IT-Sicherheit – ein Thema für die Anwaltskanzlei

Christian Laux

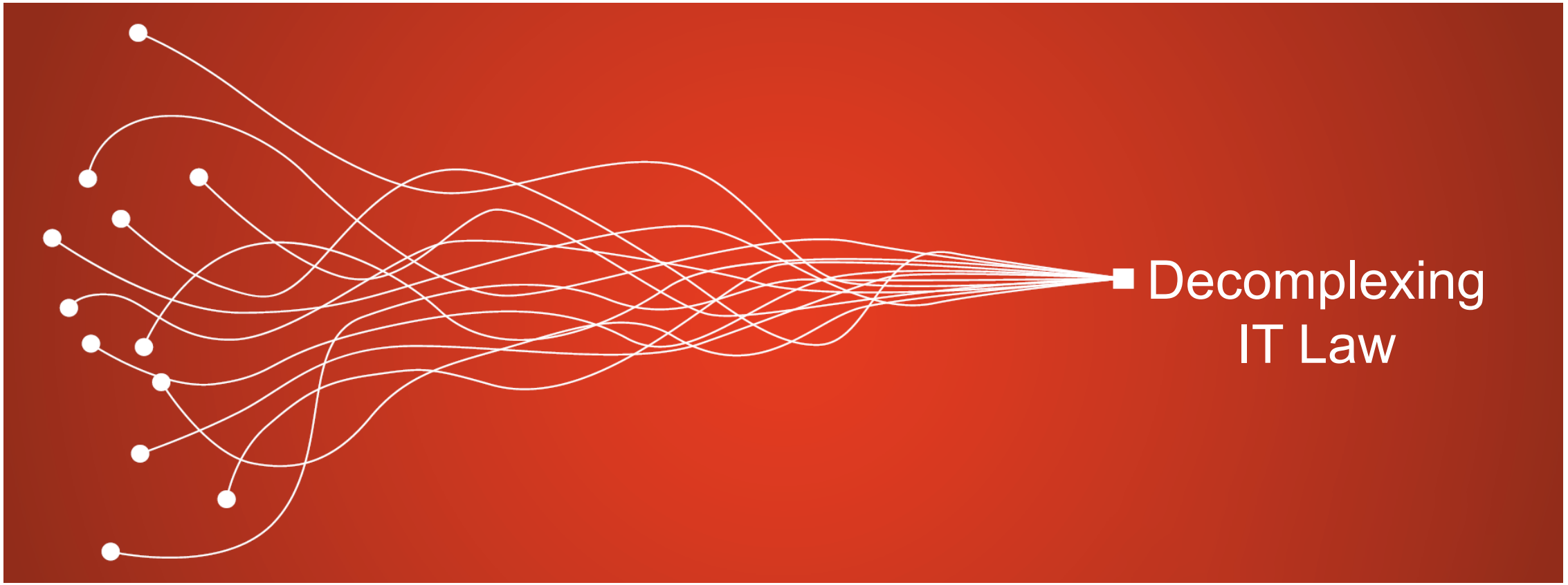
LAUX LAWYERS AG
ZURICH | BASEL

Datenschutz und Cybersecurity

SAV-Weiterbildungstage

14. September 2022

LAUX
LAWYERS AG
ZURICH | BASEL



Anwaltsrecht (Essentials)

(nicht mal dem Gericht)

Nicht ausplaudern

(nicht einmal wenn genehmigt)

Geheimnis

Konfliktverbot

Die Kanzlei schützen

(«Perimeter»)

(Versiegeln, wenn Polizei kommt)

Anwaltsgeheimnis als Kardinalpflicht

LAUX LAWYERS AG
ZURICH | BASEL

- Geheimnis als Kardinalpflicht der Anwaltschaft
- Organisatorische Entsprechung dieser Pflicht:
  - IT-Sicherheit
  - auch Kanzleien ohne Cloud (wohl eher: vor allem solche)

LAUX
LAWYERS AG
ZURICH | BASEL

Schutzziele

LAUX LAWYERS AG
ZURICH | BASEL

- Schutz vor **Ausfall** der unternehmensinternen IT
- Schutz vor **Störung von Abläufen**
  (Geschäftsabläufe, Produktion, BuHa)
- Schutz vor **Umsatzverlust** während Ausfallzeit
  („nicht geschriebene Minuten“)
- Vermeiden von **Schadenersatzpflichten**
  (Social Engineering nach Breach mit Schädigung von Klienten)

- Schutz der **Reputation**:
  - Unternehmen
  - Produkte
  - Repräsentanten
- Schutz vor **Datenverlust**
- **Geschäftsgeheimnisse**
  Anwaltsgeheimnis

Faktor Mensch

«Amateurs hack systems, professionals hack people» (Bruce Schneier)

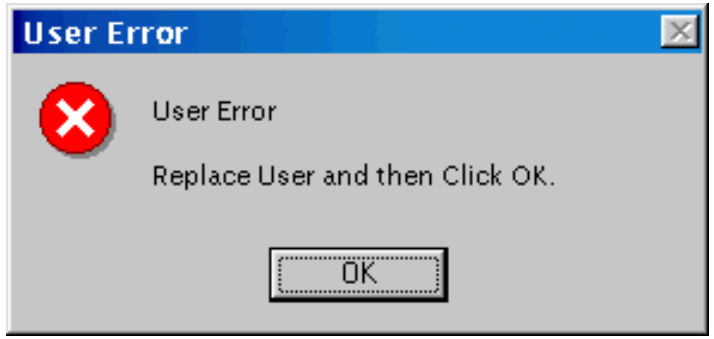
LAUX LAWYERS AG
ZURICH | BASEL

85% aller Angriffe starten beim Faktor Mensch.
Schnittstelle Mensch/Maschine bleibt Einstiegstor Nummer 1.

Mission Impossible v. «Hütchen-Spieler»

Faktor Mensch wirkt im Anwaltsmarkt eher verschärft:

- Berufsgattung mit Serviceorientierung:
  - hohe Erreichbarkeit (oft auch „Road Warriors“)
  - schnelles Arbeiten
- Information Workers:
  - rund um die Uhr Informationen speichern
  - schnell auf Informationen zugreifen können
- Netzwerker:
  - Anwältinnen sind neugierig (Anwälte auch)
  - Anwältinnen sind bereit, Interaktionen mit andern einzugehen (Anwälte auch)



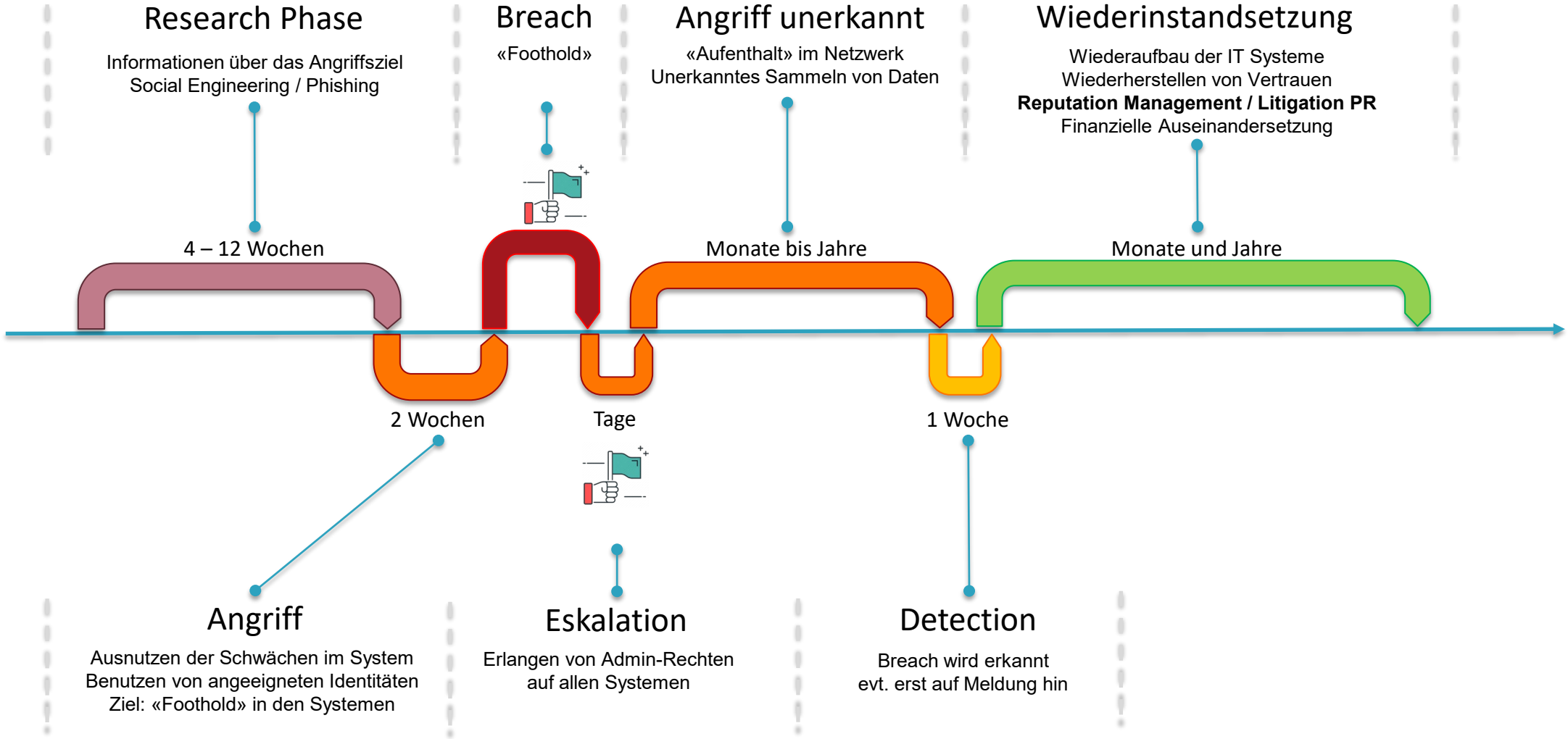
siehe aber Slide #13 …

Anwälte auf Sicherheit schulen – ein Ding der Unmöglichkeit?

Problembeschreibung

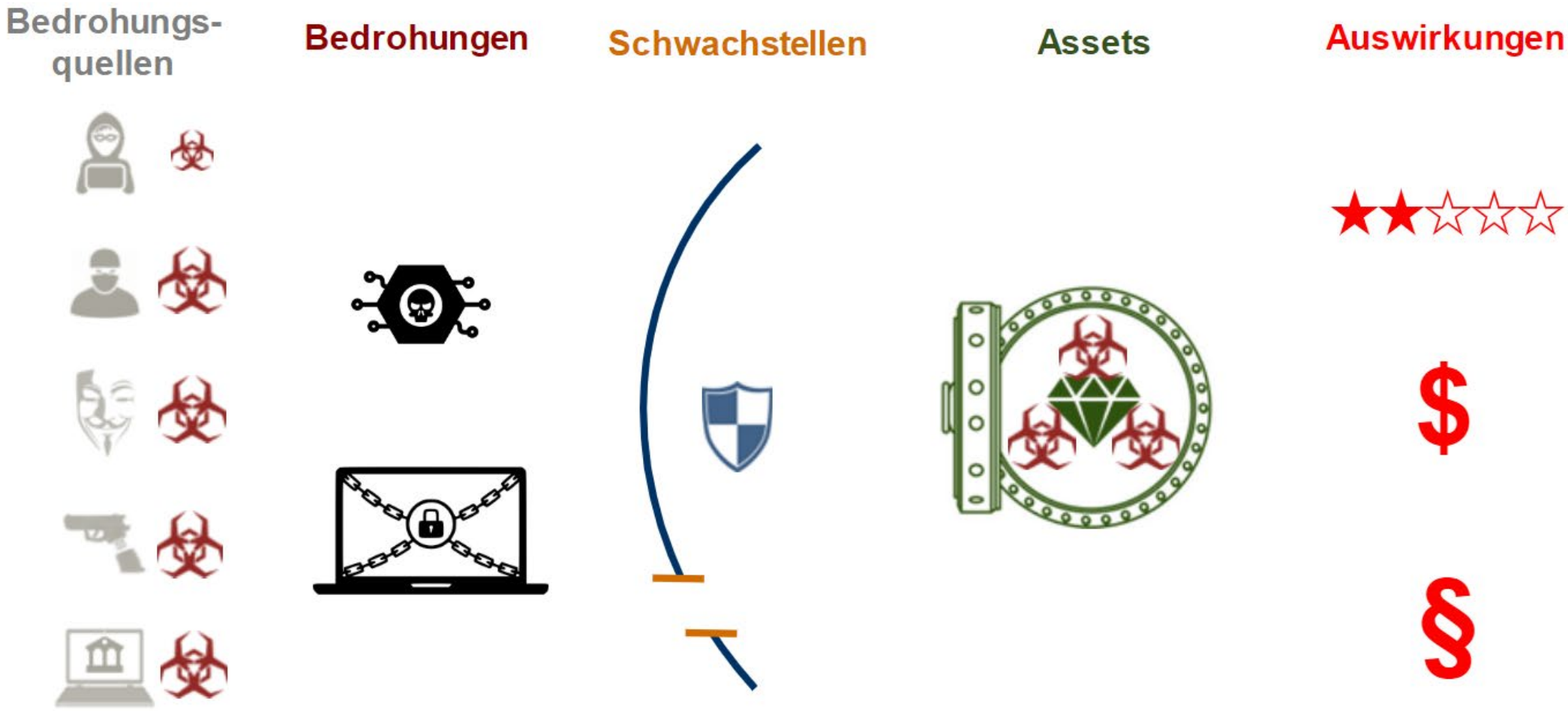
«Amateurs hack systems, professionals hack people» (Bruce Schneier)

LAUX LAWYERS AG
ZURICH | BASEL



Vorgehen Risikoanalyse

LAUX LAWYERS AG
ZURICH | BASEL



Das Problem

LAUX LAWYERS AG
ZURICH | BASEL

- Problem «KMU»
- Risk based Approach?
  - wäre ja schön
  - kleine Kanzlei heisst nicht zwingend kleines Mandat
  - Massnahmensicht muss sich an den Mandaten orientieren

Empfohlener Mindset

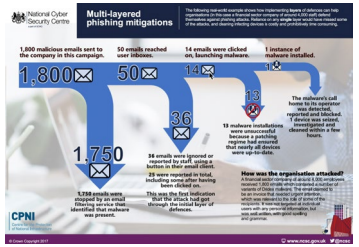
LAUX LAWYERS AG
ZURICH | BASEL

- Von den Grossen lernen – im Kleinen anwenden
- Orientierungsrahmen:
  - Security Design (Technische und Organisatorische Massnahmen)
  - Security everywhere (DevSecOps)
  - Security Operation (SOC; über Drittanbieter für Cybersicherheit)
  - Multi-layered Approach (https://www.ncsc.gov.uk/guidance/phishing#section_3)

    Technische Hürden* (Anzahl reduzieren) | Erkennen | Folgen unerkannter Angriffe mitigieren* (2FA etc.) | Incident Response
  - Penetrationstests (Plan – Do – **CHECK** – Act)
  - OWASP Top 10 (https://owasp.org/www-project-top-ten/)
  - Security Mindset

A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
A10:2021-Server-Side Request Forgery (SSRF)*

*es braucht auch technische Massnahmen, also geht es um mehr als nur den Mindset.



Kleinunternehmen schützen sich (1/2)

LAUX LAWYERS AG
ZURICH | BASEL

- Soft Faktoren:
  - Mindset (Unsichere Situationen meiden; Phishing Schulung)
  - Awareness (PICNIC; PEBCAC)
  - Kommunikation (nicht unterschätzen)

Achtung: User Bashing kann IT Sicherheit reduzieren!

- Aktionen:
  - Verstehen (Schutzbedarfsanalyse)
  - Auswählen (Reife Lösungen; Beratung für Lösungen: Sicherheitseinstellungen sind oft komplex)
  - Dokumentieren

Kleinunternehmen schützen sich (2/2)

LAUX LAWYERS AG
ZURICH | BASEL

Mindestbedarf (diese Liste hat einen direkten Bezug zum Thema Cyber-Versicherungen)

1. Passwortmanager einrichten
2. Backup-Konzept haben (regelmässig*; getrennte Speicherung; Cloud* prüfen)[1)]
3. Malware-Schutz (Software aktualisieren*; Downloads und USB Port limitieren; Firewall aktivieren*)[2)]
4. Schutz der Endgeräte (PW-Schutz*; Lokalisierungsfunktion[3)]; SW aktualisieren; ø offene WLANs; VPN)
5. vor Phishing schützen (Admin-User müssen sich besonders verhalten; andere: Mindset)

* Sicherheitseinstellungen der Lösung nutzen

1) 3-2-1 Regel: 3 Backups, 2 Techniken, 1 an einem anderen Ort
(Empfehlung: 1 Ressource sollte online nicht direkt löschbar sein)

2) bei Antivirus differenzieren (Systeme: Mac/Linux)
Kontrolle: Antivirussoftware kann auch wieder Schwachstelle werden

3) Hier ist jedoch die datenschutzrechtliche Würdigung mit einzubeziehen

Sonderfall EMP:
(1) Was tun ohne Strom und Connectivity? (Blackout)
(2) Faradayscher Käfig für genügende Anzahl Geräte im Keller?
(3) Konzept für Datenaustausch?

Kontakt

LAUX LAWYERS AG
ZURICH | BASEL

Christian Laux
Dr. iur., LL.M., Attorney-at-law, Senior Advisor/Partner

@ christian.laux@lauxlawyers.ch
w www.lauxlawyers.ch
N linkedin.com/in/christianlaux

LAUX LAWYERS AG
Schiffbaustrasse 10
P.O. Box
CH–8031 Zurich
+41 44 880 24 24

Fallback

LAUX LAWYERS AG
ZURICH | BASEL

Zum Begriff der «Kanzlei»:
Wo «fängt sie an»?
Wo «hört sie auf»?

Perimeter =

Grenze, wo die Kontrolle über die Informationen der Kanzlei endet …

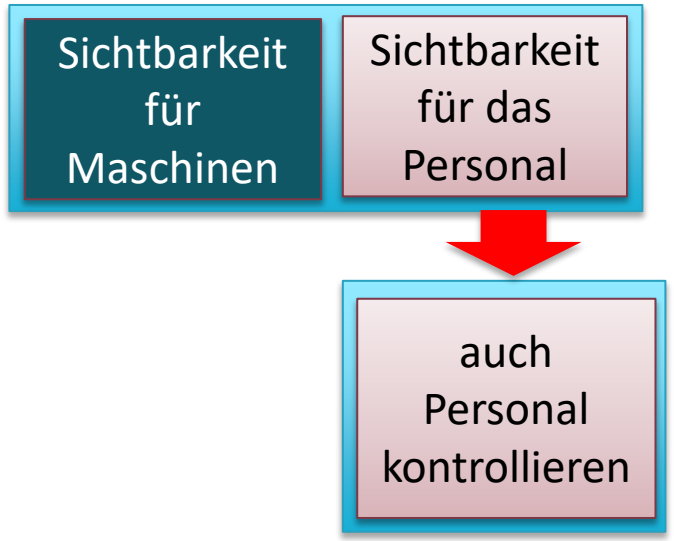
(«Perimeter»)

… Daten können auf der IT-Infrastruktur eines anderes Unternehmens sein

… und von Personal eines Dritten verwaltet werden

Wirklich?

Und was ist mit der Hauptregel?
(«**keine Offenbarung**»)



Quellen (pro memoria)

LAUX LAWYERS AG
ZURICH | BASEL

- Vertrag
- BGFA
- DSG (neu mit Meldepflichten)
- Schweizerische Standesregeln SSR
- CCBE
- Wegleitungen

Quellen (pro memoria)

LAUX LAWYERS AG
ZURICH | BASEL

Digitale Kanzlei

Elektronischer Rechtsverkehr

Worum geht es?

Wie präsentiere ich mich im Internet?

Wie baue ich die digitale Kanzlei?

IT-Security

Nutzung von Cloud-Diensten

Cloud und Datenschutz

Service

Stellenbörse

SAV-FSA Service AG Versicherungen

Pensionskasse SAV

SRO SAV-SNV

Vergünstigungen

Digitalisierung

Rechtschutzversicherungen