LUZERN

KANTON LUZERN

«Einer klickt immer!»

04. November 2022

Martin Achermann, CISO

Dienststelle Informatik | informatik.lu.ch

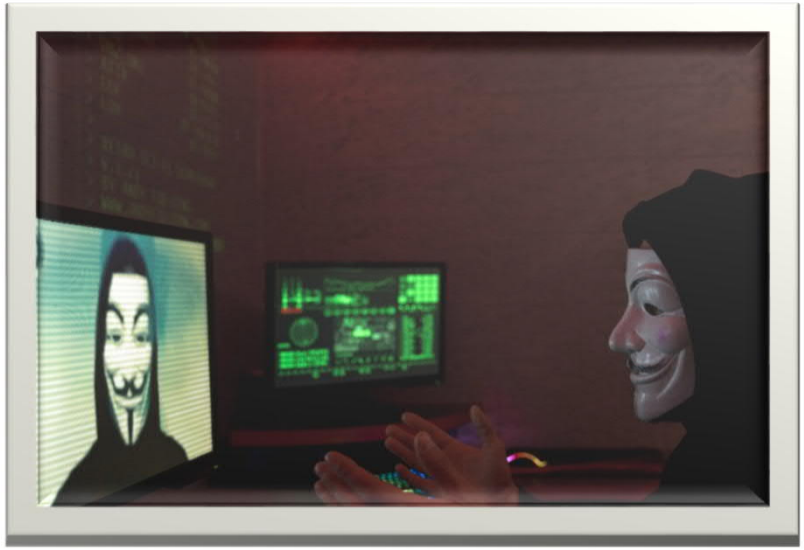
LUZERN

KANTON LUZERN

«Einer klickt immer!»

Warum der Schutz der Benutzerinnen und Benutzer erfolgskritisch ist!

1. Ein paar statistische Fakten
2. Fallbeispiel: Ransomware-Angriff auf die Landesregierung Kärnten
3. Fallbeispiel: Ransomware-Angriff auf den Energieversorger Colonial Pipeline
4. Ausblick: Was kommt als Nächstes?
5. Fragen & Antworten



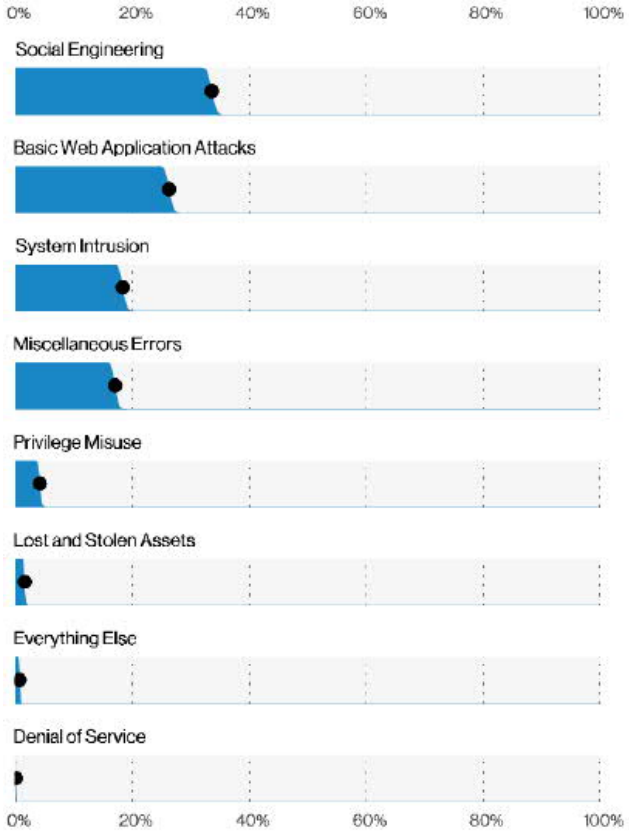
Dienststelle Informatik | informatik.lu.ch

LUZERN

KANTON LUZERN

EIN PAAR STATISTISCHE FAKTEN

Angriffsmuster und «Enabler»



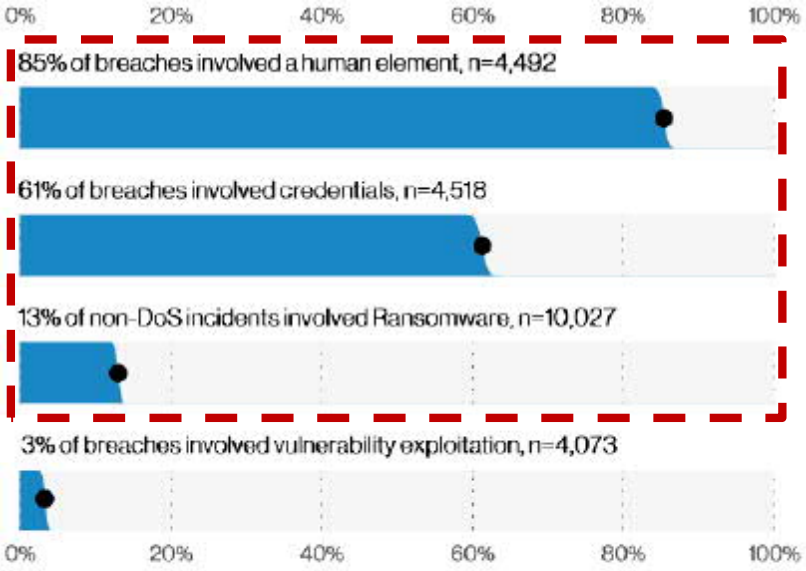
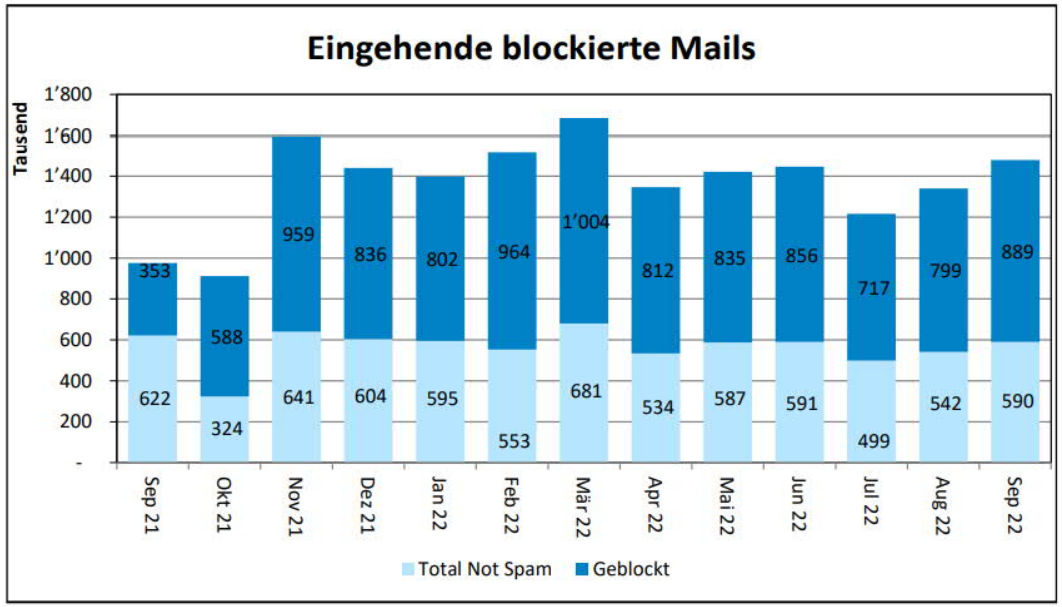


Figure 7. Select action varieties (n=4,073)

Quelle: 2021 Data Breach Investigations Report (Verizon)

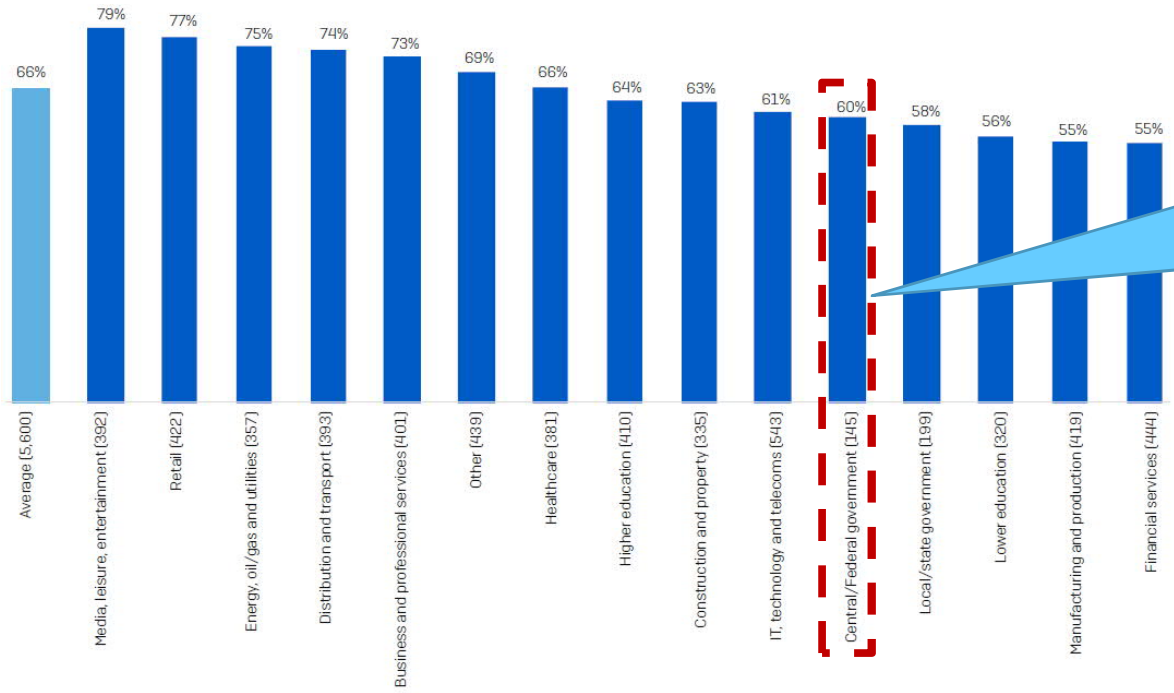
Beispiel: Schutzmassnahme



Quelle: DIIN
Monatsreporting September

> **E-Mails werden abgewiesen, sobald sie von einem nicht vertrauenswürdigen Absender kommen, eine Bedrohung darstellen (Spam, Viren, Phishing) oder unerwünschten Inhalt aufweisen.**

Von Ransomware im 2021 betroffene Organisationen



Statistisches Risiko im öffentlichen Sektor ist 60%

5,600 respondents

31 countries

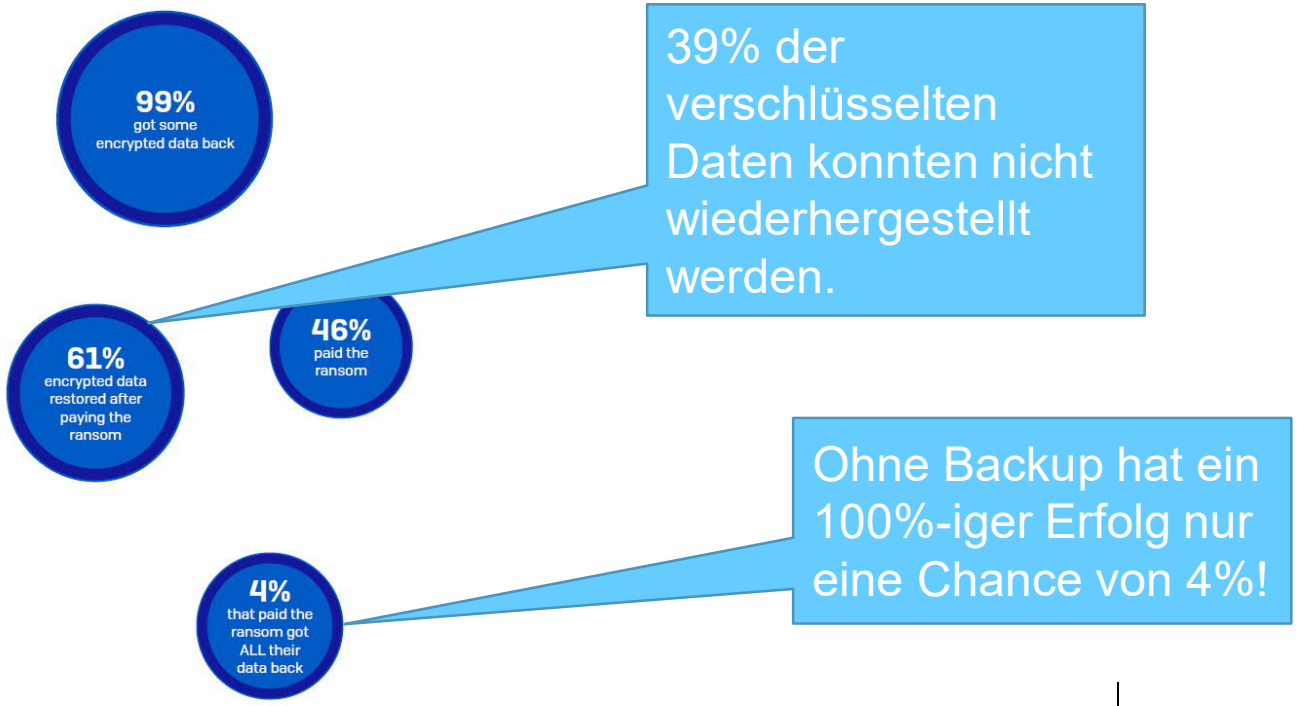
100-5,000 employee organizations

Jan/Feb 2022 research conducted

Quelle: The State of Ransomware 2022 (Sophos)

Dienststelle Informatik | informatik.lu.ch

Nicht immer können Daten wiederhergestellt werden



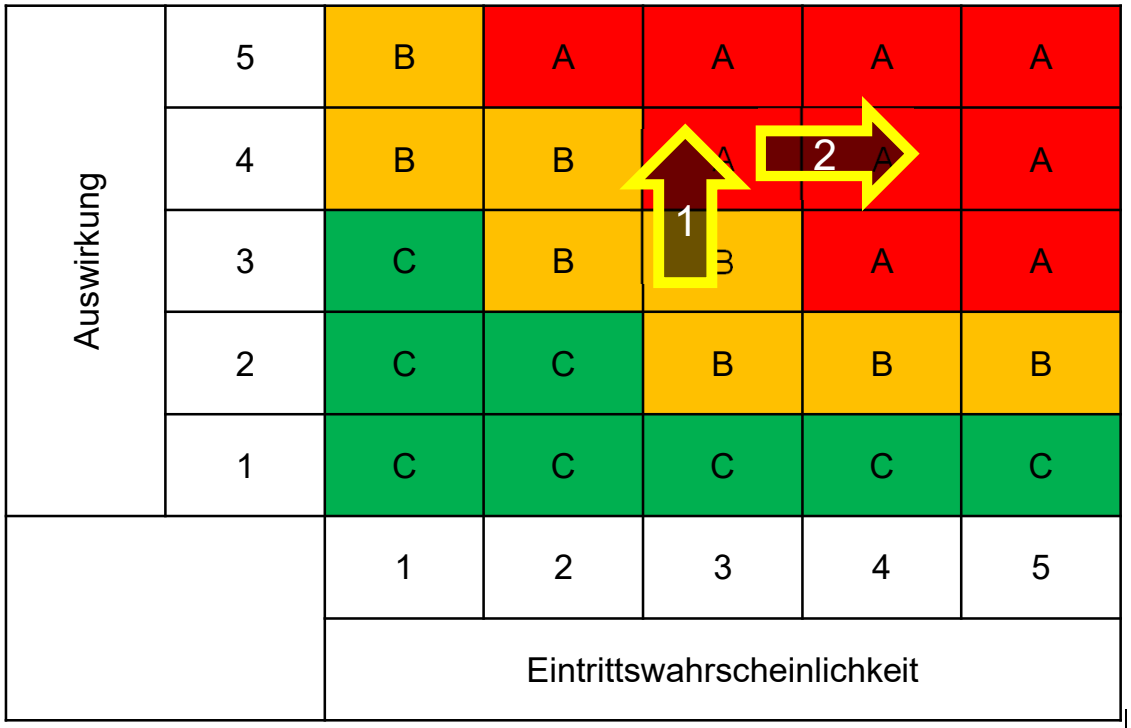
Quelle: The State of Ransomware 2022 (Sophos)

Für die Entschlüsselung der Daten hatte die Hackergruppe BlackCat fünf Millionen Euro von der Landesregierung Kärnten verlangt.

Fallbeispiel:

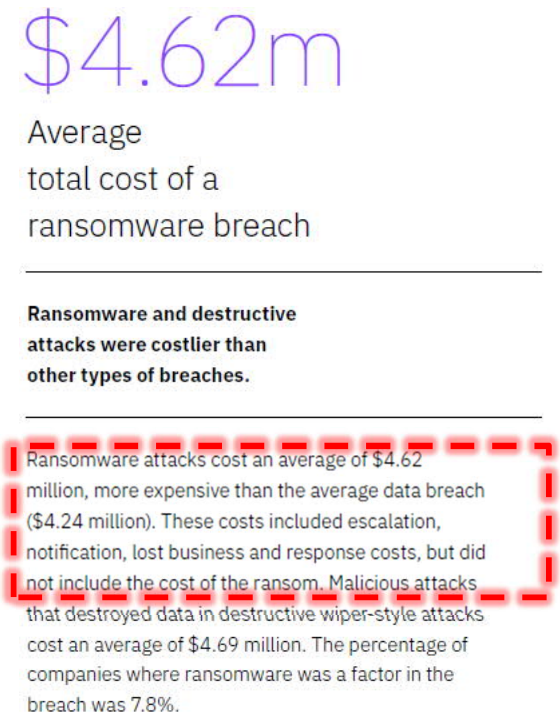
RANSOMWARE-ANGRIFF AUF DIE LANDESREGIERUNG KÄRNTEN

Das Ransomware-Risiko: Was ist passiert?



1. **2021 = Ransomware V2**
2. **2022-Q2: Systematische Angriffe auf Regierungs-organisationen**

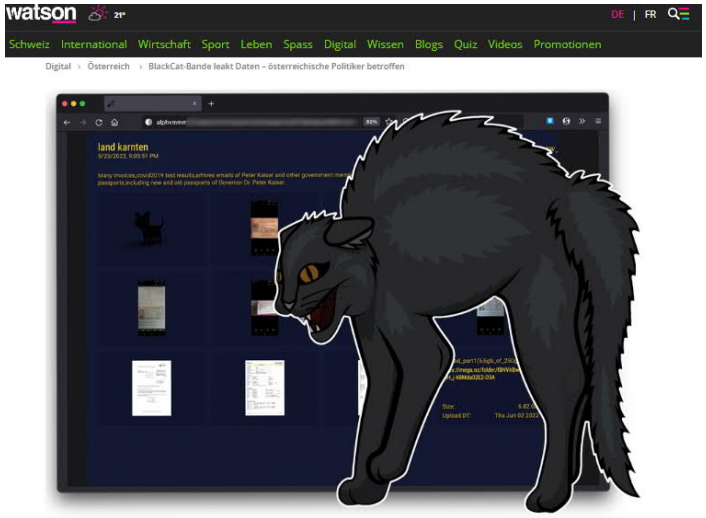
2021 = Ransomware V2



Quelle: Cost of a Data Breach Report 2021 (Ponemon)

- V2 = Double Extortion:
  1. Daten sind <u>verschlüsselt</u>
  2. Daten werden <u>auf Darknet verkauft</u>
- RaaS = Ransomware as a Service:
  - Professionelle kriminelle Organisationen
  - Ausgereifte Plattformen, z.B. Lockbit.

2022-Q2: Systematische Angriffe auf Regierungsorganisationen



Auf der Leak-Site der Ransomware-Bande ALPHA alias «BlackCat» sind Passkopien und andere gestohlene Dokumente zugänglich gemacht worden. *Bild: watson / tolos*

Erpresser-Bande «BlackCat» macht Drohung wahr und leakt (erste) Daten

- "State-Backed Hacker Believed to Be Behind Follina Attacks on EU and US"

- Wir müssen davon ausgehen, dass sämtliche Regierungsorganisationen in Europa hochfrequentierte Ziele von systematischen Cyber-Angriffen sind.
- **Damit sich der Fall Kärnten (5 Mio Euro) im Kanton Luzern nicht wiederholt, müssen wir konsequent handeln!**

Zwar kein Happy End im Fall Kärnten, aber:

Kein Lösegeld für BlackCat

Die Hackergruppe BlackCat hatte sich zu der Cyberattacke auf die Landesregierung Kärnten bekannt, bei der sie nach eigenen Angaben Daten gestohlen und verschlüsselt habe.

Die Hacker forderten fünf Millionen Euro in Bitcoin. Erst dann würde die österreichische Landesregierung eine Software zur Entschlüsselung der Daten bekommen.

ORF hatte Ende Mai berichtet, das Land Kärnten wolle kein Lösegeld bezahlen, da es zum einen keine Beweise dafür gebe, dass tatsächlich Daten gestohlen wurden, und zum anderen, weil sämtliche Daten mit Backups gesichert wurden. Seitdem seien von insgesamt 137 betroffenen Dienstleistungen 116 wiederhergestellt worden und Kaiser wiederholte: Den Hackern werde kein Lösegeld gezahlt.

Fallbeispiel:

RANSOMWARE-ANGRIFF AUF DEN ENERGIEVERSORGER COLONIAL PIPELINE

Hackerangriff auf eine Treibstoffpipeline trifft einen wunden Punkt der US-Energie-Infrastruktur

Was ist passiert?

One Stolen Password Took Down The Colonial Pipeline — Is Your Business Next?

Forbes

David Endler Forbes Councils
Forbes Technology Council C

Sep 14, 2021, 07:15am EDT

If you didn't think password security was important before, there's no way to turn a blind eye to recent events. The head of Colonial Pipeline told Congress that cybercriminals were able to launch a ransomware attack on his company — effectively shutting down half of the country's fuel supply chain — by stealing one password.

According to Mandiant (which worked with Colonial Pipeline post-breach), the VPN login belonged to an employee believed to be inactive. The firm noted that the employee "may have used" the password on a different website that was previously compromised, costing the company $2 million in ransom alone and setting off one of the biggest supply chain crises in recent history.

Analyse

Much of the information coming out of the hearing was previously known due to a separate Senate hearing Tuesday and press conference Monday that together contained several major revelations, including the announcement that the $4.4 million ransom Colonial paid to ransomware gang DarkSide was partially recovered thanks to an FBI operation. However, a few insights from the hearing added new context to the high-profile attack.

Charles Carmakal, senior vice president and CTO at Mandiant, discusses last month's ransomware attack at Tuesday's House Committee on Homeland Security hearing.

Carmakal said near the beginning of the hearing that the VPN login, which remains the earliest known compromise in the attack, was an employee login that wasn't believed to still be active. He added that the employee "may have used" the password on another website that was compromised prior.

After Thompson asked for clarification, Carmakal said the password "had been used on a different website at some point in time" and was a "relatively complex password in terms of length, special characters and case set." It is not currently known how the VPN username was obtained.

Carmakal added that the credentials have been removed and multi-factor authentication has been implemented as part of the recovery. Mandiant was called in May 7 (the day of the attack) to investigate and respond to the Colonial Pipeline attack.

Human Element (85%)

(Nachträgliche) Schutzmass-nahmen

«The Aftermath» von CP: Auch kein Happy End

THOMSON REUTERS

Following the crypto breadcrumbs

On June 7, the DOJ recovered some $2.3 million in cryptocurrency ransom paid by Colonial Pipeline, cracking down on hackers who had launched the most disruptive U.S. cyberattack on record. On May 19, Colonial Pipeline's CEO acknowledged to the media that his company had paid a $4.4 million ransom to hackers as executives were unsure how badly its systems were breached or how long it would take to restore the pipeline.

The Justice Department's seizure of ransom paid by Colonial Pipeline to hackers shows that cryptocurrency may not be that untraceable after all

The recent seizure by the U.S. Department of Justice (DOJ) of millions of dollars-worth of cryptocurrency linked to the ransomware attack on the Colonial Pipeline Co. and its subsequent ransom payment in May demonstrated the inherent traceability of cryptocurrencies and the potential for recent law enforcement successes to push criminals to alter their money laundering tactics, experts said.

LUZERN

KANTON LUZERN

AUSBLICK: WAS KOMMT ALS NÄCHSTES?

Was kommt als Nächstes?

New ransomware tool corrupts data instead of encrypting

A new variation of Exmatter, a popular exfiltration tool used by ransomware affiliate groups, corrupts system files after stealing them, rather than just encrypting them. This way, attackers can bypass security tools, retaining bargaining power since they have the only copy, and ransomware code flaws can't be used to build decryption tools.

> **Ransomware V3 mit drei neuen Eigenschaften!**

1. **Security Tools (z.B. Antivirus-Programme) werden ausgehebelt**
2. **Ransomware Gangs haben die einzige Kopie → Verhandlungsvorteil!**
3. **Es ist nicht mehr möglich, Entschlüsselungs-Tools zu bauen.**

Quelle: Infosecurity (U.K.)

LUZERN

KANTON LUZERN

FRAGEN & ANTWORTEN

Vielen Dank für Ihre Aufmerksamkeit!

KANTON LUZERN

Finanzdepartement
Dienststelle Informatik
Ruopigenplatz 1
6015 Luzern

Telefon 041 228 56 15
informatik@lu.ch