

Cybersicherheit im ARA-Alltag

Reto Steinemann

Das OT-Netzwerk – im Wandel der Zeit

IT (Informationstechnologie) vs. OT (Operative Technologie)

↗ Zweck und Anwendungsbereich

- ↗ IT: Datenverarbeitung und Informationsmanagement (Büros, Rechenzentren).
- ↗ OT: Steuerung und Überwachung von industriellen Anlagen oder Maschinen.

↗ Systeme und Geräte

- ↗ IT: Computer, Server, Netzwerke, Softwarelösungen.
- ↗ OT: Maschinensteuerungen, Sensoren, Aktoren, SCADA-Systeme.

↗ Sicherheitsanforderungen

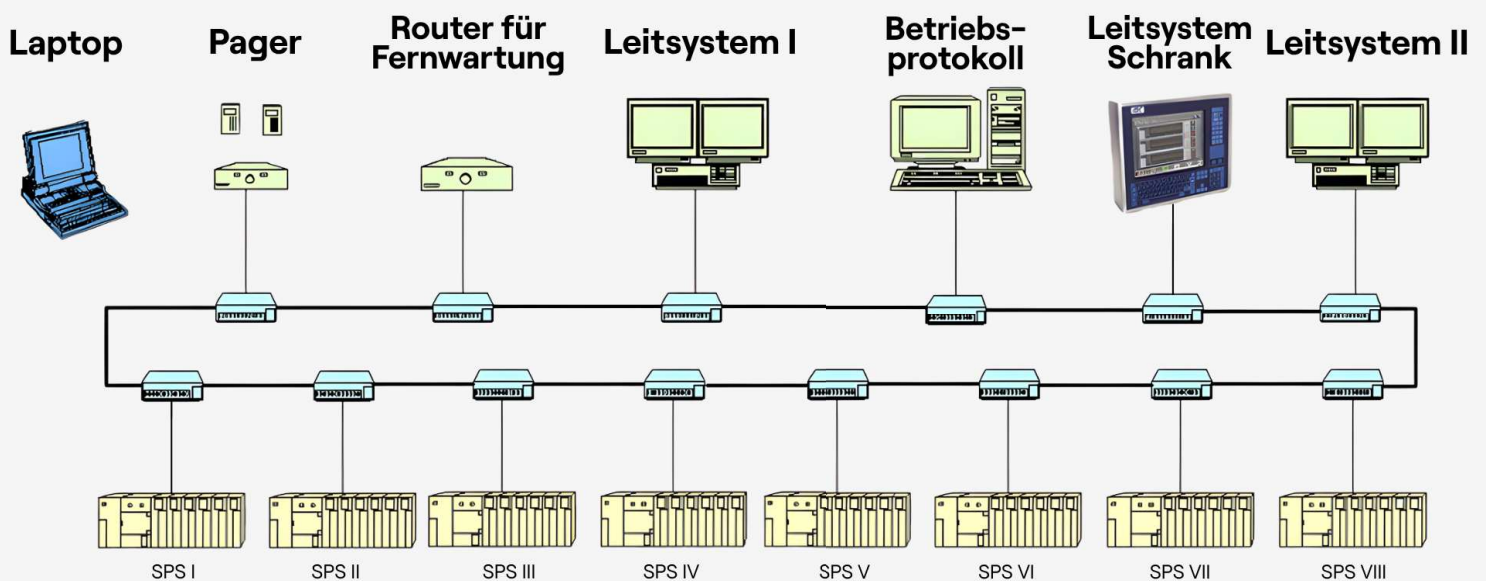
- ↗ IT: Schutz von Daten und Netzwerken (Datenschutz, Verschlüsselung).
- ↗ OT: Schutz physischer Prozesse und Systeme vor Ausfällen oder Manipulation.

Cybersicherheit im OT-Netz

- Das OT-Netzwerk im Wandel der Zeit
- Angriffswege
- Wie können wir uns schützen?
- Grundschutz



Das OT-Netzwerk 2000

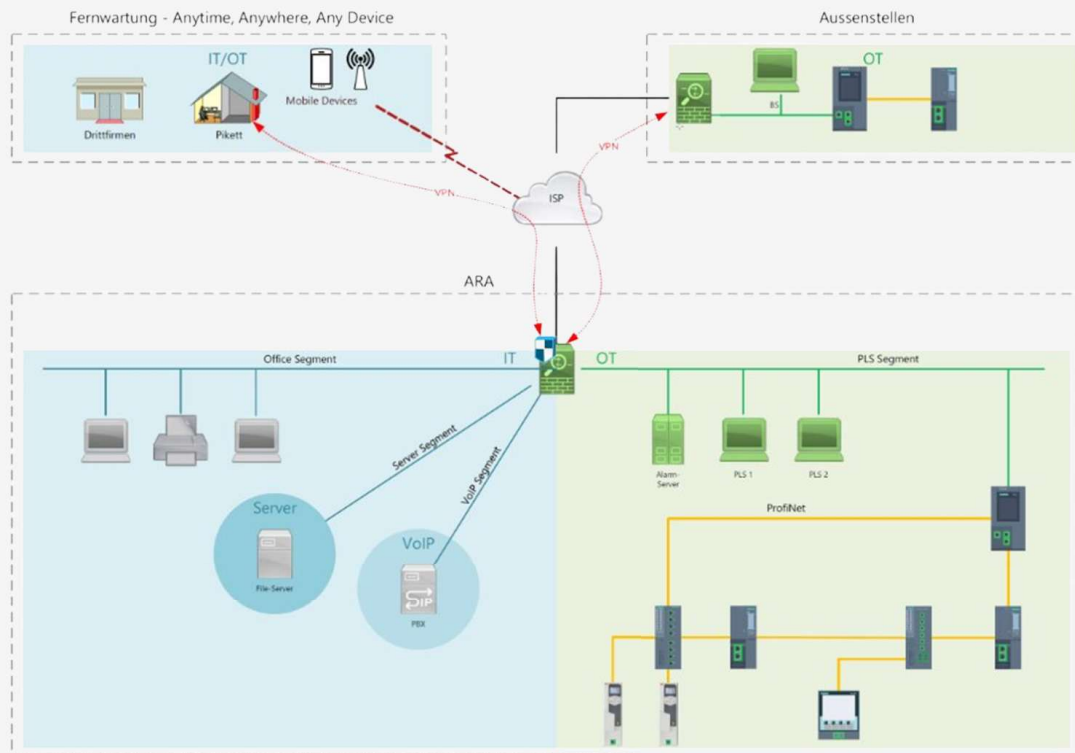


Die Standorte der Hubs und Switches richtet sich nach den örtlichen Gegebenheiten und kann heute nicht abschliessend behandelt werden.

— 100 Mbit Bus Redundanter Ring

 OLM-ITP





7

Das OT-Netzwerk – im Wandel der Zeit

Das Automationsnetz ist im Grundsatz gleich geblieben

- Der defensive Ansatz...
- Möglichst isolierte und exklusive Nutzung des Netzes
- Schutz der Leitsystemrechner und der Steuerungssysteme

Neue Fernwartungsansprüche

- „Anytime – Anywhere – AnyDevice“

Zunehmend mehr Zugriffe auf andere Netze

- Vernetzung mit der IT-Welt
- Internetzugriff für Alarmierung, Wetterdaten, etc.



8

Das OT-Netzwerk – im Wandel der Zeit

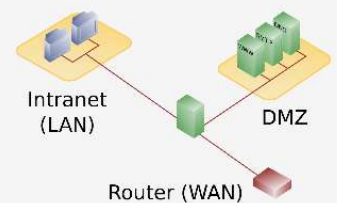
Neue Devices und neue Netze

- IT-Netz (Büro)
- Kantons-/Gemeinde-Netz
- Fremdsystem-Netz
- Telefonie-Netz
- Kamera-Netz
- WLAN (Betrieb, Gäste, Telefonie, etc.)
- DMZ-Netze (Fernwartung)



Anbindung von Aussenstellen

- Aussenstellen-Netz (LWL, SHDSL, etc.)
- VPN (All-IP, xDSL, Cabel, LTE, etc.)



9

Angriffswege

Unsichere Firmware oder Fehlkonfiguration in der Firewall

- Unsichere Geräte direkt vom Internet erreichbar

Internetzugriff

- Webseite mit Malware
- Programm heruntergeladen, mit Malware
- E-Mail mit «böartigem Link» oder Malware im Anhang

Fernwartungszugriff (VPN)

- Schlecht abgesicherter Zugang
- Befallenes Gerät im Netz (PC, Notebook, Tablet, etc.)



10

Angriffswege

Portable Medien (Memory-Stick oder externe Festplatte)

- Datei mit Schadenscode (Office-Dokument mit Makro)
- Manipulierter Memory-Stick (Rubber Ducky, Bash Bunny, etc.)

IT-Umgebung

- Befallenes Gerät (Büro-PC, etc.)

WLAN

- Schlecht geschützter Zugang
- Befallenes Gerät im Netz (Notebook, Tablet, etc.)



11

Wie können wir uns schützen?

Defense-in-Depth

- Angriffe brauchen mehrere Schritte, damit sie erfolgreich sind
- Jeder Schritt ist eine Gelegenheit, den Angriff abzuwehren
- Je mehr Schritte, desto weniger Chancen hat ein Angriff

Risikobasierter Ansatz

- Man muss nicht alles machen, aber...
- ...man muss wissen, was man nicht macht und warum
- (Schweregrad des Schadens x Wahrscheinlichkeit) vs. Kosten
- Die OT-Verfügbarkeit muss mitberücksichtigt werden



Wir brauchen einen „Grundschutz“, der die relevanten Risiken abdeckt
Strategie: «Bottom Up»



12

Grundschutz

Bewusstsein bei den Benutzern schaffen

- Welche OT-Systeme haben wir?
- Welche Risiken bestehen?

Massnahmen

- Bewusstsein (von allen Beteiligten)
- IKT-Minimalstandard
- OT-Security-Checkliste
 - Bestandesaufnahme (Inventur)
 - Periodische Überprüfung



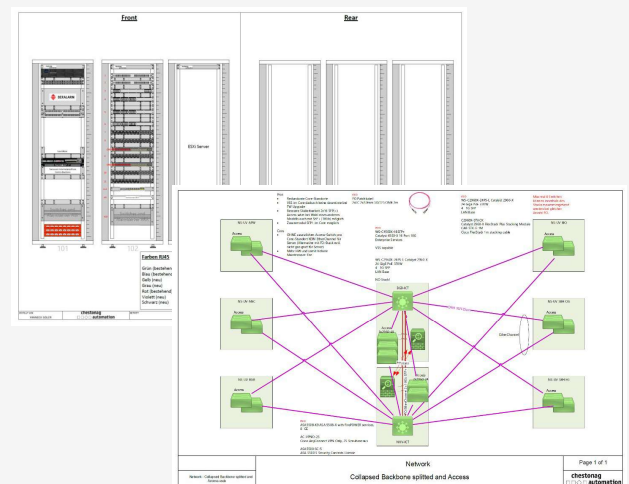
Grundschutz

Segmentierung der Netze

- Nur so viel Internetzugang wie nötig
- Möglichst kein Zugriff in das OT-Netz (VPN!)
- Nur gezielter Zugriff aus dem OT-Netz
- Weiter Netze für spezifische Anforderungen

Massnahmen

- Ausbau der Netzwerkkonzepte
 - Standardisiert
 - Segmentierung / restriktive Firewall-Regeln
- Professionelle Komponenten
 - Benötigter Funktionsumfang
 - Verfügbarkeit / Redundanz



Grundschatz

Pers6nliche Benutzer und Passwortrichtlinien

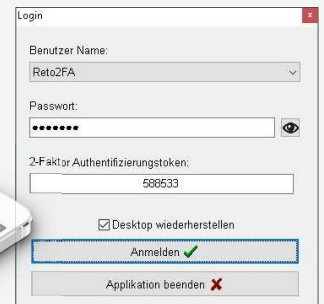
- Alle Systeme m6ussen gegen ungewollten Zugriff gesch6utzt sein
- Benutzer m6ussen eindeutig identifiziert werden

Massnahmen

- Awareness-Schulungen
- Passwortrichtlinien im Leitsystem
- Multifaktor-Authentifizierung
 - Leitsystem
 - Fernwartungszugang

Top 20 deutscher Passw6orter:

1	123456	11	qwertz
2	123456789	12	michael
3	passwort	13	killer
4	hallo123	14	michelle
5	12345678	15	hallo
6	ichliebedich	16	sonnenschein
7	1234567	17	alexander
8	1234567890	18	Passwort
9	lol123	19	abc123
10	12345	20	daniel



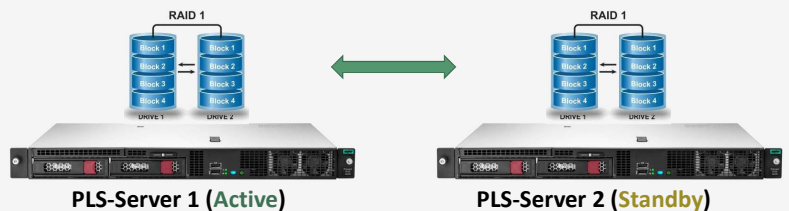
Grundschatz

Backup der Projekt-/Archivdaten

- Datenverlust verhindern
- Rasche Wiederherstellung

Massnahmen

- PLS-Server
 - Redundant
 - RAID-Speicher
 - Standardhardware (Lager)
- Versioniertes Backup
 - Auf der Anlage mit einem NAS
 - Bei CAG als Dienstleistung



Grundschutz

Regelmässige Wartung

- Patchen der Systeme (Firewall, PC's, etc.)
- Kontrolle der Konfigurationen
- Kontrolle der Benutzerlisten und Passwörter

Massnahmen

- Wartungsverträge/-Offerten mit definierten Leistungen
 - Periodische Wartung der Systeme
 - Einspielen von Patches und Updates (Systemspezialisten)
 - Kontrolle der Systeme (Systemspezialisten, Projektleiter)

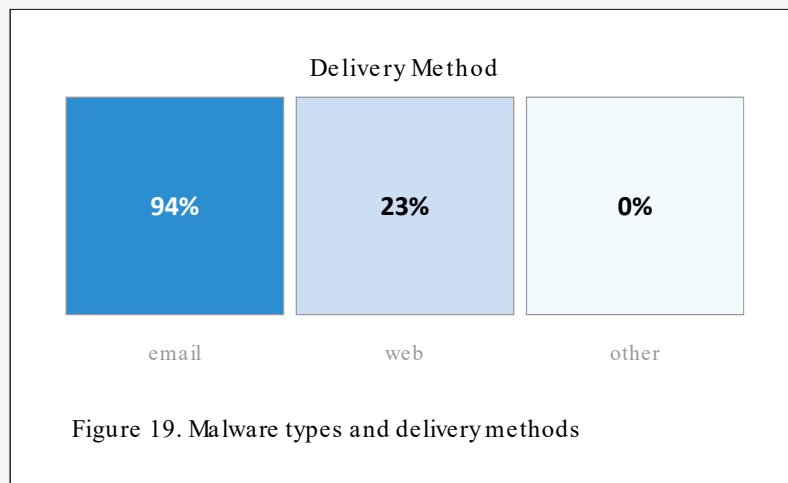


Cybersicherheit im IT-Netz

- Angriffswege
- Updates
- Surfen & E-Mails
- Social Engineering
- Passwörter & 2ter Faktor
- Meldepflicht für Cyberangriffe



Cybersicherheit im IT-Netz - Angriffswege



Hauptursachen für erfolgreiche Angriffe



Alte Systeme/Software



World Wide Web



E-Mail

Wenn wir diese drei Ursachen beheben, sind wir schon sehr sicher



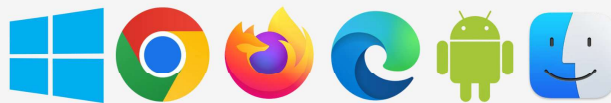
Cybersicherheit im IT-Netz - Updates

Es war noch nie so einfach, Updates durchzuführen

- Automatisch
- Zuverlässig und stabiler (als auch schon...)

Die wichtigsten Updates

- Betriebssystem
- Browser
- Mailclient



JUST DO IT.



Cybersicherheit im IT-Netz – sicher «Mailen»

- Sich nie unter Druck setzen lassen
- Keine Passwörter eingeben
- Keine unerwarteten Anhänge öffnen
- Keine unbekanntes Links anklicken
- Keine Makros aktivieren

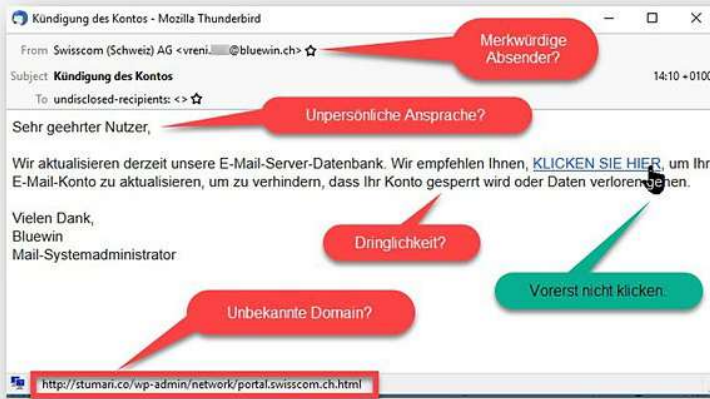
Im Zweifelsfall

- Zweite Meinung einholen
- Absender/-in direkt kontaktieren

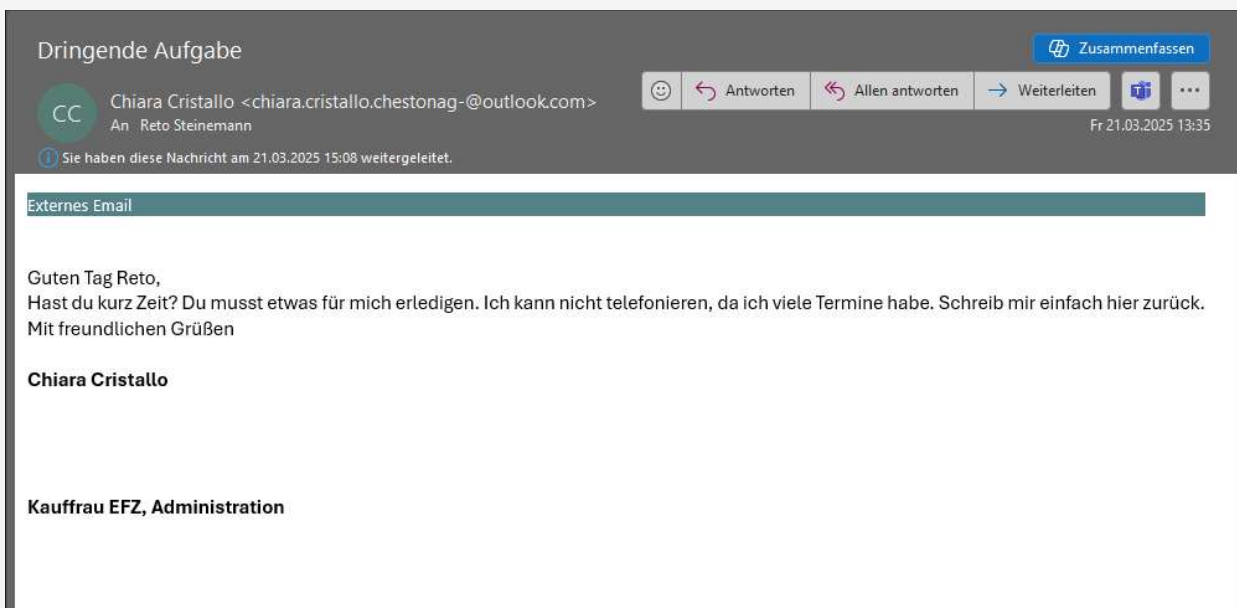


Beispiele

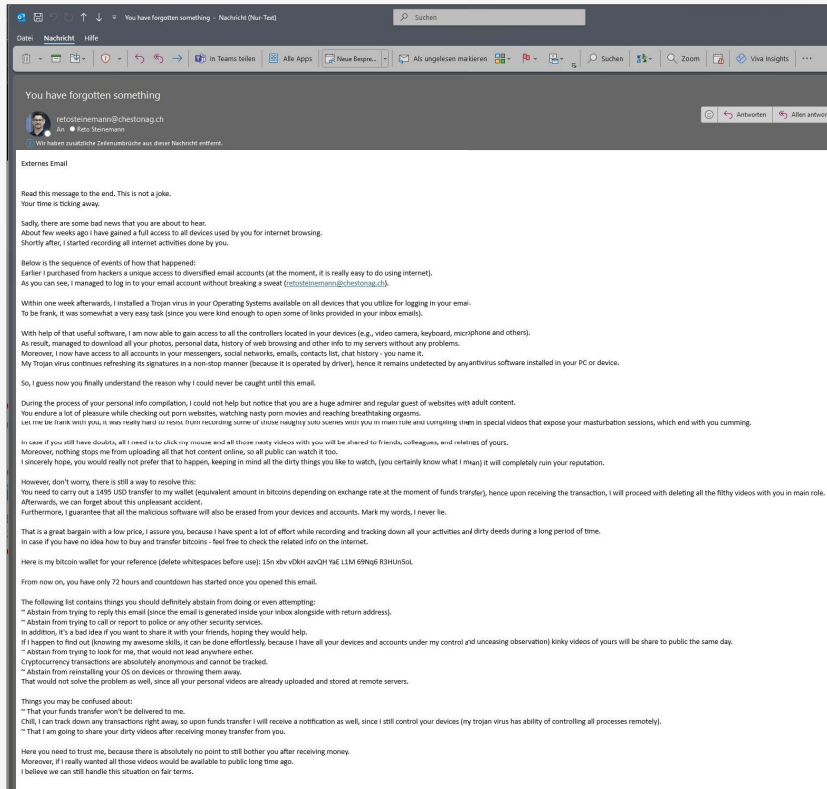
Phishing oder nicht?



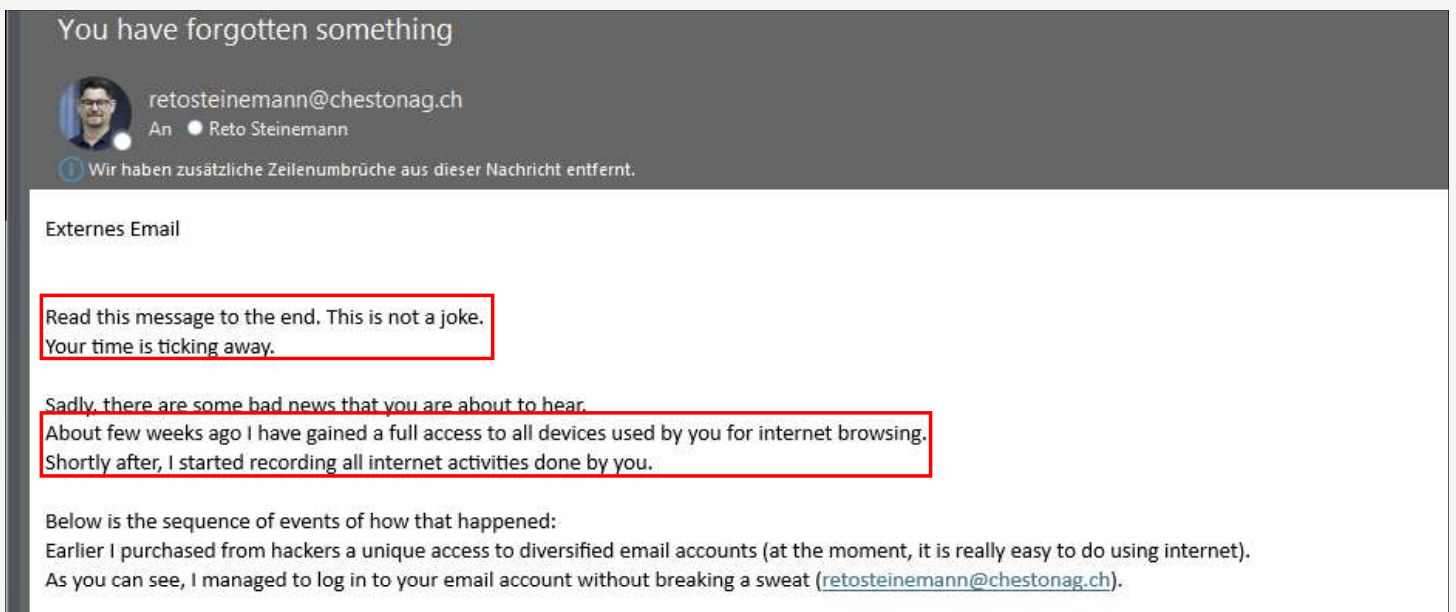
Beispiele



Beispiele



Beispiele



Beispiele

In case if you still have doubts, all I need is to click my mouse and all those nasty videos with you will be shared to friends, colleagues, and relatives of yours. Moreover, nothing stops me from uploading all that hot content online, so all public can watch it too. I sincerely hope, you would really not prefer that to happen, keeping in mind all the dirty things you like to watch, (you certainly know what I mean) it will completely ruin your reputation.

However, don't worry, there is still a way to resolve this:

You need to carry out a 1495 USD transfer to my wallet (equivalent amount in bitcoins depending on exchange rate at the moment of funds transfer), hence upon receiving the transaction, I will proceed with it. Afterwards, we can forget about this unpleasant accident.

Furthermore, I guarantee that all the malicious software will also be erased from your devices and accounts. Mark my words, I never lie.

That is a great bargain with a low price, I assure you, because I have spent a lot of effort while recording and tracking down all your activities and dirty deeds during a long period of time. In case if you have no idea how to buy and transfer bitcoins - feel free to check the related info on the Internet.

Here is my bitcoin wallet for your reference (delete whitespaces before use): 15n xbv vDkH azvQH YaE L1M 69Nq6 R3HUn5oL

From now on, you have only 72 hours and countdown has started once you opened this email.



Beispiele

The following list contains things you should definitely abstain from doing or even attempting:

~ Abstain from trying to reply this email (since the email is generated inside your inbox alongside with return address).

~ Abstain from trying to call or report to police or any other security services.

In addition, it's a bad idea if you want to share it with your friends, hoping they would help.

If I happen to find out (knowing my awesome skills, it can be done effortlessly, because I have all your devices and accounts under my control and unceasing observation) kinky videos of yours will be shared to my contacts.

~ Abstain from trying to look for me, that would not lead anywhere either.

Cryptocurrency transactions are absolutely anonymous and cannot be tracked.

~ Abstain from reinstalling your OS on devices or throwing them away.

That would not solve the problem as well, since all your personal videos are already uploaded and stored at remote servers.

Things you may be confused about:

~ That your funds transfer won't be delivered to me.

Chill, I can track down any transactions right away, so upon funds transfer I will receive a notification as well, since I still control your devices (my trojan virus has ability of controlling all processes remotely).

~ That I am going to share your dirty videos after receiving money transfer from you.

Here you need to trust me, because there is absolutely no point to still bother you after receiving money.

Moreover, if I really wanted all those videos would be available to public long time ago.

I believe we can still handle this situation on fair terms.



Social Engineering - Schutz

➤ Auf Details achten

- Stimmt die E-Mail-Adresse, oder ist da doch ein Buchstabe anders?

➤ Sich nicht unter Druck setzen lassen

- Man hat immer fünf Minuten Zeit, um kurz durchzuatmen und sich das Ganze nochmals zu überlegen.

➤ Über andere Kanäle Korrektheit der Nachricht bestätigen

- Wenn der Chef einem eine «dringende» E-Mail geschickt hat, kurz per Telefon nachfragen. Einen Kollegen fragen. Macht die Nachricht Sinn? Hat er sie auch bekommen?

➤ Sich auf sein Bauchgefühl verlassen

- Scheint die Anrede etwas zu höflich? Die Redewendungen etwas steif? Oder erweckt die E-Mail sonst irgendwie Misstrauen?



31

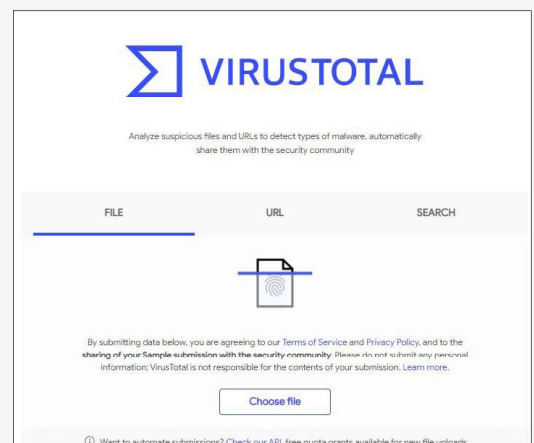
Was tun im Zweifelsfall?

➤ Für E-Mails mit dubiosem Anhang aus vertrauter Quelle

➤ <https://www.virustotal.com/gui/home/upload>

➤ Falls die Probleme bereits da sind:

- Netzwerk trennen
- PC nicht ausschalten
- Spezialisten kontaktieren



32

Cybersicherheit im IT-Netz - Passwörter

➤ Sichere Passwörter

- ...sind schwer zu erraten
- ...sind lange
- ...sind einfach zu merken
- ...nur für eine Webseite oder Applikation verwenden

Beispiele:

- **Thomas** = schlechtes Passwort, einfach zu erraten
- **@#hJSDF23** = schlechtes Passwort, schwer zu merken
- **JedenMorgenEsselchEineBratwurst** = gutes Passwort, schwer zu erraten, einfach zu merken



Welche Passwörter nutzen Herr und Frau Schweizer am häufigsten?

Ok, das ist jetzt auch kein Ruhmesblatt:

1. dominaria
2. admin
3. purzi123
4. Divinorum88
5. 123456
6. chocolat36
7. 1a2s3d4f5g6h
8. password
9. 123456789
10. pascal87



Cybersicherheit im IT-Netz - Passwortmanager

➤ Alle Passwörter werden in eine Anwendung verwaltet

- Webseiten, Applikation, etc.
- Als Anwendung/App oder als Cloud-Service erhältlich

➤ Es gibt nur ein "Master-Passwort" zum merken

- Alle anderen Passwörter sind im Passwort-Manager gespeichert
- Viel einfacher, als sich 30 verschiedene Passwörter zu merken

➤ Keine "Redundanz"

- Ist der Passwort-Manager gehackt, ist alles bekannt
- Ist das Master-Passwort vergessen sind die Passwörter nicht mehr zugänglich

1Password

LastPass

Avira

DASHLANE

bitwarden



Meldepflicht für Cyberangriffe auf kritische Infrastrukturen

➤ Seit dem 1. April gilt:

- Betreiber kritischer Infrastrukturen müssen Cybervorfälle innert 24 Stunden dem Bundesamt für Cybersicherheit (BACS) melden

➤ Wer ist betroffen?

- Energieversorgung (Strom, Gas, Öl)
- Wasser- & Abwasserbetriebe
- ICT / Telekom / Logistik
- Gesundheitswesen, Verwaltung & Behörden

➤ Was muss gemeldet werden?

- Cyberangriffe (Malware, Phishing, Ransomware)
- Sicherheitsrelevante IT-Störungen
- Unbefugter Zugriff auf Daten / Systeme

➤ Ziel der Meldepflicht

- Frühzeitige Erkennung von Cyberbedrohungen
- Verbesserung der Zusammenarbeit zwischen Staat & Wirtschaft
- Stärkung der IT-Sicherheit in der Schweiz



Wie müssen Betroffene nun reagieren?

➤ Zuständigkeiten klären

- Wer meldet einen Vorfall? Was muss die verantwortliche Person bei einem Vorfall tun?

➤ Zugang zum Cyber Security Hub einrichten

- Über die BACS-Webseite kann ein Antragsformular ausgefüllt werden

➤ BACS-Webseite besuchen & einen Überblick erschaffen

- Solange man kein Zugang auf das CSH hat, muss ein Vorfall direkt über die BACS-Seite gemeldet werden.

www.ncsc.admin.ch

www.chestonag.ch/news/meldepflicht



BACS Halbjahresbericht



und dem Iran Mitte Juni 2025. Neben missbräuchlicher Manipulation der Systeme selbst wird hierzu auch sogenannte «Wiper»-Schadsoftware eingesetzt, die Systeme unbrauchbar macht und so den Betrieb von Versorgungs- oder Produktionssystemen verunmöglicht. Dies zeigt der Einsatz von «PathWiper» gegen kritische Infrastrukturen in der Ukraine im Juni 2025 exemplarisch.¹⁰³ Im Kontext der Schweiz wurden solche Sabotageakte durch staatliche Cyberakteure bislang nicht beobachtet und gelten als äusserst unwahrscheinlich. Hingegen sind Auswirkungen durch Kollateralschäden wegen eines Angriffs im Ausland jederzeit möglich.¹⁰⁴

Häufiger als solche gezielten Angriffe werden opportunistische Manipulationsversuche von ungenügend geschützten und im Internet exponierten industriellen Steuerungen beobachtet. Haktivisten-Gruppen versuchen, durch solche Angriffe möglichst viel Aufmerksamkeit zu er-

<https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2025-1.html>



37

Fazit

➤ Technische Massnahmen - Systemlieferanten

- Die OT- (und IT-)Systeme und die Risiken müssen bekannt sein
- Guter Grundschutz aufbauen
- Regelmässige Wartung

➤ Organisatorische Massnahmen - Cybersecurity-Experten

- Prozesse müssen beschrieben sein (Ein-/Austrittsprozess, Awareness-Schulungen,...)
- Es muss definiert sein, was wir tun, wenn etwas passiert

➤ Umgang mit IT-/OT Systemen

- Nie unter Druck setzen lassen
- Bedachter und Sorgfältiger Umgang
- Einhalten der Nutzungsrichtlinien



38

«IT/OT-Sicherheit ist kein Zustand, sondern ein Prozess»

Vielen Dank für Ihre
Aufmerksamkeit!

Chestonag Automation AG
Reto Steinemann
Wächterweg 4
CH-5707 Seengen
retosteinemann@chestonag.ch
+41 62 767 7004

