Zürcher Hochschule
für Angewandte Wissenschaften

School of Engineering
InIT Institut für angewandte Informationstechnologie

# Online-Vertiefungsworkshop «Predictive Maintenance»
# **Track Data Security**

## ZHAW School of Engineering
## Schwerpunkt Information Security

# Themen



- **Setting the Scene:** Ihre Schwerpunkte und Erwartungen
- **Umfeld:** Sicherheit, Risiken, Digitalisierung, Angreiferprofile
- **Angriffsmethoden:** Vernetzung, Schwachstellen, Malware, Phishing, Social Engineering
- **Baseline Security:** Schutzmassnahmen, Organisation, Industrial Automation
- **Nächste Schritte:** Informationsquellen, Unterstützungsnetzwerke, Konkrete Schritte

Photo by Karolina Grabowska from Pexels

- **Wir behandeln nicht:** Technische und firmenspezifische Detailfragen, rechtliche Probleme
- **Disclaimer:** Die beispielhafte Erwähnung von Produkten beinhaltet weder Billigung noch Kritik

# **Setting the Scene:** Ihre Schwerpunkte und Erwartungen

# Vorstellung

Zürcher Hochschule für Angewandte Wissenschaften
School of Engineering
InIT Institut für angewandte Informationstechnologie

Dr. Peter Berlich

berp@zhaw.ch
https://www.zhaw.ch/de/ueber-uns/person/berp/

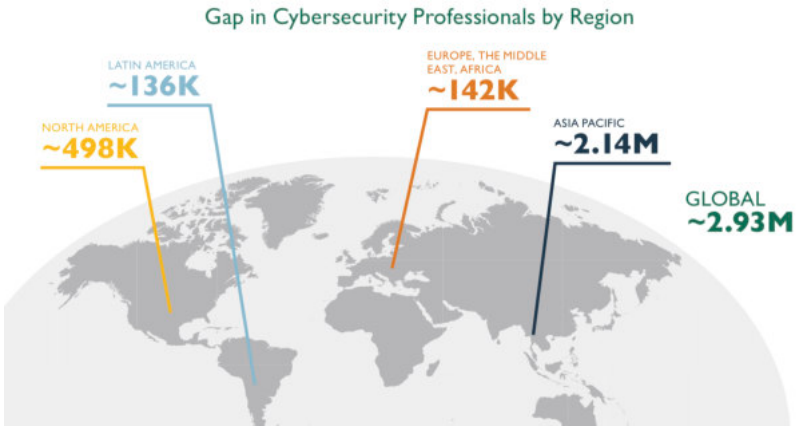
- Dozent IT-Sicherheit
- Studiengangleiter
  CAS Angewandte IT-Sicherheit
- Projektleiter SeCoSS, OptiPhish
- Forschungsprojekte,
  Weiterbildung, Dienstleistungen

- 20 Jahre IT-Sicherheit

# CAS Angewandte IT-Sicherheit @ ZHAW

Zürcher Hochschule für Angewandte Wissenschaften
School of Engineering
InIT Institut für angewandte Informationstechnologie

- "Skills gap": Steigende Nachfrage nach IT-Sicherheitsexperten
  - IT-Sicherheit ein Kernthema der Digitalisierung
  - Unternehmen aller Bereiche sind herausgefordert, mit der Entwicklung Schritt zu halten
  - Aus Unternehmenssicht: Externe Suche oder interne Qualifikation?
  - Für Teilnehmer/innen: Bestehende Kenntnisse erweitern und auf akademischem Niveau konsolidieren




Quelle: https://www.isc2.org/Research/Workforce-Study

- Für wen?
  - Für IT-Experten
  - Für Praktiker und Quereinsteiger
- Inhalte
  - Grundlagen der IT-Sicherheit
  - Architektur und Management
  - Kryptografie und Netzwerksicherheit
  - Software- und Systemsicherheit
- Separat oder als Baustein zum MAS
  - MAS Informatik https://www.zhaw.ch/de/engineering/weiterbildung/detail/kurs/mas-informatik/
  - MAS Industrie 4.0 https://www.zhaw.ch/de/engineering/weiterbildung/detail/kurs/mas-industrie-4-0/
- Informationen und Anmeldung
  - Dauer 1 Semester, jährlich, im Herbstsemester
  - https://www.zhaw.ch/de/engineering/weiterbildung/detail/kurs/cas-angewandte-it-sicherheit/

# Vorstellung

Zürcher Hochschule für Angewandte Wissenschaften
School of Engineering
InIT Institut für angewandte Informationstechnologie

- Kurzvorstellung
- Hintergrund
- Erwartungen

Photo by Sara Garnica from Pexels

# **Umfeld:** Sicherheit, Risiken, Digitalisierung, Angreiferprofile

# IT-Sicherheits-Markt: Diversifizierung und laufende Veränderung

Zürcher Hochschule für Angewandte Wissenschaften
School of Engineering
InIT Institut für angewandte Informationstechnologie

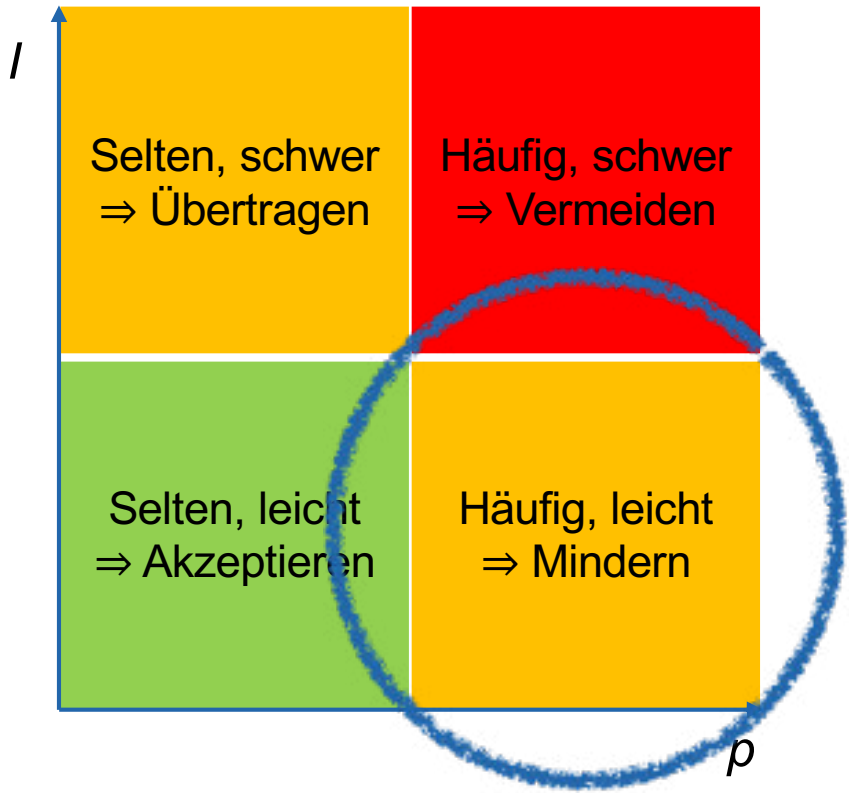
| Treiber | Auswirkungen |
|---|---|
| • Politisch<br>– Wettbewerbsfähigkeit hängt mittelbar und unmittelbar von Sicherheit und Datenschutz ab<br>– Funktionieren des Staates hängt von Sicherheit ab<br>– Politische Beeinflussung und Erpressbarkeit | • Politisch<br>– Datenschutzgesetzgebung<br>– Regulierung und Gesetze für Sicherheitsmassnahmen<br>– Regulierung und Gesetze gegen Sicherheitsmassnahmen (z.B. Verschlüsselung) |
| • Wirtschaftlich<br>– Kostendruck/Security als Cost of Doing Business<br>– Verluste durch Sicherheitsvorfälle<br>– Digitalisierung (Automatisierung von Produktion und Abläufen) in Industrieländern<br>– Wirtschaftswachstum und Verbreitung von Technologie in Schwellenländern | • Wirtschaftlich<br>– Erhöhte Nachfrage nach und Abhängigkeit von Sicherheitsdienstleistungen<br>– Zunehmender Reifegrad der Prozesse im Unternehmen<br>– Entstehen einer IT-Sicherheitsindustrie |
| • Sozial<br>– Akzeptanz von IOT<br>– Integration digitaler Dienstleistungen in den Alltag<br>– Cybercrime | • Sozial<br>– Technologiewissen verbreitet sich und wird zur Voraussetzung sozialer Teilhabe<br>– Individueller Bedarf an IT-Sicherheit |
| • Technologisch<br>– Technische Innovation auf Angreiferseite<br>– Technische Innovation in IT allgemein | • Technologisch<br>– Technologische Innovation auf der Verteidigerseite<br>– Sicherheitsinnovation kann mit IT-Innovation nicht immer Schritt halten, unausgereifte Produkte |

# Was ist Sicherheit?



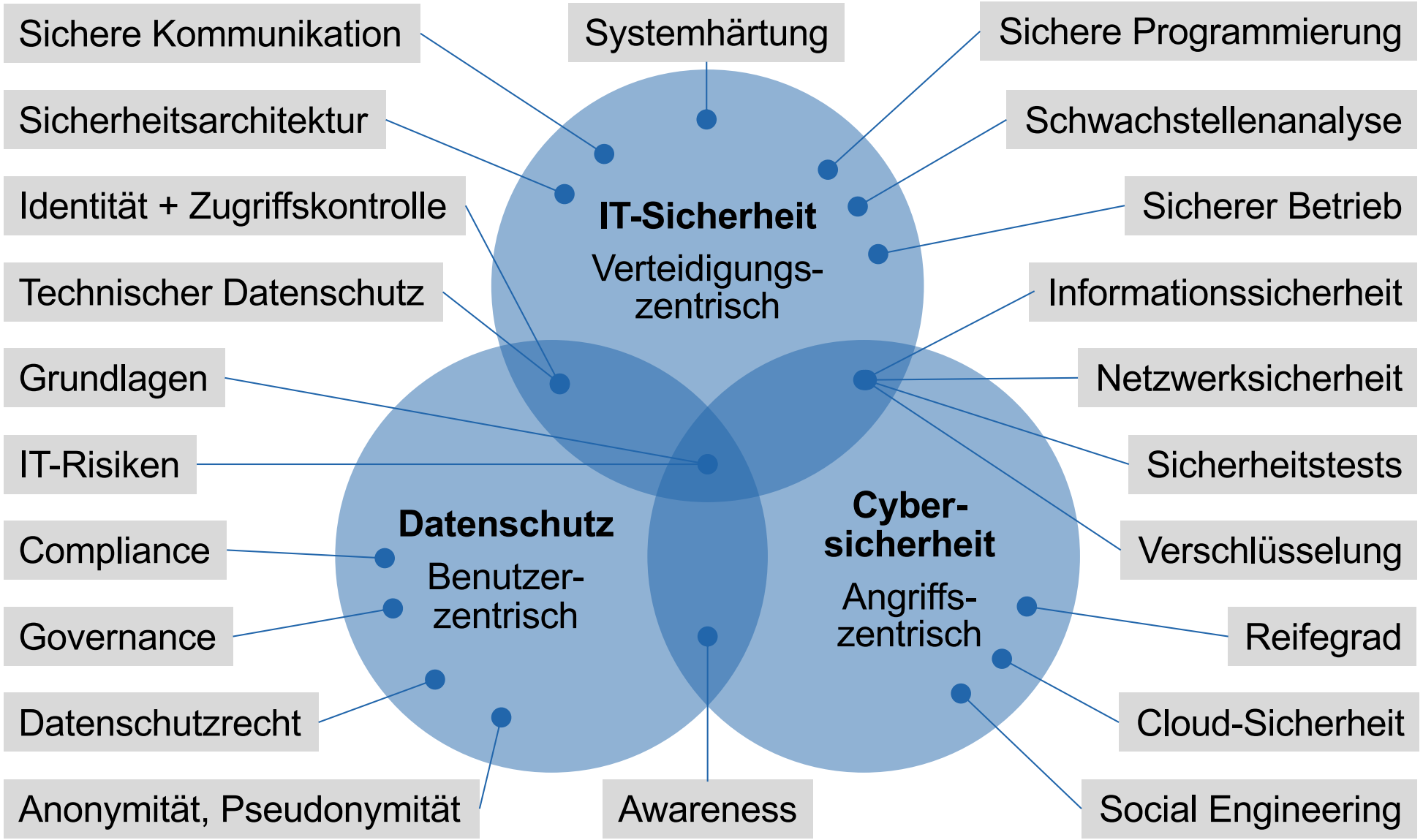
- Sicherheit ist **eine** von mehreren Möglichkeiten, um Risiken zu behandeln
  - Risiko **vermeiden**
    - Beispiel: Eine Dienstleistung nicht in Anspruch nehmen
  - Risiko **übertragen**
    - Beispiel: Versicherung – für IT-Anwender selten eine Option
  - Risiko **mindern**
    - Beispiel: Sich durch Sicherheits-massnahmen schützen
  - (Rest-)Risiko **akzeptieren**

- Behandlung von Risiko richtet sich allgemein nach
  - Wahrscheinlichkeit (p = probability) und
  - Kosten pro Vorfall oder allgemein Auswirkungen (I = Impact)



# “Welche” Sicherheit?

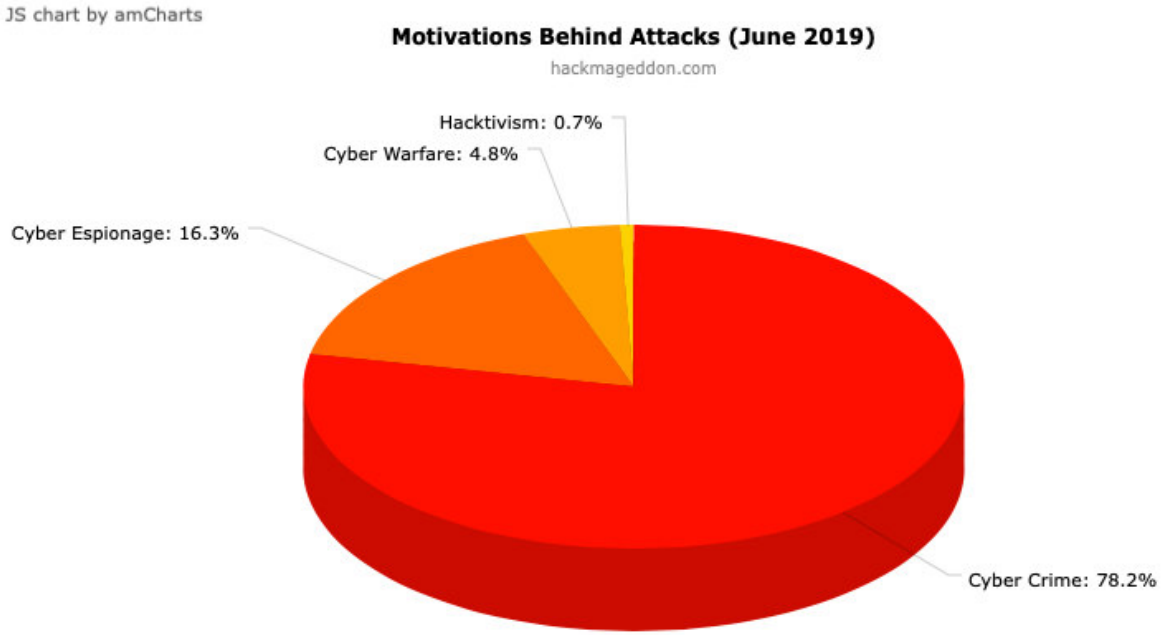
Zürcher Hochschule für Angewandte Wissenschaften
School of Engineering
InIT Institut für angewandte Informationstechnologie



# Wer sind die Angreifer?



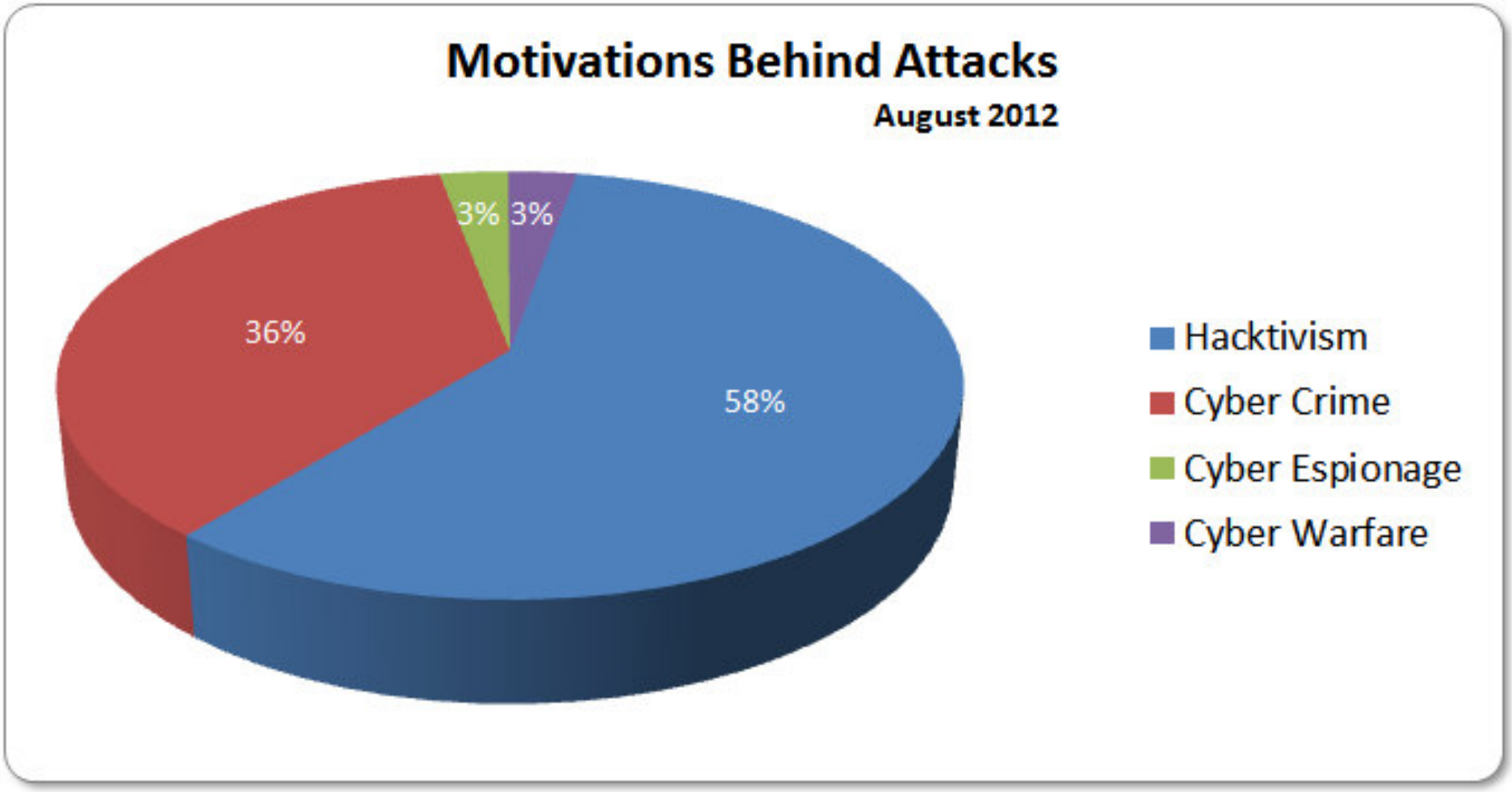
- Die meisten Angreifer sind Kriminelle
  - cum grano salis… Attribution is hard




Quelle: https://www.hackmageddon.com/2019/08/12/june-2019-cyber-attacks-statistics/

# Wer sind die Angreifer? (2012)



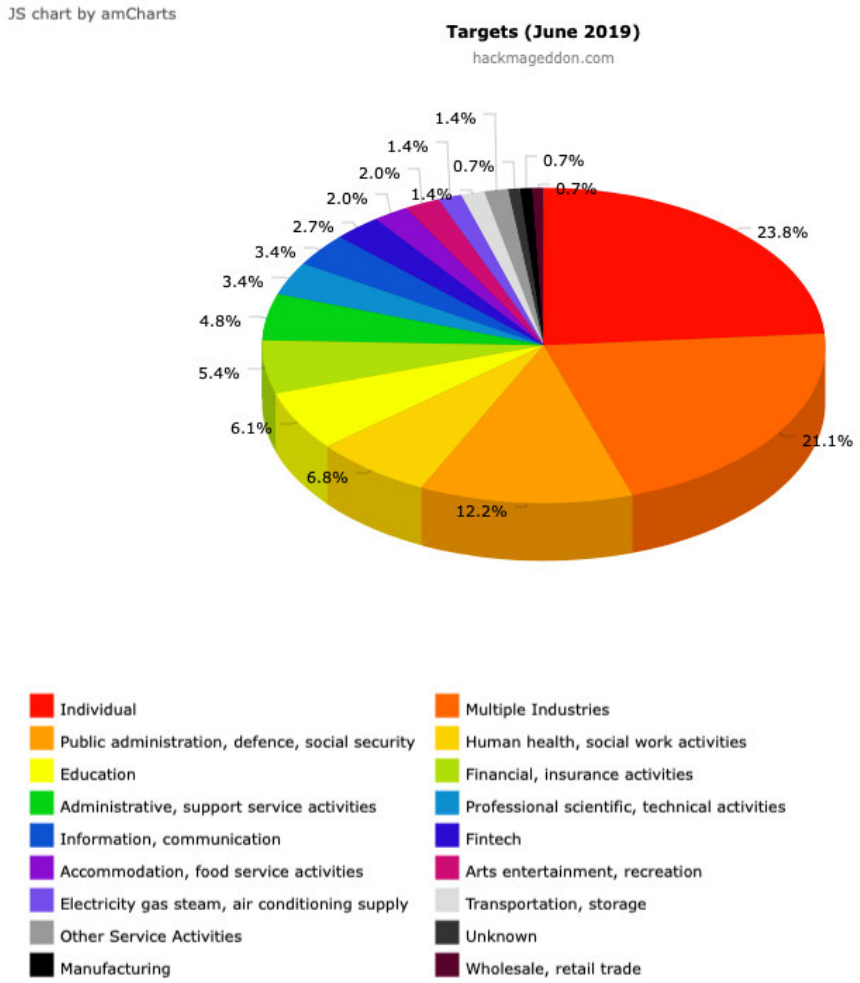



Quelle: http://paulsparrows.files.wordpress.com/2012/09/motivations-behind-attacks-august-20121.png

# Wer sind die Angegriffenen?

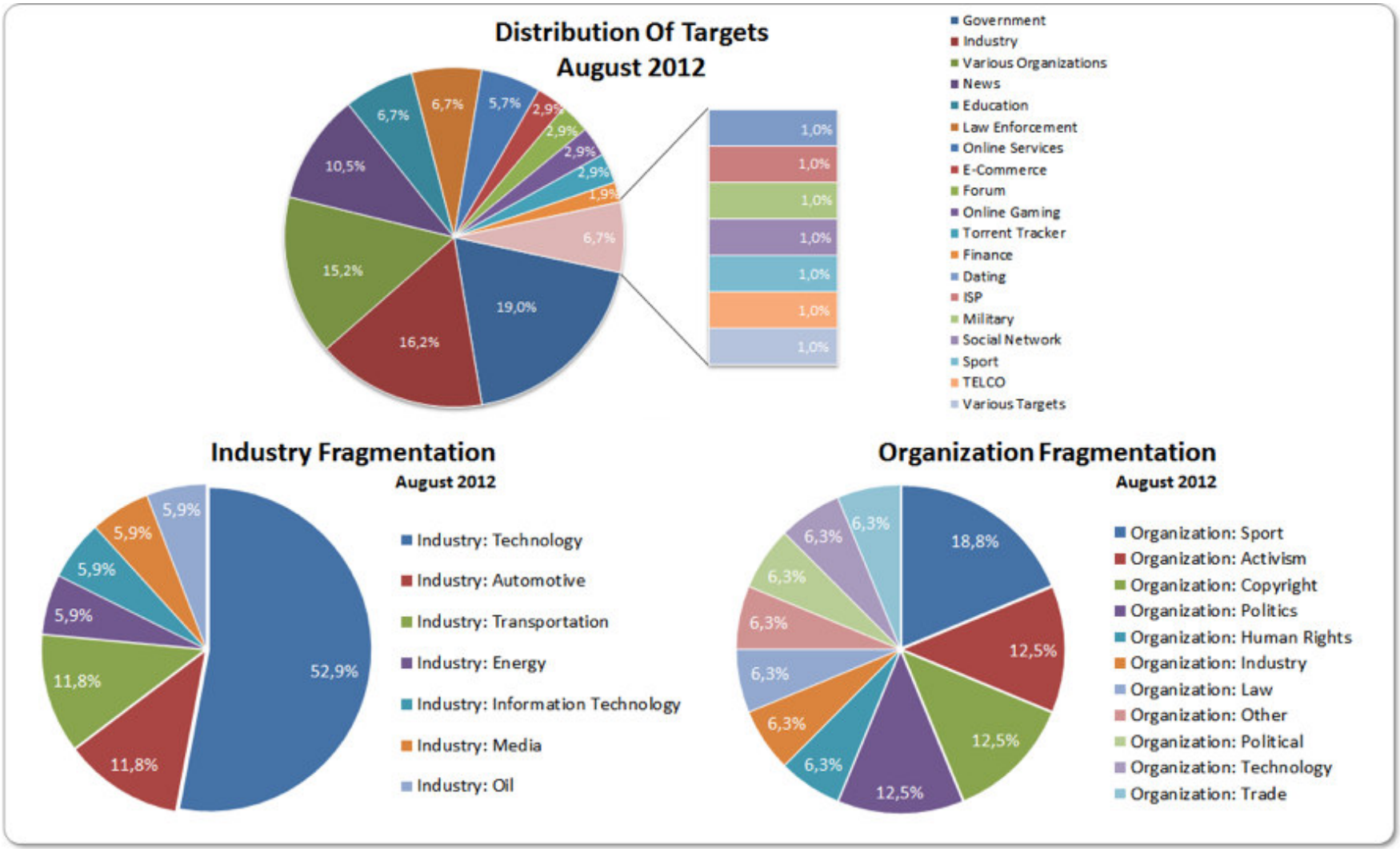


- Die meisten Angegriffenen sind individuelle Benutzer




Quelle: https://www.hackmageddon.com/2019/08/12/june-2019-cyber-attacks-statistics/

# Wer sind die Angegriffenen? (2012)




Caveat: Zuordnung evtl. nicht direkt vergleichbar mit Vorseite

Quelle: http://paulsparrows.files.wordpress.com/2012/09/distribution-of-targets-augut-2012.png

# **Angriffsmethoden:** Vernetzung, Schwachstellen, Malware, Phishing, Social Engineering

# Wie gehen Angreifer vor?



- Der (klischeebehaftete) Angriff eines fähigen Hackers von aussen auf das Netzwerk existiert
- Dieser verlässt sich jedoch auf vorhandene Schwachstellen
  - Fehlerhafte Konfiguration
  - Ungepatchte Sicherheitslücken
  - Einfache Passwörter
  - etc.
- Angriffe sind automatisiert und skalierbar
  - Sie können sich nicht darauf verlassen, unwichtig oder unsichtbar zu sein
- Daneben gibt es zum Beispiel
  - Angriffe durch eigene Mitarbeiter
  - Angriffe unter Ausnutzung der Gutgläubigkeit der Mitarbeiter
  - Angriffe unter Zuhilfenahme von Unaufmerksamkeit oder Unkenntnis, z.B. Öffnen infizierten Mailanhangs


Photo by Saksham Choudhary from Pexels

# Angreifermodell

Zürcher Hochschule für Angewandte Wissenschaften
School of Engineering
InIT Institut für angewandte Informationstechnologie

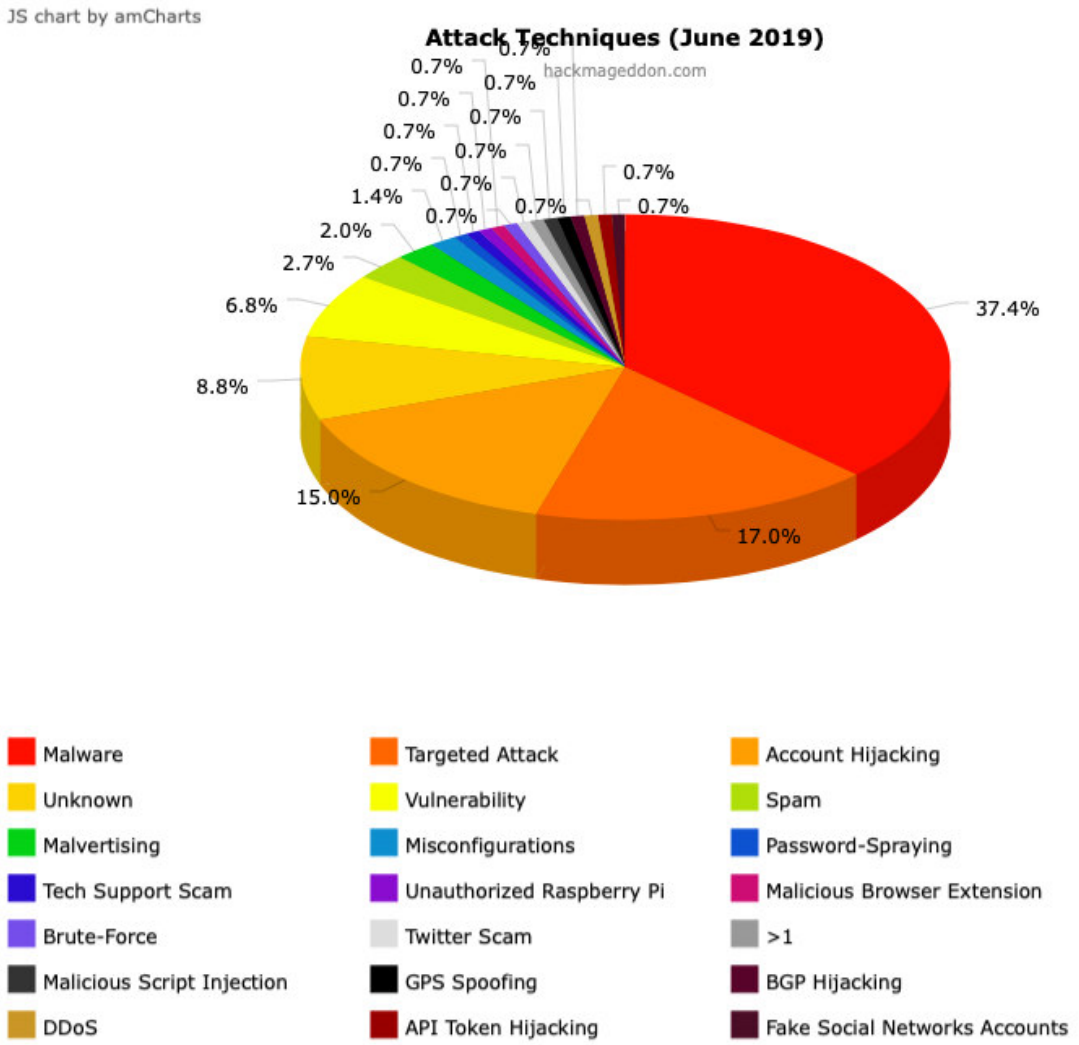
| Angreifer Level | Angreifer-beispiele | Fähigkeiten | Zielstrebigkeit | Nachhaltigkeit | Ressourcen |
|---|---|---|---|---|---|
| **SL4** | Staat, Regierungs-behörden | ICS-spezifisch | Hoch, es wird ein bestimmtes Ziel angegriffen | Entwickelt (Kampagne) | Arbeitsteilige Teams, finanzielle Mittel |
| Ohne gleichwertiges Funding nur begrenzte Abwehrmöglichkeiten für Verteidiger | | | | | |
| **SL3** | Hacktivist, organisiertes Verbrechen | ICS-spezifisch | Mittel, Fokus auf erfolg-versprechende Angriffe | Entwickelt (Angriff) | Gruppe, begrenzte finanzielle Mittel |
| **SL2** | Insider, Thrill Seeker, Script kiddies | Allgemeine | Niedrig | Gering | Einzeltäter |
| **SL1** | Gutwilliger oder fahrlässiger Insider | Keine | Zufällige oder gelegentliche Übertretungen | Unabsichtlich | Einzeltäter |

Quellen: IEC 62443, https://download.schneider-electric.com/files?p_Doc_Ref=998-20186845, https://isasecure.org/en-US/Documents/Articles-and-Technical-Papers/2018-IEC-62443-and-ISASecure-Overview_Suppliers-Pe

Quelle: https://www.pexels.com/photo/photo-of-guy-fawkes-mask-with-red-flower-on-top-on-hand-38275/

# Wie arbeiten die Angreifer?

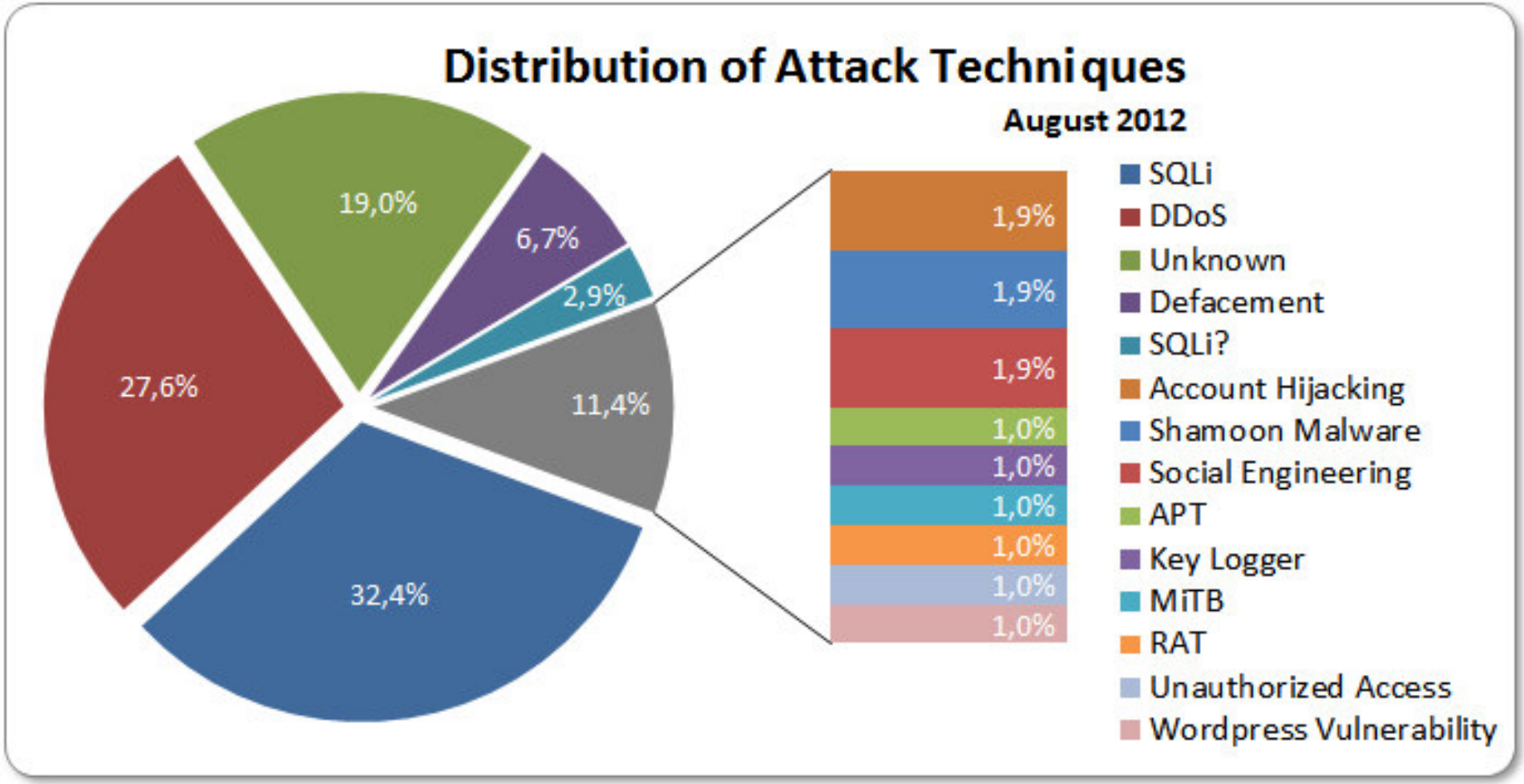





Quelle: https://www.hackmageddon.com/2019/08/12/june-2019-cyber-attacks-statistics/

# Wie arbeiten die Angreifer? (2012)

Zürcher Hochschule für Angewandte Wissenschaften
zh aw School of Engineering
InIT Institut für angewandte Informationstechnologie




Quelle: http://paulsparrows.files.wordpress.com/2012/09/distribution-of-attack-techniques-august-2012.png

Caveat: Aufteilung evtl. nicht direkt vergleichbar mit Vorseite

# Beispiel Hacktivism



- Angekündigter Angriff auf Facebook
- Der angekündigte Angriff war entweder erfolglos, oder er fand nicht statt
  - Jed(r) kann ein Video hochladen…
- In anderen Fällen waren die Angreifer sehr wohl erfolgreich
- Beispiel: DDOS-Angriff auf div. Banken einschl. PostFinance 2010 https://doi.org/10.1111/jcc4.12024
- Hacktivism kann sich auch gegen Unbeteiligte richten

Quelle: http://www.youtube.com/watch?v=Q6crH8qmyZ8

# Beispiel Cyber Warfare



**Stuxnet (2011)**

- Ziel waren iranische Urananreicherungsanlagen
- Mit an Sicherheit grenzender Wahrscheinlichkeit ein staatlicher Angriff
  - Komplexer Angriff mit mehreren, “unverbrauchten” (unbekannten = wertvollen) Sicherheitslücken
  - Leak (Glaubwürdigkeit?) https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html
- Technisch hochentwickelt
  - Konnte Airgaps überspringen, indem es USB Drives infizierte
  - Schadenseinwirkung “zufällig”, sieht aus wie ein normaler technischer Fehler
  - Zielte auf Geräte eines bestimmten Typs (Siemens) mit bestimmten Seriennummern
- Nur durch Zufall entdeckt

- Viele verwandte Systeme ähnlich verwundbar.
- Es wäre trivial, Stuxnet zu patchen (Seriennummern!) und/oder weiterzuentwickeln

Quelle: http://upload.wikimedia.org/wikipedia/commons/f/f3/Siemens_Simatic_S7-416-3.jpg

# Beispiel: Ransomware



- Angriff auf ungesicherte Systeme unter Zuhilfenahme unaufmerksamer Benutzer
- Gelangt durch E-Mail oder andere Wege auf den Rechner
- Verbreitet sich über alle Dateien, auf die der Benutzer Zugriff hat, insb. Network Shares
- Nach einer Karenzzeit werden Daten verschlüsselt und eine Erpressungsbotschaft angezeigt
- Es gibt keine Garantie, dass die Daten nach Zahlung entschlüsselt werden!

- Häufiger Angriff in den letzten Jahren mit mehreren prominenten Opfern (Grossunternehmen, Behörden)


Quelle: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#/media/File:Wana_Decrypt0r_screenshot.png

# Beispiele Social Engineering



**Vorgetäuschter Supportanruf**

- Ein Benutzer erhält wegen einer angeblichen Vireninfektion einen Anruf... vom "Microsoft Helpdesk» (in Wirklichkeit einem kriminellen Callcenter)
- Der Benutzer wird aufgefordert, dem "Helpdesk" Zugriff auf den PC zu geben.
- Schaden: Kreditkarteninformationen, Daten kopiert oder zu Erpressungszwecken verschlüsselt

**(Einige) Weitere Social-Engineering-Angriffe**

- **Chef-Masche:** Anruf oder E-Mail, die um Unterstützung bei einem “vertraulichen” Projekt bittet, oft um Überweisung von Geld
- **Phishing:** E-Mail mit vorgetäuschtem Absender, die den Empfänger auf eine gefälschte Website lockt, um Login-Daten zu erhelten
  - **Spear-Phishing:** Gezielter Angriff auf eine einzelne Person, die zuvor genau ausgespäht wurde
- **Vorschussbetrug:** Dem Opfer wird eine Gelegenheit für ein profitables Geschäft vorgetäuscht. Auf dem Weg zum vermeintlichen Gewinn werden immer neue “Gebühren” fällig

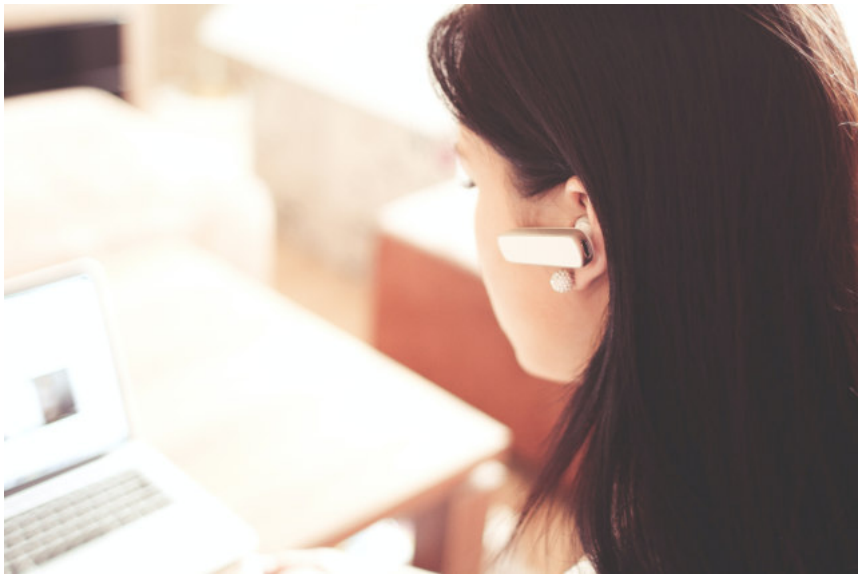


Photo by picjumbo.com from Pexels

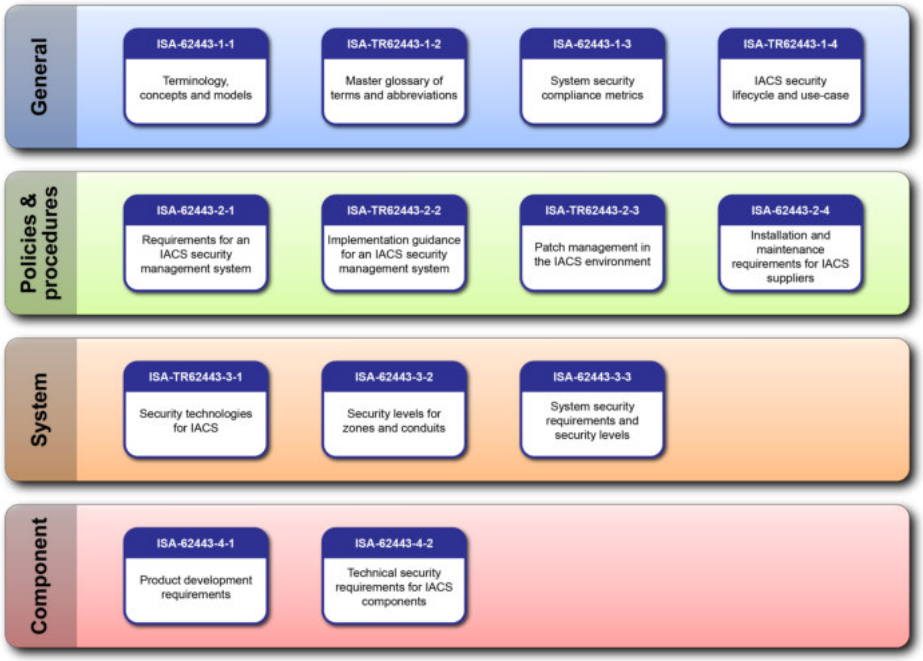
Zürcher Hochschule
für Angewandte Wissenschaften
zh aw
School of Engineering
InIT Institut für angewandte Informationstechnologie

# **Baseline Security:** Schutzmassnahmen, Organisation, Industrial Automation

# Problemfelder Industrial Automation

Zürcher Hochschule für Angewandte Wissenschaften
School of Engineering
InIT Institut für angewandte Informationstechnologie

- Allgemeines
  - Die folgenden Probleme treten auch bei IOT und anderen “Smart Devices” auf
  - Sie beziehen sich auf keinen spezifischen Hersteller
- Produktlebenszyklus
  - (Im Vgl. zu Office-IT) Kleinserien, Spezialanforderungen
  - Lange Investitionszyklen beim Kunden, führt zu Legacy Hardware und Software im Betrieb
- Design
  - Lückenhafter Security Software Development Lifecycle (Definition/Umsetzung Anforderungen, «Security by Obscurity»)
  - Integration proprietärer und nicht-proprietärer Komponenten
  - Nachrüstung zentraler Features wie Vernetzung und Fernbedienbarkeit auf die ursprüngliche Architektur
  - Notwendige Realtime-Fähigkeit im Konflikt mit Sicherheitsfeatures wie z.B. Virenscan
  - Integration mit herstellereigenen Cloud Services, ggf. mit herstellerexklusivem Zugriff und Analysefunktionen
- Betrieb
  - Eigene Zugangsmechanismen
  - Bedienung erfordert ggf. geteilte Benutzerkonten
- Wartbarkeit
  - Ggf. zertifizierte Software, die nicht einfach gepatcht werden kann
  - Wartbarkeit nur durch Drittparteien. Software-Updates hängen vom Hersteller ab, evtl. nicht rentabel
  - Fehlende Überprüfbarkeit durch den Kunden




Planned and published ISA 62443 work products for IACS Security

Quelle: https://en.wikipedia.org/wiki/Cybersecurity_standards#/media/File:ISA-62443_Standard_Series_2012.png

Quelle und weiterführende Information: https://www.computertechreviews.com/cybersecurity-in-industrial-automation/

# Maturity Level (Reifegrad) Hersteller

Zürcher Hochschule für Angewandte Wissenschaften
School of Engineering
InIT Institut für angewandte Informationstechnologie

**CMMI 4 & 5 Ständige Verbesserung**

- Wirksamkeit und Leistungsfähigkeit kontrolliert, ständige Verbesserung

**CMMI 3 Definiert**

- Wiederholbare Prozesse nachgewiesen

**CMMI 2 Verwaltet**

- Wiederholbare Prozesse definiert

**CMMI 1 Anfang**

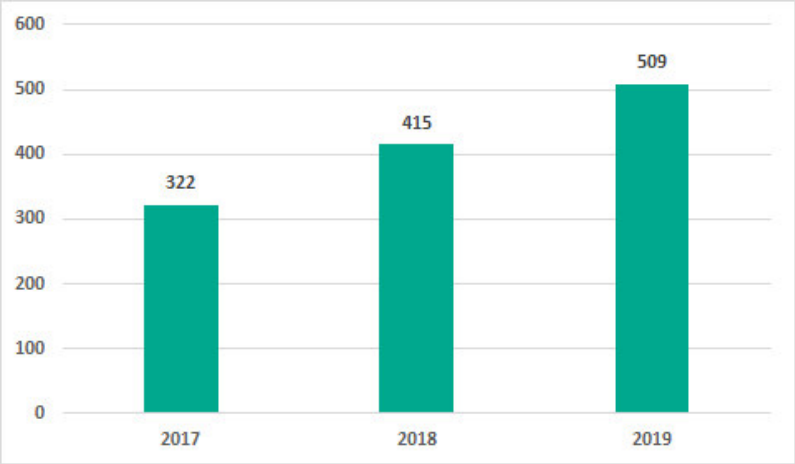
- Produktentwicklung für den Einzelfall, ggf. undokumentiert

Photo by ThisIsEngineering from Pexels

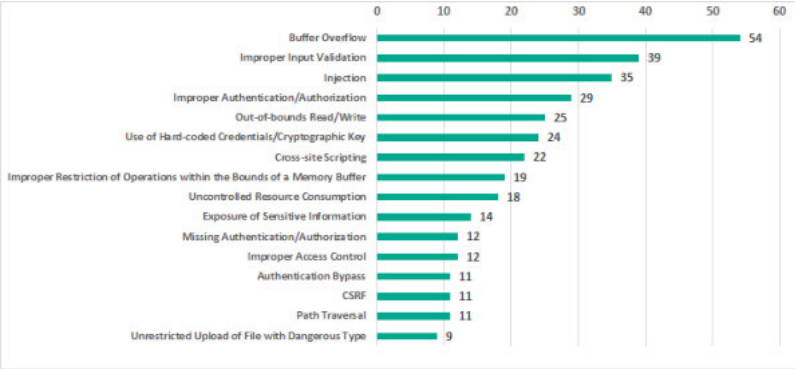
Quelle: IEC 62443-4-1
Weiterführende Informationen: https://iiconsortium.org/pdf/SMM_Description_and_Intended_Use_2018-04-09.pdf

# Angriffe auf Industrial Control Systems

Zürcher Hochschule für Angewandte Wissenschaften
School of Engineering
InIT Institut für angewandte Informationstechnologie




Number of vulnerabilities in different ICS components, as published on the US ICS-CERT website




Most common vulnerability types published in 2019

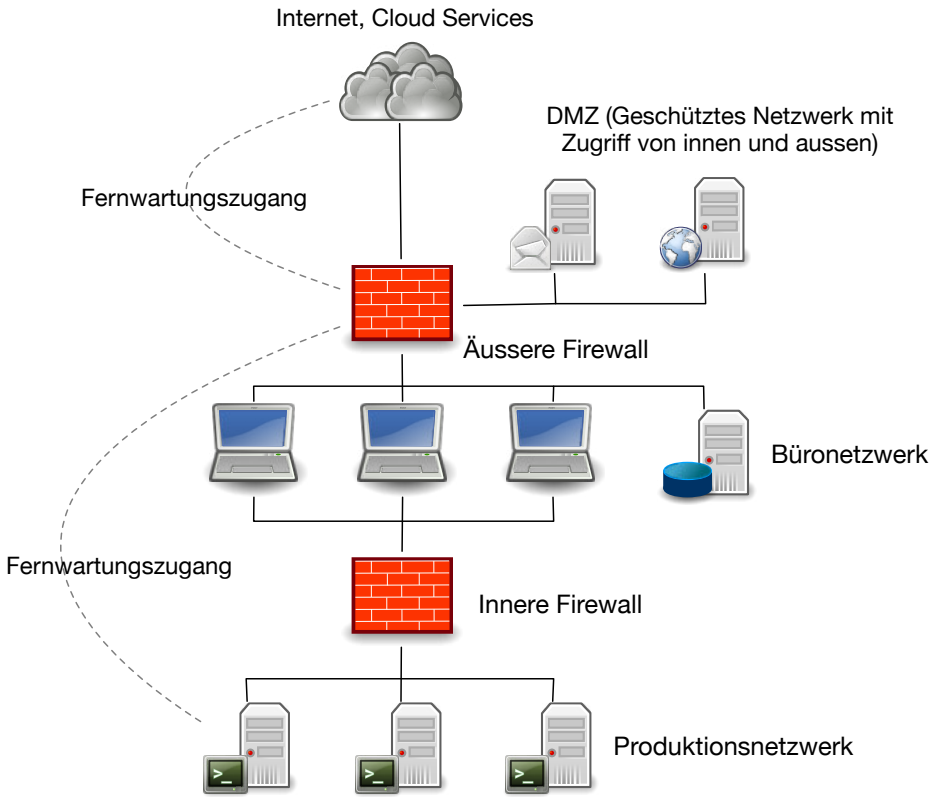
- Anzahl Sicherheitslücken nimmt zu – Funktion des Alters der Produkte, Anzahl Produkte, Marktgrösse und der Attraktivität für Angreifer
- Kein gutes Zeichen hinsichtlich Nachfrage nach sicheren Systemen oder Marktregulierung
- Die identifizierten Sicherheitslücken sind in ihrer Art grundlegend und hätten in Entwicklung und Test auffallen müssen
- Lücken bestehen aber oft auch in zugelieferten Komponenten wie Netzwerkmodulen und Betriebssystemen (s. Quellen)

Quellen: https://ics-cert.kaspersky.com/reports/2020/04/24/threat-landscape-for-industrial-automation-systems-overall-global-statistics-h2-2019/
https://ics-cert.kaspersky.com/reports/2020/04/24/threat-landscape-for-industrial-automation-systems-vulnerabilities-identified-in-2019/

# Office-IT und Produktion

- Office-IT und Produktion sind getrennte Bereiche mit verschiedenen Risikoprofilen
  - Ggf. unter getrennter Verantwortung
  - Office-IT oft selbstgewartet jedoch Massenproduktue
  - Produktionssysteme ggf. Kleinserien, auch fremdgewartet
  - Lange Investitions- und Lebenszyklen bei Produktionssystemen
  - Das Risiko für das Unternehmen ist bei Produktionssystemen im Zweifel höher (Ausfall der Produktionskette, möglicherweise geringerer Schutz)

- Operative Trennung, jedoch gemeinsame Prinzipien
  - Risiken werden vom Management verantwortet
  - Baseline Security: Grundlegende Sicherheitsmassnahmen, die überall eingeführt werden
  - Kompensatorische Massnahmen, wo dies nicht möglich ist
  - Beispiel: Netzwerkabschottung, falls Zugriff durch Drittanbieter, fehlender Virenschutz oder fehlende Wartbarkeit



# Sicherheit in beiden Bereichen ermöglichen

Zürcher Hochschule für Angewandte Wissenschaften
School of Engineering
InIT Institut für angewandte Informationstechnologie

**Office-IT**

- Eigener Netzwerkbereich
- Standardisierung auf eine Plattform
- Standardsicherheitsmassnahmen (Patching und Software Updates, Systemhärtung, Virenscanner, Verschlüsselung, regelmässige Prüfung von Zugriffsrechten)
- Bei Integration von Cloud Services Herstellerzusagen über Sicherheit und Datenschutz einholen (Vorsicht insb. bei internationaler Auslagerung von Daten)

**Produktion**

- Zweckmässige Sicherheitsanforderungen mit dem Hersteller vertraglich festlegen
- Grundsätzlich als “fremde” IT behandeln, was Sie nicht kontrollieren können
- Eigener Netzwerkbereich, ggf. weitere Segmentierung innerhalb des Produktionsnetzwerks
- Monitoring der Geräte und des Netzwerks auf verdächtigen Traffic
- Fernsteuerung nur aus dem Produktionsnetzwerk, ggf. über VPN/VLAN (Virtual LAN)

# **Nächste Schritte:** Informationsquellen, Unterstützungsnetzwerke, Konkrete Schritte

# Wo stehen wir als Verteidiger?

Zürcher Hochschule für Angewandte Wissenschaften
School of Engineering
InIT Institut für angewandte Informationstechnologie

- **Level 5:** Strategische, laufende Verbesserung und Weiterentwicklung
- **Level 4:** Monitoring und Kontrolle durch Datensammlung und -analyse
- **Level 3:** Taktische Verbesserungen, Standardisierung, Dokumentation
- **Level 2:** Prozesse dokumentiert und wiederholbar
- **Level 1:** Unstrukturiert, ad-hoc, abhängig vom Einsatz Einzelner

Quelle: https://krebsonsecurity.com/2015/04/whats-your-security-maturity-level/ nach eigenen Angaben anhand von Material von https://www.blue-lava.net/; Weiterführende Information: CMMI, https://csrc.nist.gov/Projects/Program-Review-for-Information-Security-Assistance/Security-Maturity-Levels, https://www.exida.com/Blog/iec-62443-levels-levels-and-more-levels

Quelle: Photo by R L from Pexels

# Konkrete Schritte



- Interne Verantwortlichkeiten klären/definieren
  - Betriebliche und organisatorische Verantwortung, ggf. analog Betrieb/IT
  - Budget klären – auch verfügbare Zeit von Experten im Unternehmen
  - Zeitrahmen festlegen
- Inventar erstellen
  - Anwendungen, Dienstleistungen, Zuständigkeiten bei Geschäftspartnern und Zulieferern identifizieren
  - Identifizierung von geschäftskritischen Ressourcen, mindestens grobe Erarbeitung Risikoszenarien
- Grundlegende Massnahmen (Baseline Controls) einführen
  - Konfiguration, Prozesse, Richtlinie einführen und umsetzen, Schulungen wo nötig
  - Regulatorische (Datenschutz!) und gesetzliche Rahmenbedingungen berücksichtigen, wo verlangt
- Laufende Kontrollen, Reports und Verbesserungen
  - Überprüfungen (auch bei Vorfällen), Ablösung Altsysteme, Nachführung Richtlinie

# Wie helfen uns Standards?



- **Checkliste:** Hinreichend vollständige Abdeckung
- **Externe Referenz:** Neutraler Massstab mit Industriebezug
- **Struktur:** Praxiserprobte und methodisch validierte Struktur
- **Unterstützung:** Erspart die Erarbeitung/Bearbeitung des Themas mit limitierten Ressourcen
- **Kein "Kochbuch":** 1:1 Übernahme i.a. nicht realistisch, Anpassung unumgänglich und hilfreich

| Bezeichnung | Aufgabe |
|---|---|
| ID.AM-1 | Erarbeiten Sie einen Inventarisierungsprozess, welcher sicherstellt, dass zu jedem Zeitpunkt ein vollständiges Inventar Ihrer IKT-Betriebsmittel (Assets) vorhanden ist. |
| ID.AM-2 | Inventarisieren Sie all Ihre Softwareplattformen/-Lizenzen und Applikationen innerhalb Ihrer Organisation. |
| ID.AM-3 | Katalogisieren Sie all Ihre internen Kommunikations- und Datenflüsse. |
| ID.AM-4 | Katalogisieren Sie alle externen IKT-Systeme, die für Ihre Organisation relevant sind. |
| ID.AM-5 | Priorisieren Sie die inventarisierten Ressourcen (Geräte, Anwendungen, Daten) hinsichtlich ihrer Kritikalität. |
| ID.AM-6 | Definieren Sie klare Rollen und Verantwortlichkeiten im Bereich der Cybersecurity. |

*Tabelle 3: Aufgaben ID.AM*

| Standard | Referenz |
|---|---|
| CCS CSC 1 | 1, 2 |
| COBIT 5 | BAI09.01, BAI09.02, BAI09.05, DSS05.02, APO02.02, APO03.03, APO03.04, PO01.02, DSS06.03 |
| ISA 62443-3:2013 | SR 7.8 |
| ISO 27001:2013 | A.6.1.1, A.8.1.1, A.8.1.2, A.8.2.1, A.11.2.6 |
| NIST-SP-800-53 Rev. 4 | AC-4, CA-3, CA-9, PL-8, CM-8, AC-20, SA-9, CP-2, RA-2, SA-14, CP-2, PS-7, PM-11 |
| BSI 100-2 | M 2.225, M 2.393, B 2.10, M 2.193 |

*Tabelle 4: Referenzen ID.AM*

Quelle: https://www.melani.admin.ch/dam/melani/de/dokumente/2018/04/IKT-Minimalstandard.pdf.download.pdf/IKT-Minimalstandard.pdf

# Danke für Ihre Teilnahme!

Kontakt und Fragen zur Präsentation, Forschung, Weiterbildung, Dienstleistungen:
berp@zhaw.ch

# Weiterführende Informationen

# Einschlägige Standards (Auswahl)

- MELANI/NCSC (Melde- und Analysestelle Informationssicherung/National Cyber Security Center)
  - Minimalstandard zur Verbesserung der IKT-Resilienz https://www.melani.admin.ch/dam/melani/de/dokumente/2018/04/IKT-Minimalstandard.pdf.download.pdf/IKT-Minimalstandard.pdf
- ISO (International Standards Organization)/IEC (International Electrotechnical Commission)
  - ISO/IEC 27001: Code of practice for information security management https://www.iso.org/standard/54534.html (kostenpflichtig)
  - ISO/IEC 27002: Information security management systems – Requirements https://www.iso.org/standard/54533.html (kostenpflichtig)
  - ISO/IEC 27036 Teil 1–4: Information security for supplier relationships https://www.iso.org/search.html?q=27036&hPP=10&idx=all_en&p=0&hFR%5Bcategory%5D%5B0%5D=standard (kostenpflichtig)
- ISA (International Society for Automation)/IEC
  - ISA/IEC 62443: Security for Industrial Automation and Control Systems https://www.isa.org/templates/two-column.aspx?pageid=124560 (kostenpflichtig)
- Andere
  - BSI (Bundesamt für Sicherheit in der Informationstechnik) https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html
  - CIS (Center for Internet Security) https://www.cisecurity.org/controls/ (Registrierung)
  - ETSI (European Telecommunications Standards Institute) https://www.etsi.org/committee/1393-cyber
  - ISACA (Information Systems Audit and Control Association): CObIT https://www.isaca.org/resources/cobit (Mitgliedschaft)
  - ISF (Information Security Forum): Standard of Good Practice https://www.securityforum.org/tool/standard-of-good-practice-for-information-security-2020/ (Mitgliedschaft)
  - ITU (International Telecommunications Union) https://www.itu.int/itu-t/recommendations/index.aspx?ser=X
  - NIST (National Institute of Standards and Technology): https://csrc.nist.gov/publications/sp800
  - OWASP (Open Web Application Security Project) https://owasp.org/www-project-top-ten/

# Unterstützungsnetzwerke (Auswahl)

Zürcher Hochschule für Angewandte Wissenschaften
School of Engineering
InIT Institut für angewandte Informationstechnologie

- Industrievereinigungen
  - Inno-Pack https://inno-pack.net/
- Kantone
  - Datenschutzbeauftragter Kanton Schaffhausen https://sh.ch/CMS/Webseite/Kanton-Schaffhausen/Behorde/Verwaltung/Volkswirtschaftsdepartement/Datenschutz-405580-DE.html
  - Datenschutzbeauftragter Kanton Thurgau https://www.datenschutz-tg.ch/ds/
  - Datenschutzbeauftragter Kanton Zürich https://dsb.zh.ch/
- Bund
  - Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB) https://www.edoeb.admin.ch/
  - FedPol/KOBIK (Koordinationsstelle zur Bekämpfung der Internetkriminalität) https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/cybercrime.html
  - ISB (Informatiksteuerungsorgan des Bundes) https://www.isb.admin.ch/
  - MELANI (Melde- und Analysestelle Informationssicherung) https://www.melani.admin.ch/ und https://www.govcert.ch/
  - VBS Cyber Defence https://www.vtg.admin.ch/de/aktuell/themen/cyberdefence.html
- Ausland
  - BSI (Bundesamt für Sicherheit in der Informationstechnik) http://www.bsi.bund.de/
  - ENISA (European Union Agency for Cybersecurity) https://www.enisa.europa.eu/
- Netzwerke für IT-Sicherheitsexperten
  - (ISC)² Chapter Switzerland (International Information Systems Security Certification Consortium) https://www.isc2chapter-switzerland.ch/
  - CCC Zürich (Chaos Computer Club) http://www.ccczh.ch/
  - ICT Switzerland https://ictswitzerland.ch/themen/cyber-security/
  - ISACA Switzerland (Information Systems Audit and Control Association) http://www.isaca.ch/
  - ISSS (Information Security Society Switzerland) https://www.isss.ch/de/, Partnerschaft mit SwissICT (https://www.swissict.ch/professional-group/security/)

# Weitere Tools und Unterlagen (Auswahl)

Zürcher Hochschule für Angewandte Wissenschaften
School of Engineering
InIT Institut für angewandte Informationstechnologie

- GCA (Global Cyber Alliance)
  - GCA Cyber Security Toolkit https://gcatoolkit.org/de/kmu/
- ICT Switzerland
  - Cybersecurity-Schnelltest für KMU https://ictswitzerland.ch/themen/cyber-security/check/
- ISB (Informatikstrategieorgan des Bundes)
  - Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html
- MELANI (Melde- und Analysestelle Informationssicherung)
  - Checklisten und Anleitungen https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen.html
  - Massnahmen zum Schutz von Industriellen Kontrollsystemen https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/massnahmen-zum-schutz-von-industriellen-kontrollsystemen--ics-.html
  - Merkblatt Informationssicherheit für KMU und Minimalstandard zur Verbesserung der IKT-Resilienz (s.o.) https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/merkblatt-it-sicherheit-fuer-kmus.html
- Sicherheitsberichterstattung in der IT-Presse
  - Heise Security https://www.heise.de/security/
- Konferenzen und Events
  - Auf Anfrage… die Liste würde sonst wirklich zu lang