Grafenauweg

Kanton Zug

Cybersecurity in der Verwaltung

Wie schützt sich der Kanton Zug

14. Juni 2022

Lernplattform elearning.zg.ch (Video)

Agenda

1. Aktuelle Cyber-Bedrohungslage?
2. Cyberdelikte verhindern?
3. Was tun bei einem Cyberangriff?
4. Wie macht der Kanton Cybersecurity?
5. Fragen

1. Aktuelle Cyber-Bedrohungslage

Mythen und Fehleinschätzungen?

„Der Kanton Zug bzw. unser Unternehmen ist doch viel zu klein und unbekannt, um Hacker anzulocken.“

„IT-Sicherheit ist teuer und belastet den normalen Betrieb! - Eine Cyber-Versicherung denkt uns den Schadenfall.“

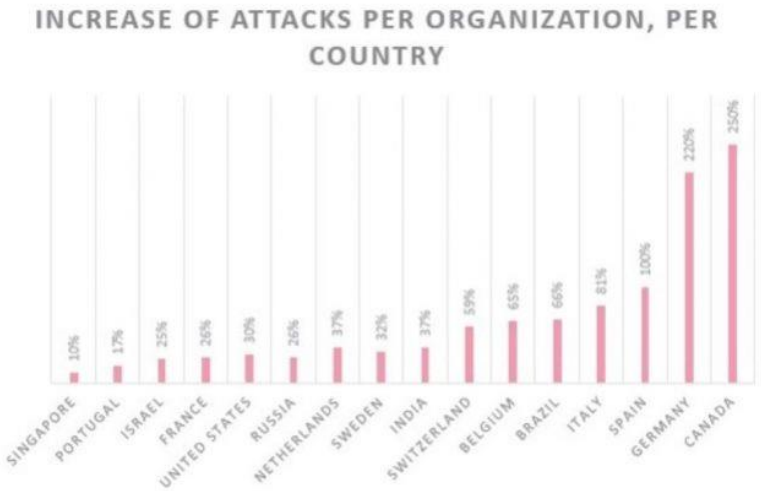
„Wir haben keine kritischen Daten, die für Hacker interessant sind.“

„Wir haben gut geschulte Mitarbeitende, Phishing von vertraulichen Daten (z.B. Passwörter) ist nicht möglich.“

„Wir brauchen kein Schwachstellen-Management - Unsere IT-Verantwortlichen haben Störungen im Griff.“

Cyber-Angriffe massiv gestiegen

6% aller Schweizer Organisation waren direkt oder indirekt betroffen



Quelle: Checkpoint Halbjahresbericht 2021

30 bis 50 Prozent der Firmen zahlen Lösegeld.

Quelle: Cybersicherheitsfirma Zendata

Hacker schlagen in der Schweiz zu: Die unfassbar lange Opfer-Liste (watson.ch)

Schwere Cyber-Ransomware Attacken auf CH-Firmen

- Amag Schweiz mit Neuaufbau der IT-Systeme (31.01.2020)
- Swisswindows AG / Ging nach Angriff sogar Konkurs (27.02.2020)
- Griesser Storenhersteller Aadorf komplette Produktion gestoppt (April 2021)
- Zürich Versicherung spanische Kundendaten im Darknet angeboten (Juni 2021)
- Der Schokoladenhersteller Camille Bloch wird gehackt (Oktober 2021)
- Media-Markt ERP-System gehackt 50 Mio Forderung (9.11.2021)
- Produktion des Fahrzeugbauers Bucher Industries wird lahmgelegt. (Nov. 2021)
- Autohändler Emil Frey Diebstahl von Kunden-Daten (12.1.2022)
- Die CPH-Gruppe in Perlen, Produktion Zeitungspapierfabrik gestört (Januar 2022)

Cyber-Attacken auch auf CH-Verwaltungen und Spitäler

- Gewerbeschule (AGS) Basel-Stadt (9.4.2021)
- Hirslanden Klinik (14.8.2021)
- Rolle (24.8.2021)
- EasyGov-Plattform des Bundes (August 2021)
- Montreux (11.10.2021)
- Mellingen (27.10.2021)
- Stadtverwaltung Yverdon (13.1.2022)
- Das Internationale Rote Kreuz (IKRK) (20.1.2022)

Aktuell: 24.5.2022 Hacker legen ganzes österreichisches Bundesland lahm (IT-Systeme der Kärntner Landesverwaltung)
Alle Services für die Bürgerinnen und Bürger mussten eingestellt werden – **Fünf Millionen Dollar in Bitcoins gefordert.**

Halbjahresbericht NCSC 2021/Juli-Dezember

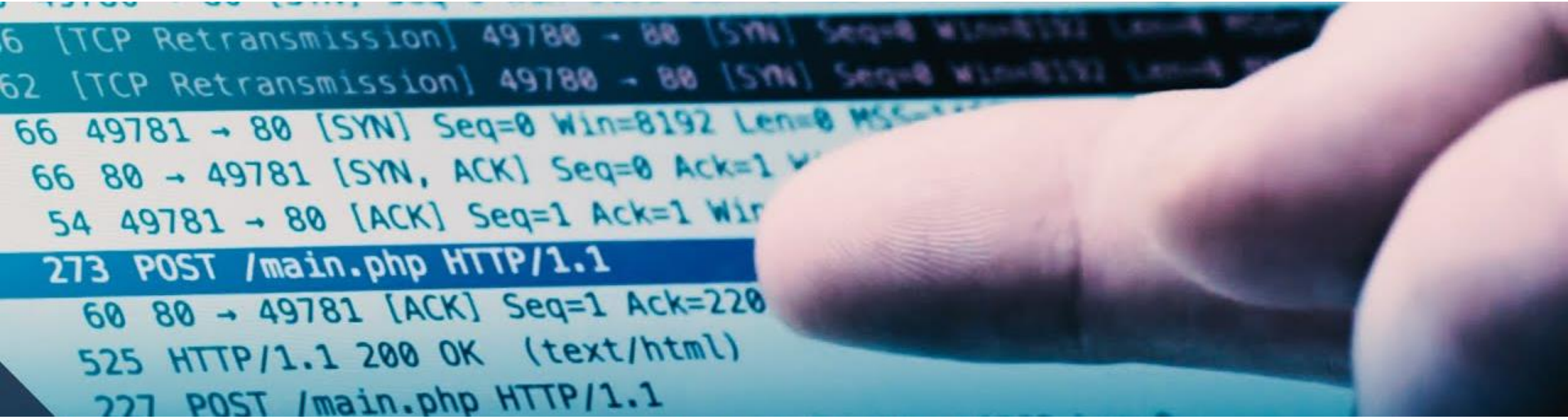
Insbesondere **CEO-Betrug, Fake-Support-Anrufe, Fake-Strafverfolgungs-E-Mail und Kleinanzeigenbetrug** wurden sehr häufig gemeldet. Trend zu aufwändigeren, individualisierten Vorgehen - Insgesamt sind im Berichtszeitraum bei der Anlaufstelle des NCSC 11'480 Meldungen zu Cybervorfällen eingegangen.

- **Ransomware und Datenabfluss** (Daten werden wegkopiert und dann verschlüsselt) → Doppelte Erpressung (Falls Lösegeld wegen vorhandenem Backup möglich droht Veröffentlichung der Daten)
- **Sicherheit folgt Funktionalität** Viele kritische Schwachstellen in Software-Komponenten (Java Log4j)
- **Phishing weiterhin im Trend** Spitzenreiter sind Paketankündigungen, Zustellprobleme, doppelt bezahlte Rechnungen, O365-Probleme

Nationalen Zentrums für Cybersicherheit (NCSC)

Link: https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2021-2.html

2. Cyberdelikte verhindern - Wegleitung



Zehn Tipps, um Cyberangriffe zu verhindern (I)

1. **Sichern Sie Ihre Daten**

   Regelmässig und zusätzlich getrennt (offline) und ausser Haus (offsite)

2. **Regeln Sie den Umgang mit Unternehmensinformationen**

   Möglichst wenig Personeninformation auf Webseiten und in Clouddiensten

3. **Sensibilisieren Sie Ihre Mitarbeitenden im Umgang mit E-Mails**

   Durchführung Phishing Sensibilisierung Übung

4. **Verwenden Sie sichere Passwörter.**

   Setzen Sie für Remote-Zugriffe zwingend auf eine Zwei-Faktor Authentisierung.

5. **Regeln Sie den Zugriffsschutz auf Daten**

   Mitarbeitende sollten standardmässig über keine Adminrechte verfügen.

Zehn Tipps, um Cyberangriffe zu verhindern (II)

6. **Verwenden Sie für Zahlungen ein separates System/Computer**
   Auf dem Sie nicht im Internet surfen oder E-Mails empfangen.
7. **Regeln Sie die Prozesse, die den Zahlungsverkehr betreffen**
   Zum Beispiel Vier-Augen-Prinzip und Kollektivunterschrift
8. **Umsetzen Einspielung von automatischen Sicherheitsupdates**
   Zwingend Betriebssystem und Office-Anwendung
9. **Installieren Sie einen Virenschutz**
   Auf jedem Computer ist der Echtzeitschutz aktiviert
10. **Schützen Sie Ihr Unternehmensnetzwerk vor dem Internet (Firewall)**
    Unterteilen Sie Ihr IT-Netz minimal in Produktion, Personal und Buchhaltung.

Checkliste **Vorbereitung** für Cyberangriff

- Gibt es in Ihrem Unternehmen ein Krisenteam für den Fall eines Cyberangriffs?
- Ist das Krisenteam mit notwenigen Ressourcen und Kompetenzen ausgestattet?
- Verfügt das Krisenteam über ein aktuelles Handbuch mit Kontaktdaten?
- Ist das Team mit den Prozessen der Strafverfolgung oder der technischen Beratung vertraut?
- Unterzieht sich das Krisenteam regelmässigen Übungen?

Checkliste **Erste Hilfe** bei einem Cyberangriff

1. **Isolieren**

   > Trennen Sie alle Systeme umgehend vom Netzwerk. Vergessen Sie nicht, das WLAN auszuschalten.

   > Warten Sie mit dem Wiederaufsetzen der Systeme, bis die Polizei oder das spezialisierte Unternehmen die Spuren gesichert hat.

2. **Kontaktieren**

   > Kontaktieren Sie umgehend die Polizei.

   > Spezialisierte privatwirtschaftliche Unternehmen helfen Ihnen, Ihre Infrastruktur zu reparieren und gegebenenfalls wiederherzustellen.

   > Melden Sie auch Angriffsversuche ohne Schaden bei MELANI

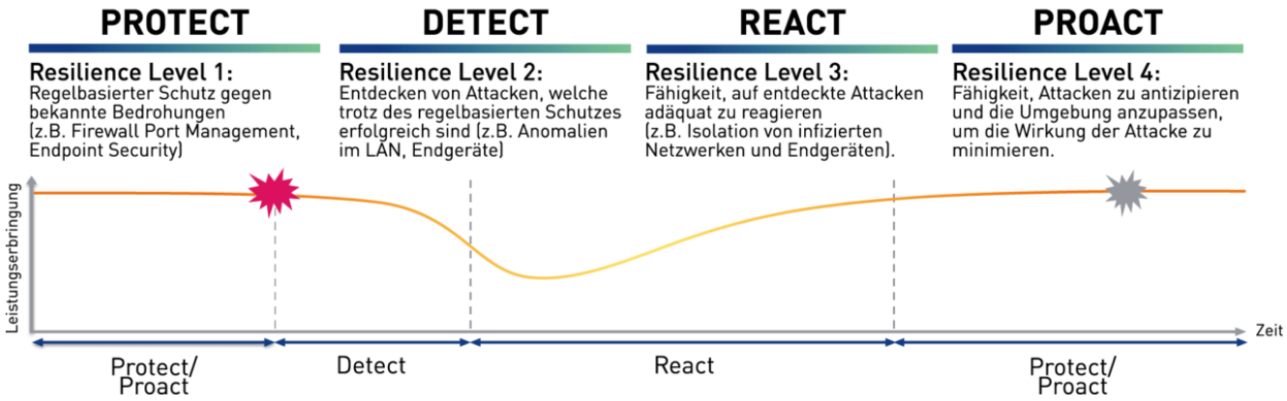
Checkliste **Nachbearbeitung** eines Cyberangriff

Lesson Leraned: Kann etwas verbessert werden?

- Präventive oder zeitnahe Erkennung eines Vorfalls?
- Qualität und Geschwindigkeit der Vorfalleinschätzung (Schadenausmass, usw.)?
- Angemessene und zeitnahe Reaktion/Eskalation bei Bedarf?
- Bewältigung des Vorfalls mit Sofortmassnahmen zur Eindämmung des Schaden?
- Massnahmen und Hilfsmittel zur Aufrechterhaltung eines Notbetriebs?
- Interne Zusammenarbeit sowie die Zusammenarbeit mit externen Instanzen?
- Kommunikation nach innen und aussen?
- Effektivität und Effizienz des Notfallhandbuches?

Fazit

- Schlecht gewartete IT-Systeme und im Umgang mit Cybergefahren ungeschulte Mitarbeitende erhöhen das Risiko, auf der täglich wachsenden Liste der Ransomware-Opfer zu landen.



3. Was tun bei einem Cyberangriff

Checkliste Malwarebefall – was tun?

Ergreifen Sie erste Gegenmassnahmen im Firmennetz:

- Trennen Sie möglichst umgehend betroffene Geräte und Computer vom Netzwerk
- Detektieren Sie täterische URL und IP-Adressen sowie das Infektion-Ausmass
- Blockieren Sie täterische URL und IP-Adressen auf der Firewall.

Meldung:

Kontaktieren Sie Ihren IT-Partner sowie MELANI und die Zuger Polizei und definieren Sie zusammen das weitere Vorgehen.

Sichern Sie die relevanten Daten:

Sichern Sie Logs der Firewall, E-Mails etc.

Checkliste DDoS-Angriff – was tun?

Ergreifen Sie erste Gegenmassnahmen:

- Kontaktieren Sie Ihren Internetprovider, um den Angriff zu stoppen.
- Unter Umständen können Sie selbst Gegenmassnahmen ergreifen, indem Sie die IP-Adressen auf der Firewall blockieren (GEO-Blocking) oder Routing anpassen.

Meldepflicht:

- Kontaktieren Sie MELANI und die Zuger Polizei
- Teilen Sie Internetprovider und Quell- und Zieladressen des Angriffs mit.

Überprüfen Sie Ihr Netzwerk:

- DDoS-Angriffe werden häufig benutzt, um Angriffe wie Einschleusen von Malware oder Diebstahl von Daten zu verschleiern. Überprüfung auf Anomalien!

Ich habe einen Vorfall – Wem muss/kann ich es melden?

Zuger Polizei

i) Bei akuten und laufenden Fällen sich bei der **Einsatzzentrale** melden. Mann wird dann mit einem Sachbearbeiter verbunden und kann das weitere Vorgehen besprechen.
ii) Möglichkeit, direkt auf einer Polizeidienststelle zu Bürozeiten die Anzeige zu deponieren.
iii) Falls der Cyberangriff bereits Vergangenheit ist und es nun um die Strafanzeige geht, empfehlen wir, diese direkt schriftlich bei der Staatsanwaltschaft des Kantons Zug zu machen.

Meldestelle Melani

Kontakt (admin.ch)

Weitere Informationen:

Nationales Zentrum für Cybersicherheit (NCSC)

Informationen für Unternehmen (admin.ch)

Deutschland Bundesamt für Informationssicherheit

BSI - Ich habe einen IT-Sicherheitsvorfall - Was soll ich tun? (bund.de)

Fazit

VERHALTEN BEI IT-NOTFÄLLEN

Ruhe bewahren & IT-Notfall melden
Lieber einmal mehr als einmal zu wenig anrufen!

IT-Notfallrufnummer:

Wer meldet?

Welches IT-System ist betroffen?

Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?

Wann ist das Ereignis eingetreten?

Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

Weitere Arbeit am IT-System einstellen | Beobachtungen dokumentieren | Maßnahmen nur nach Anweisung einleiten

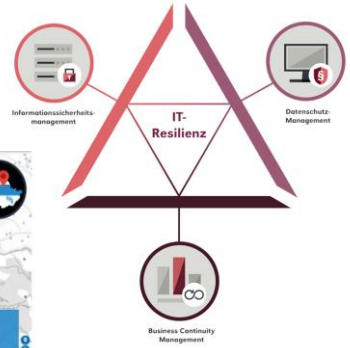
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

Ohne Vorkehrung ist man verloren!

- Not-Organisation (Kontakte)
- IT-Unterstützungspartner (Bereitschaft)
- Entscheid Lösegeld bezahlen oder Unterbruch und Neuinstallation (Wer verfügt über BitCoin Knowhow bzw. Zahlungs-Konto…)
- …

4. Wie macht der Kanton Cybersecurity?

Kann der Kanton Zug sich einen Datendiebstahl erlauben?



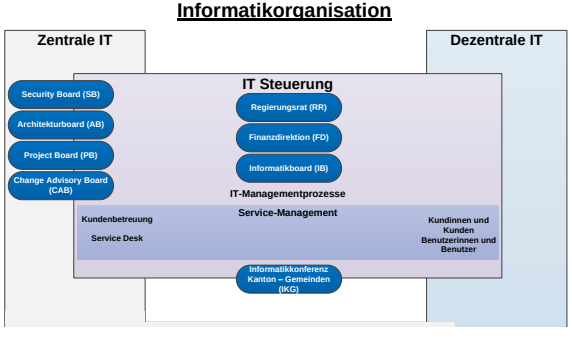
Die Widerstandsfähigkeit ist immer ein Spannungsfeld

Ziel IT-Sicherheit - Informatikstrategie 2018-2022

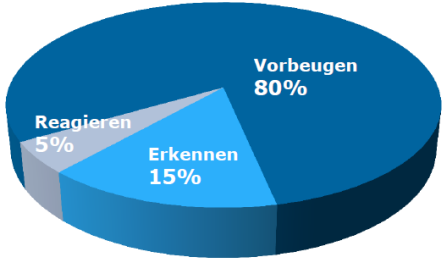
«Die Sicherheit, Verfügbarkeit und Integrität sind gewährleistet.»

Massnahmen:

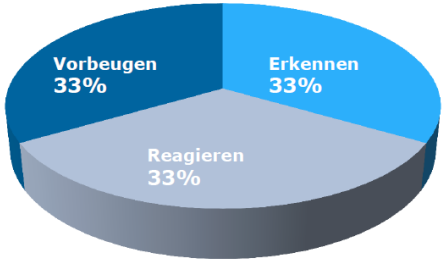
- IT-Sicherheit als Teil der Rechenzentrum-Strategie
- Business Continuity Management verbessern und Notfallplanung festlegen
- Kompetenzen IT-Sicherheitsbeauftragten festlegen
- Verantwortlichkeiten der Direktionen zur IT-Sicherheit definieren



Herausforderung Cyber Security?



Ausgaben Cybersecurity heute



Ausgaben Cybersecurity morgen

Bei der heute geforderten Digitalisierung reicht der Fokus auf präventive Massnahmen nicht mehr aus! Gefordert sind:

- Visibilität bzgl. Cyber-Angriffe.
- Vorbereitete Reaktionsmöglichkeiten bezüglich Gegenmassnahmen

Was macht der Kanton Zug gegen Cyber-Angriffe?

Die fünf Kernpunkte:

1. **IT-Governance:** (Organisation / Prozesse / ISO27001 Zertifizierung)
2. **Sensibilisierung:** User-Ausbildung (Awarness)
3. **Vorbeugen:** Robuste IT-Infrastruktur (Technisch Proaktiver IT-Schutz)
4. **Erkennen:** Einführung SecurityOperationCenter (SOC) in Planung
5. **Reagieren** (Notfall-Krisenbewältigung mit digitaler Notfallkoffer www.zglogin.ch)

Merkblätter zur Verhinderung von Cyberbetrug

Kanton Zug

Infos zum Coronavirus | Kontakt | iZug | Deutsch

Behörden | A bis Z | Online-Dienstleistungen | zg.ch durchsuchen

Startseite ▸ Behörden ▸ Sicherheitsdirektion ▸ Zuger Polizei ▸ Prävention ▸ Kriminalität ▸ Cyberbetrug_Internetbetrug

Kriminalität ↑

Cyberbetrug_Internetbetrug

Cyberbetrug_Internetbetrug

Downloads

Typ	Titel	Bearbeitet
	Factsheet Romance Scam	03.10.2019
	Merkblatt Phishing	13.10.2016
	Merkblatt_Betrügerische Online-Shops	13.10.2016
	Merkblatt_Fingierte Immobilienanzeigen	13.10.2016
	Merkblatt_Geld erschwindeln mit Identitätsmissbrauch	13.10.2016
	Merkblatt_Internetbetrug über Websites, Auktionsplattformen und Kleinanzeigen	13.10.2016
	Merkblatt_Lieferbetrug	13.10.2016
	Merkblatt_Vorschussbetrug	13.10.2016

- Cyberbetrug_Internetbetrug — Kanton Zug (zg.ch)

Weitere bereit gestellte Dienste

Merkblätter Informationssicherheit
Merkblätter Informationssicherheit — Kanton Zug (zg.ch)

Lernplattform Schulung Informationssicherheit:
https://elearning.zg.ch/ela

Tipps&Tricks zu Phishing E-Mails
https://extranet.zg.ch/phishing.html

Fragen?

Informationssicherheit entsteht durch einen Beitrag von allen Beteiligten.
Helfen Sie mit dabei!

Rudolf Gisler

IT-Security — Kanton Zug (zg.ch)