- Köflach (Steiermark) **Stadtwerke**: April 2021 (allerdings ohne Erfolg)

Who am I?

- Armin Simma
- Im Bereich Informatik tätig seit über 30 Jahren
- seit 15 Jahren Schwerpunkt IT-Sicherheit
- Hochschullehrer an FHV seit 20 Jahren

- aktuelle Lehr- und Forschungsschwerpunkte:
  - IT-Sicherheit in Produktionsanlagen
  - Software-Sicherheit

E-Mail: armin.simma@fhv.at

Quelle: hydro.com

Quelle : https://www.tagblatt.ch

- Ähnliches kann aber auch jedes Unternehmen treffen.
- Auch kleine Betriebe (in Vlbg und Umgebung z.b.) nicht mehr uninteressant für Angreifer
- Hydro Aluminium, Nenzing

“Mich trifft das nicht, weil…” (zu klein, zu…)

Ähnliches kann aber auch jedes Unternehmen treffen.

Auch kleine Betriebe (in Vlbg und Umgebung z.b.) nicht mehr uninteressant für Angreifer

Mondelez (Suchard), Hydro Aluminium, Palfinger (Salzburg)…; vor einigen Jahren KMU im Bregenzerwald Opfer von Cyber Angriff; weitere sind mir bekannt;

Es gibt die Aussage: Es geht nicht darum, **ob** man angegriffen wird sondern **wann** und v.a. ob man rechtzeitig erkennt und reagiert.

Beispiele aus der Region

- Bsp: **Swisswindows** Mörschwil bei Rohrschach (Bodensee)**:**
  - CEO Nesa Meta : «Eine massive Cyberattacke auf unsere Systeme führte jedoch im Mai 2019 zu einem herben Rückschlag für unser Unternehmen.» **Unternehmen im Konkurs**
- Fatzer AG aus Romanshorn: Sept 2020

Quelle : https://www.tagblatt.ch

Vorarlberg

Walser GmbH, Rankweil

Walser IT-Systeme aufgrund einer Cyberattacke lahmgelegt

E-Mail-Verkehr nur eingeschränkt möglich/nicht möglich

Rankweil, 26. August 2019. Unsere IT-Systeme sind gesetzeswidrig angegriffen worden. In der Folge wurden alle IT-Systeme abgeschaltet. IT-Sicherheitsexperten

E-Mail-Betrug: Vorarlberger Firma zahlt 150.000 Euro

30. Jänner 2018, 10:54

11 POSTINGS

Mitarbeiterin überwies knapp 150.000 Euro ins Ausland – 83.000 Euro konnten zurückgeholt werden

Ein Technologie-Unternehmen im Bregenzerwald ist durch die Methode "CEO fraud" (Chef-Betrug) um rund 67.000 Euro betrogen worden. Eine Mitarbeiterin überwies in fünf Tranchen insgesamt knapp 150.000 Euro ins Ausland, in enger Zusammenarbeit der Kriminalpolizei mit der Haus-Bank konnten aber 83.000 Euro sichergestellt und rückgeführt werden, informierte am Dienstag die Vorarlberger Polizei.

Österreich

Angriff auf **österreichisches Hotel (Romantik Seehotel Jaegerwirt**) schafft es sogar in NY Times

- elektr. Türen durch Angreifer kontrolliert -> Erpressung

EUROPE

The New York Times

Hackers Use New Tactic at Austrian Hotel: Locking the Doors

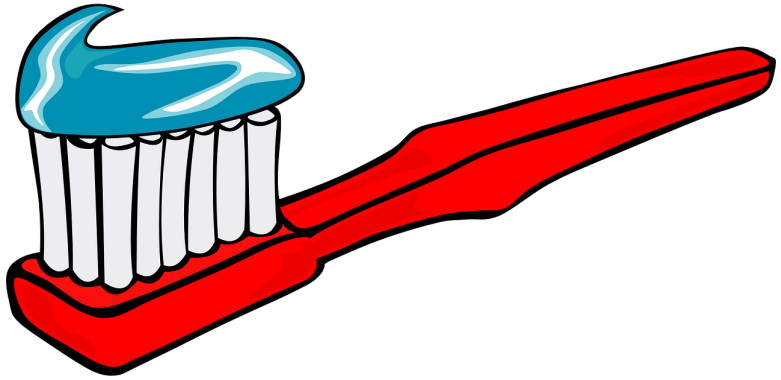
By DAN BILEFSKY JAN. 30, 2017

The ransom demand arrived one recent morning by email, after about a dozen guests were locked out of their rooms at the lakeside Alpine hotel in Austria.

The electronic key system at the picturesque Romantik Seehotel Jaegerwirt had been infiltrated, and the hotel was locked out of its own computer system, leaving guests stranded in the lobby, causing confusion and panic.

https://www.nytimes.com/2017/01/30/world/europe/hotel-austria-bitcoin-ransom.html?_r=0

Maßnahmen



- Hygiene
- So wie tägliches Zähneputzen, sind auch regelmäßige (einfache) Maßnahmen in IT-Sicherheit notwendig

Maßnahmen

- Updates
- Passwörter [1]
- Backup
- Awareness und Schulung von Mitarbeitenden
- Schwachstellenscan (alte Versionen von SW vorhanden?)
- Eventuell Pentrations-Test
- Übliche Technologien: Firewall, Virenscan…
- Produktionsunternehmen: Achtung auf “Alt-Systeme”

[1] Lustiges Video zu Passwort-Sicherheit: https://youtu.be/opRMrEfAIiI?t=42

Was sollte man mitbringen für Job/ Karriere in Cyber Sec?

- Neugierde
- Starkes technisches Interesse
- Keine “Angst” vor Technik
  -> “Herumprobieren” in IT-Systemen
- Durchhaltevermögen und hohe Aufmerksamkeit (Details oft wichtig)
- Laufendes Dazulernen
- Problemlöse-Kompetenz
- Methodisches/ Strukturiertes Vorgehen

Was sollte man mitbringen für Job/ Karriere in Cyber Sec?

- Vorab: Es gibt verschiedene (tw. sehr unterschiedliche) „Cyber Sec“- Bereiche, z.b.
  - Informationssicherheit (**Organisatorisch**, “High Level”, “Management”-nahe, People-Orientiert, weniger Technik
  - **Technische** Bereiche:
    - Netzwerk-Security
    - Pentesting
    - Incident Detection/ Response (SOC)
    - Forensik
    - Software-Sicherheit
    - Usw.

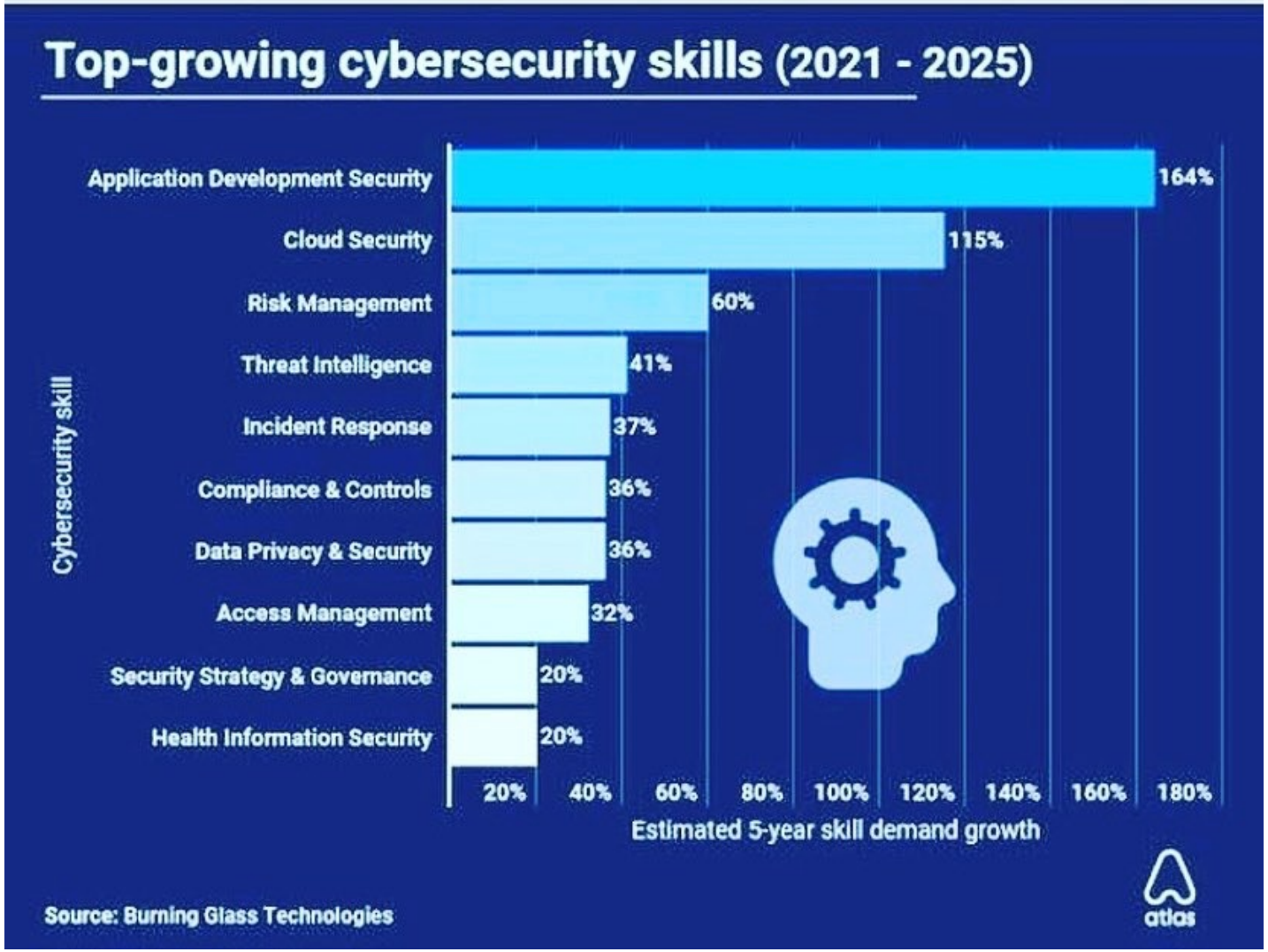
Was sollte man mitbringen für Job in Cyber Sec?

- Technische Details (Know-How)
  - Kann man erlernen!
- Virtualisierung (als Anwender)
- System-Administration
- Kommandozeile / Shell (insb. Linux)
- Computernetzwerke
- Web-Technologien

- Zum Teil aus *“Getting Into Cyber Security: 5 Skills You NEED to Learn”*
  - https://www.youtube.com/watch?v=Kx4y9c7w2JQ

[…] cyber security seems to be much harder to get into, but once you do… your value increases drastically and you get the benefit of being experienced and proven in a field with a **0% unemployment** rate.
-- Thomas; Incident Response Team

Quelle: Kommentare in https://insights.dice.com/cybersecurity-skills/

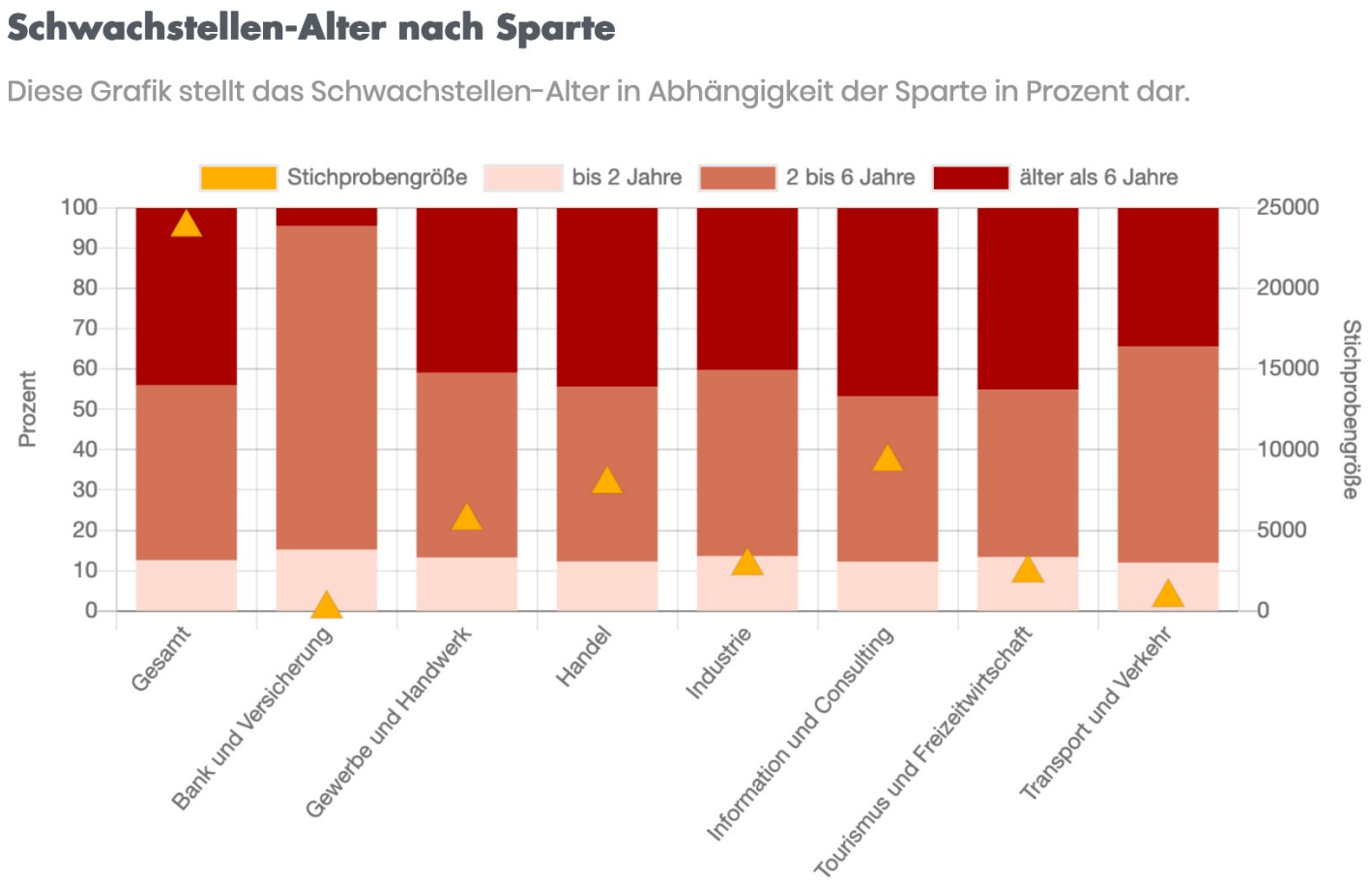


Cyber-Sec-Kurse von uns (FHV mit AIT)

- https://dih-west.at/events/einfuehrung-cyber-security-2/
- Kostenlos!
- Herbst 2021 oder Anfang 2022

- Bei Interesse bitte bei mir melden:
- armin.simma@fhv.at

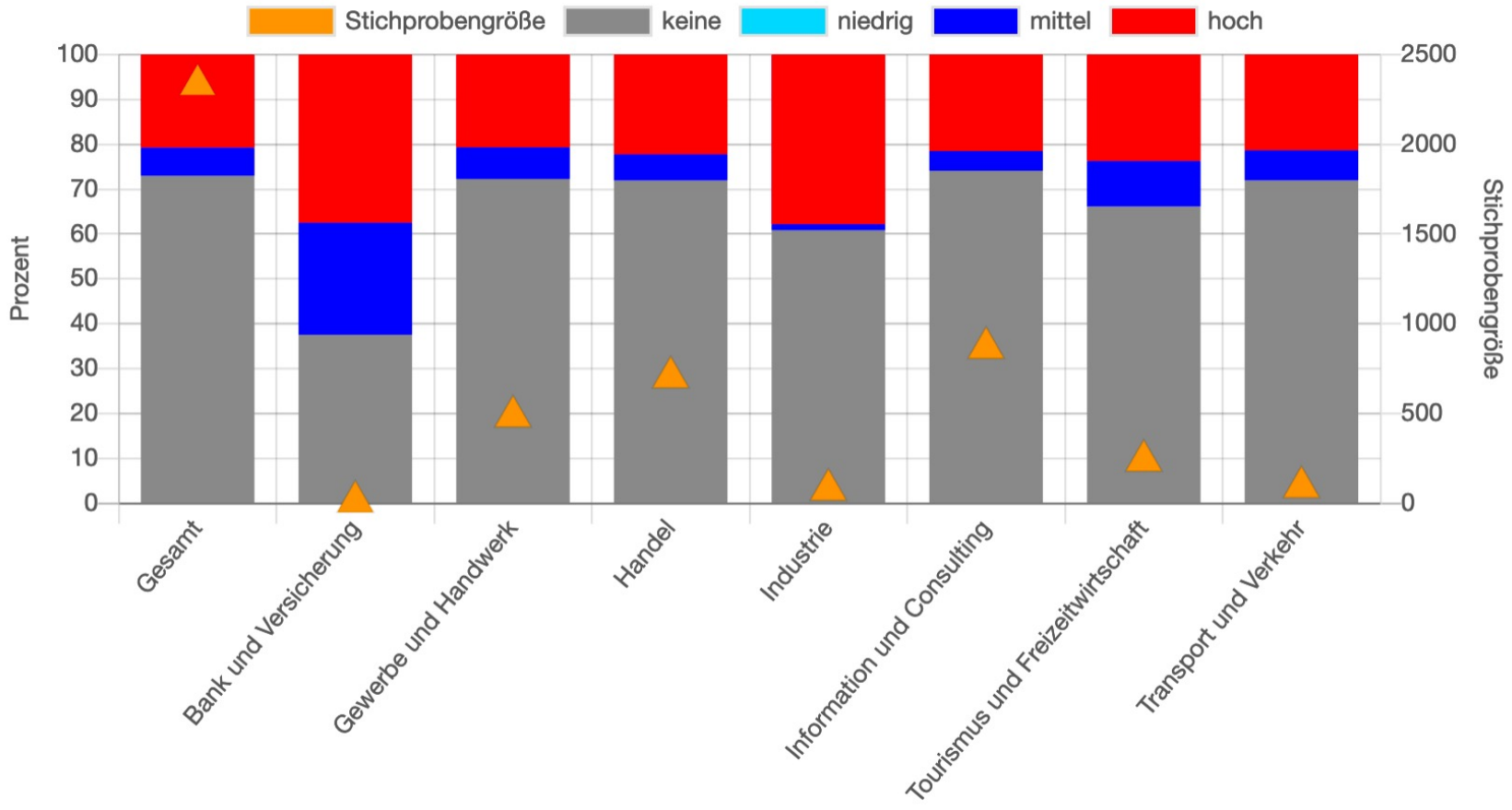
Bekannte Schwachstellen in Vlbg



Quelle: https://www.it-wachdienst.com/blog/osint-2020-vorarlberg/
Martin Herfurt

Schwachstellen-Kritikalität nach Sparte

Diese Grafik stellt die jeweils höchste Schwachstellen-Kritikalität der Unternehmen in Abhängigkeit der jeweiligen Sparte in Prozent dar.



Quelle: https://www.it-wachdienst.com/blog/osint-2020-vorarlberg/
Martin Herfurt