Cyber Defense Night

UBIT STEIERMARK

IT-Fails & IT-Sicherheit

(Praxisbeispiele und Learnings aus der Realität)

2026-05-05 MP09, Graz

(Martin) Leyrer

martin@leyrer.priv.at

https://martin.leyrer.priv.at

@leyrer@23.social

https://media.ccc.de/search?p=leyrer

- Der Leyrer / Du Leyrer / Dem Leyrer sein …
- „Du Martin“ ist auch OK, Siezen verwirrt mich
- Mitglied im Chaos Computer Club (CCCe.V.)
- 30+ Jahre in der IT, 40+ Jahre am Gerät
- Beruflich: Palliative Systemadministration, Senior Lab Services Consultant, T-Shaped Professional
- Sammelt alte Hardware (NeXTCube anyone?)

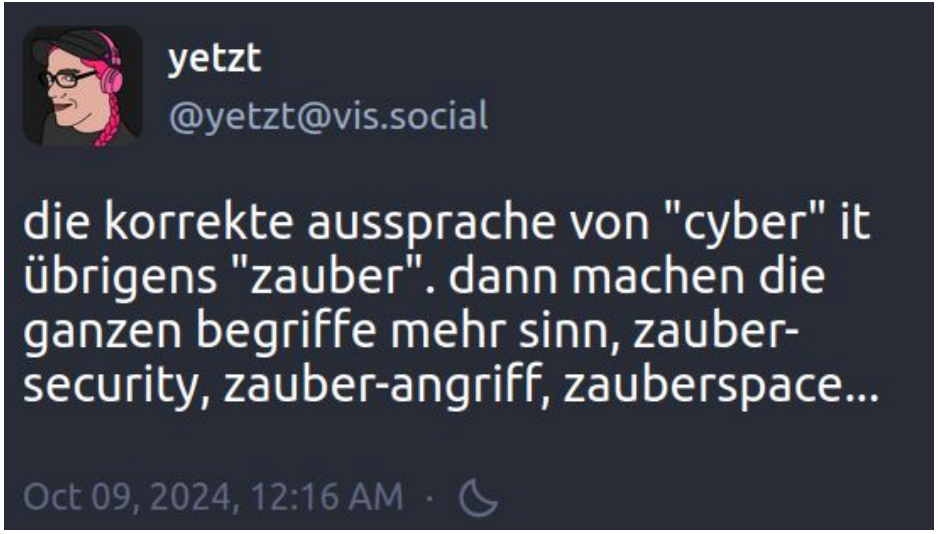

Manner
WIEN
FAIRTRADE
COCOA
ORIGINAL
Neapolitaner

Cyber Defense Night

CYBER Defense Night

CYBER CYBER

https://loet.bar/products/cyberrolle
https://cyber.equipment/



Cybercrime im engeren Sinne

- Straftaten, die an IT-Systemen oder Daten begangen werden
- § 118a StGB - Widerrechtlicher Zugriff auf ein Computersystem
- § 126b StGB - Störung der Funktionsfähigkeit eines Computersystems

https://www.zivilschutz.steiermark.at/thema/cybercrime/

Cybercrime im weiteren Sinn

- „Herkömmliche“ Delikte, die mit Hilfe des Internets begangen wurden
- Zum Bespiel Internetbetrug, Erpressungen im Internet …

https://www.zivilschutz.steiermark.at/thema/cybercrime/

Tatmittel Internet

[Bei der Internetkriminalität] handelt es sich aber weniger um ein eigenes Deliktfeld, sondern um ein Tatmittel, das „durch alle Bereiche des Strafrechts“ reicht.

Betrug, Erpressung oder Drohungen verlagern sich zunehmend ins Digitale, oft ohne direkten Kontakt zwischen Täter und Opfer und häufig über Landesgrenzen hinweg.

— Steir. Landespolizeidirektor Gerald Ortner

https://www.meinbezirk.at/steiermark/c-lokales/polizei-kaempft-mit-steigender-gewalt-und-cyberkriminalitaet_a8563078

Ciderkriminalität

2026-04-30: In den vergangenen Tagen wurden der Polizei bislang zwei Fälle aus der Südsteiermark angezeigt, bei denen Weinbaubetriebe Opfer von Cyberkriminellen wurden.

https://www.polizei.gv.at/stmk/presse/aussendungen/pressedb5f.html?prid=5a7237635a54507862696b3d&pro=4

Cidercrime

- Bei derartigen Angriffen gelangen Täter meist über manipulierte E-Mails, gefälschte Links oder unsichere Downloads auf Computer oder mobile Geräte.
- Anschließend werden persönliche Daten verschlüsselt und für die Freigabe ein Lösegeld gefordert.
- In vielen Fällen kommt es trotz Zahlung zu keiner Wiederherstellung der Daten.

Also eigentlich ...

- Anschließend werden persönliche Daten verschlüsselt und für die Freigabe ein Lösegeld gefordert.
- Es werden alle Daten, im ganzen, erreichbaren Netzwerk verschlüsselt.

Es geht nur um Geld

In vielen Fällen kommt es nach Zahlung zu ~~keine~~r Wiederherstellung der Daten.

Ich schweife kurz ab …

Wenns nicht um Geld geht

- Advanced Persistent Threat - APT „fortgeschrittene, andauernde Bedrohung“
- Ziel: über einen längeren Zeitraum sensible Informationen ausspähen (Industrie- oder Staatsspionage).
- Meist staatliche oder staatsnahe Akteure

APT28 / Fancy Bear — Operation Roundish

- GRU-Einheit 26165
- Roundcube-XSS-/RCE-Ketten gegen öffentlich zugängliche Webmail-Dienste; manipulierte Office-Dokumente ; Phishing mit Man-in-the-Middle-Angriff
- März–April: Über 170 Konten von ukrainischen Staatsanwälten und Strafverfolgungsbeamten gehackt

Zurück zum Cidercrime

Die Polizei empfiehlt

- Installieren Sie eine zuverlässige Antivirensoftware.
- Vermeiden Sie das Herunterladen von Dateien aus unbekannten Quellen.
- Seien Sie vorsichtig beim Öffnen von E-Mail-Anhängen und Links.
- REGELMÄSSIG Updates für OS und Anwendungen installieren
- Sichern Sie Ihre Daten regelmäßig auf externen Speichermedien.
- Verwenden Sie eine Firewall, um den Netzwerkverkehr zu überwachen.
- Achten Sie auf ungewöhnliche Systemaktivitäten.

Empfehlungen 1/4

- Installieren Sie eine zuverlässige Antivirensoftware.
- REGELMÄSSIG Updates für OS und Anwendungen installieren

- Microsoft Defender?
- Kaspersky?
- Laufende Updates sollten 2026 „Standard“ sein?

Empfehlungen 2/4

- Vermeiden Sie das Herunterladen von Dateien aus unbekannten Quellen.
- Seien Sie vorsichtig beim Öffnen von E-Mail-Anhängen und Links.

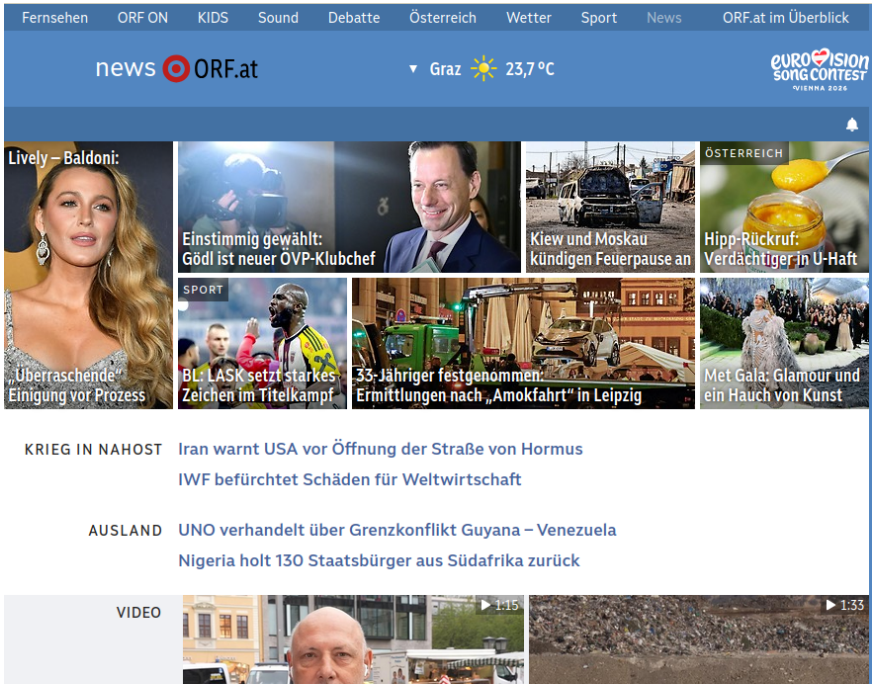
- Victimblaiming
- Microsoft macht Dir das nicht einfach
- Digitale Grundbildung

Ich schweife „kurz“ ab …

Microsoft „Safe“Links

Original URL:

https://www.orf.at/



„Safe“ URL:

https://eur02.safelinks.protection.outlook.com/?url=https%3A%2F%2Forf.at% 2F&data=05%7C02%7C%40orf.at%7C0fbe5e98c2ac40e227b708dc10880558%7C2e9f06b0166945898789 10a06934dc61% 7C1%7C0%7C638403423578665559%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0% 3D%7C3000%7C%7C%7C&sdata=bMPrbif%2B96QoKY5WarbxCTonEn6AGkwj%2FdpB0YEN4go%3D&reserved=0

Seriöslich?

- Seien Sie vorsichtig beim Öffnen von E-Mail-Anhängen und Links.

https://
eur02.safelinks.protection.outlook.com
/?url=https%3A%2F%2Forf.at%
2F&data=05%7C02%7C%40orf.at
%7C0fbe5e98c2ac40e227b708dc10880558%
7C2e9f06b016694589878910a06934dc61%
7C1%7C0%7C638403423578665559%
7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJ
QIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6M
n0% 3D%7C3000%7C%7C%7C&sdata=bMPrbif
%2B96QoKY5WarbxCTonEn6AGkwj
%2FdpB0YEN4go%3D&reserved=0

Erster!

How to stop O365 from clicking on email links?

Question

For years we've noticed that something, we assume O365, is clicking on users' email links before they do. We saw this especially when attempting phishing simulation campaigns and every test user showed as "clicked" before they even had a chance to. We worked around this for years by having another service do URL rewriting that requires device registration but we're moving away from that. I've looked over the O365 Security Policies multiple times, we have Safe Linking and everything else shut off does anyone know where the setting is that's having Microsoft pre-click on links in emails?

EDIT - Thanks everyone! While not exactly what I was hoping for, u/no_regerts_bob helped point out where you can exclude URL domains from being clicked in the Security console under Policies & Rules -> Threat Policies -> Advanced Delivery -> Phishing Simulation.

Email Adresse

vorname.nachname@example.com

abteilung@example.com

Vorsicht?

FROM: e-signature@a-trust.at

Vorsicht!

FROM:

"e-signature@a-trust.at"
<notification-atrust@myt.mu>

Email Adresse

"Beliebiger Text"
<vorname.nachname@example.com>

Zurück zum Thema

Empfehlungen 3/4

- Sichern Sie Ihre Daten regelmäßig auf externen Speichermedien.

Empfehlungen 4/4

- Verwenden Sie eine Firewall, um den Netzwerkverkehr zu überwachen.
- Achten Sie auf ungewöhnliche Systemaktivitäten.


RCE IN INTERNET-FACING SERVICE
Why is it, when something happens, it is always you three?
FORTINET
CITRIX
MS EXCHANGE
imgflip.com

Empfehlungen 4/4

- Verwenden Sie eine Firewall, um den Netzwerkverkehr zu überwachen.
- Achten Sie auf ungewöhnliche Systemaktivitäten.
- Zero Trust
  - Aufwand !!!
- Überwachung
  - Wer? Schichtbetrieb?

Polizei - Fazit

- Sollte der Verdacht bestehen, Opfer eines Cyberangriffs geworden zu sein, wird geraten, das betroffene Gerät sofort vom Internet zu trennen und Anzeige bei der Polizei zu erstatten.
- Die Polizei appelliert an die Bevölkerung, **insbesondere ältere Personen** und Unternehmen **über die Gefahren von Cyberkriminalität zu informieren** und wachsam zu bleiben.

Ich schweife kurz ab …

“Ältere Personen”

- Sir Timothy John Berners-Lee, Erfinder des World Wide Web
  * 8. Juni 1955
- Vinton „Vint“ Gray Cerf, Vater des Internets
  * 23. Juni 1943

Phishing via Signal

Attacke auf Ministerinnen

Ministerinnen und Abgeordnete erhielten Phishing-Nachrichten, hinter denen Russland vermutet wird. Grüne und Linke reagieren unterschiedlich.

26.4.2026 18:07 Uhr

Kommt jetzt das Social-Media-Verbot für Julia Klöckner? Die Bundestagspräsidentin ist von einem Phishing-Angriff betroffen
Foto: dts Nachrichtenagentur/imago

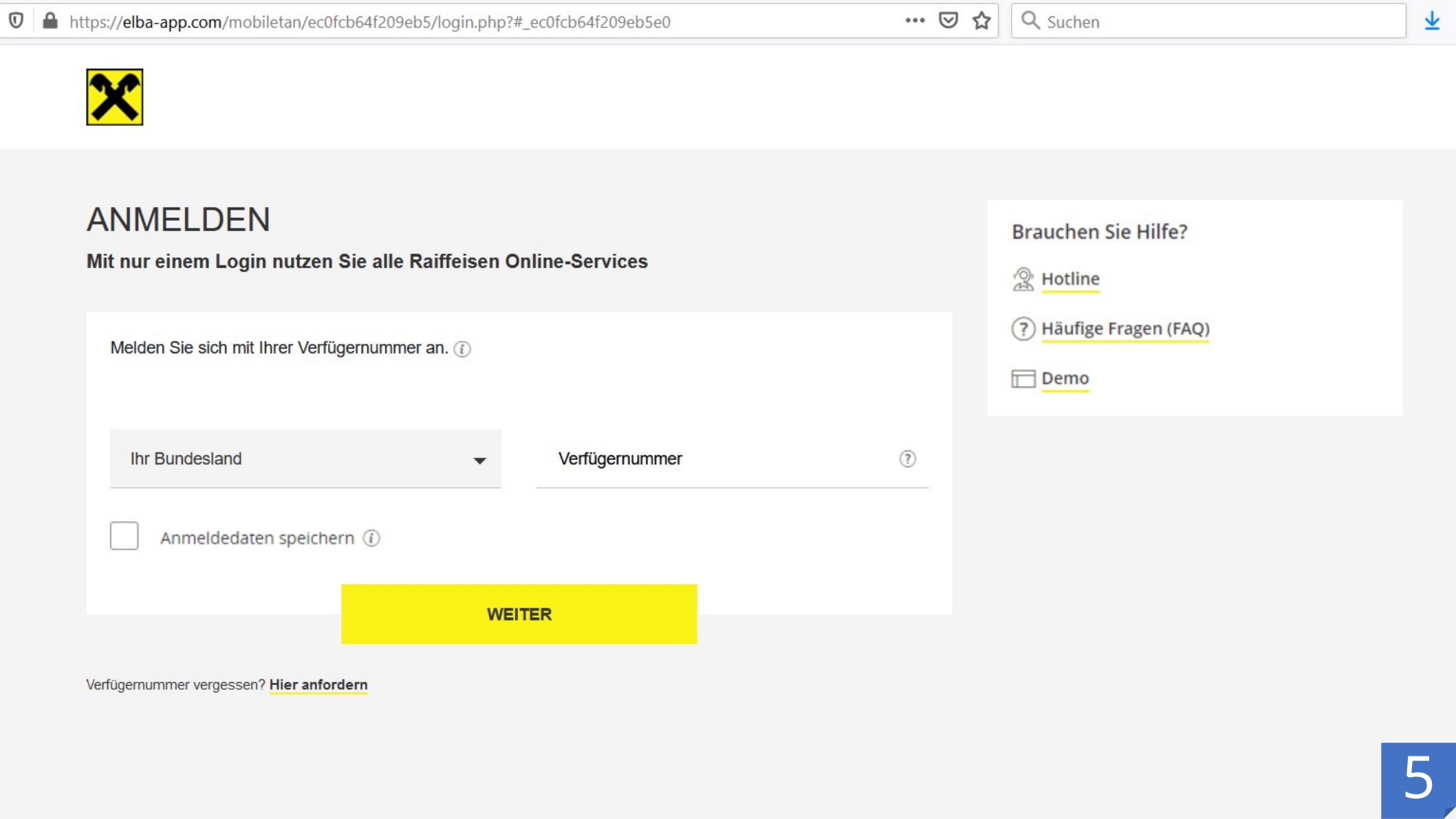
Security expert Troy Hunt hit by phishing attack

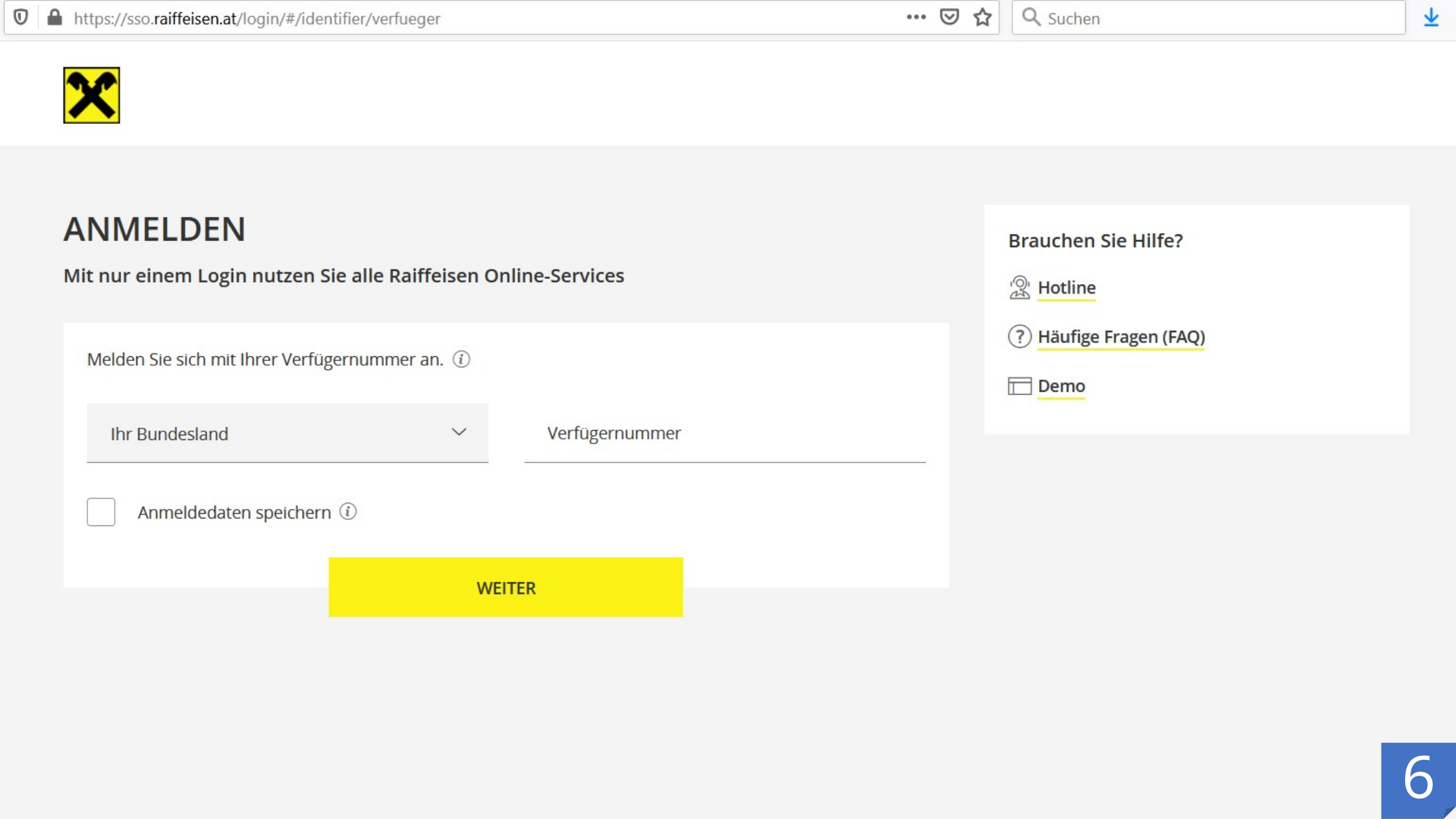
Troy Hunt

Hi, I'm Troy Hunt, I write this blog, create courses for Pluralsight and am a Microsoft Regional Director and MVP who travels the world speaking at events and training technology professionals →

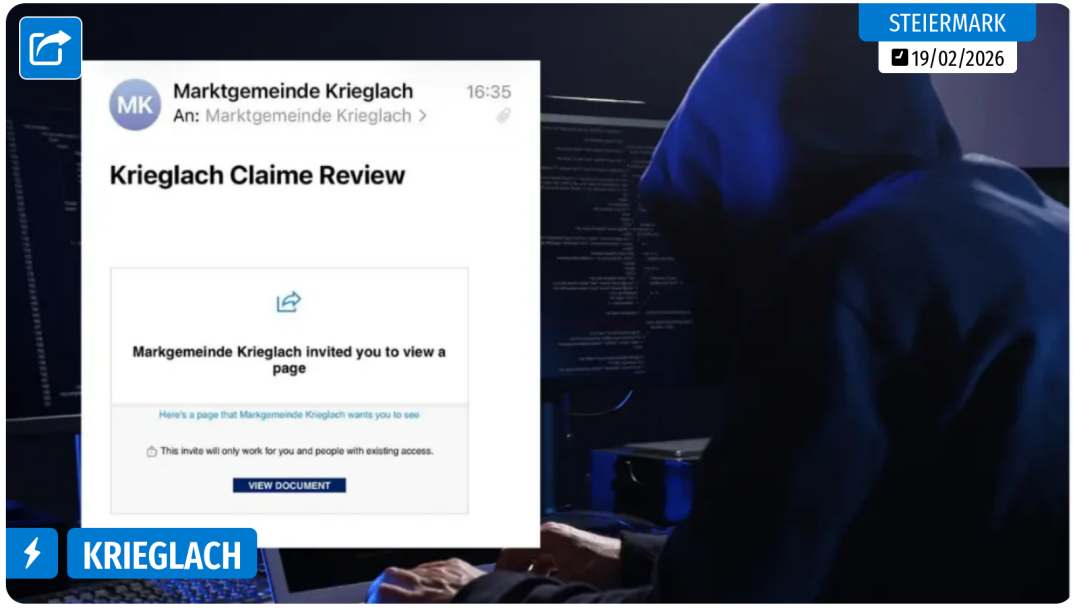
A Sneaky Phish Just Grabbed my Mailchimp Mailing List
https://www.troyhunt.com/a-sneaky-phish-just-grabbed-my-mailchimp-mailing-list/


FAKE
?!


https://elba-app.com/mobiletan/ec0fcb64f209eb5/login.php?#_ec0fcb64f209eb5e0
Suchen
ANMELDEN
Mit nur einem Login nutzen Sie alle Raiffeisen Online-Services
Melden Sie sich mit Ihrer Verfügernummer an.
Ihr Bundesland
Verfügernummer
Anmeldedaten speichern
WEITER
Verfügernummer vergessen? Hier anfordern
Brauchen Sie Hilfe?
Hotline
Häufige Fragen (FAQ)
Demo


https://sso.raiffeisen.at/login/#/identifier/verfueger
Suchen
ANMELDEN
Mit nur einem Login nutzen Sie alle Raiffeisen Online-Services
Melden Sie sich mit Ihrer Verfügernummer an.
Ihr Bundesland
Verfügernummer
Anmeldedaten speichern
WEITER
Brauchen Sie Hilfe?
Hotline
Häufige Fragen (FAQ)
Demo

Veröffentlicht am 19. Februar 2026, 21:14 / ©Montage: Canva & Screenshot Gemeinde Krieglach



In der Gemeinde Krieglach haben Unbekannte am Mittwochabend Zugriff auf das offizielle E-Mail-Konto der Gemeinde erlangt

Cyberangriff: Betrüger schicken Mails im Namen von steirischer Gemeinde

Gefälschte Nachrichten aus dem Gemeindeamt sorgten in Krieglach im Mürztal (Steiermark) für Aufregung. Es handelte sich um einen Hackerangriff.

„Es handelte sich um einen Hackerangriff“

Ein Hacker ist jemand, der versucht einen Weg zu finden, wie man mit einer Kaffeemaschine Toast zubereiten kann.

— CCC Gründer Wau Holand

Phishing

- Über die kompromittierte Adresse wurden Nachrichten an zahlreiche Kontakte verschickt mit der Aufforderung, einen Link zu öffnen, um ein angebliches Dokument abzurufen.
- Die Mails wirkten auf den ersten Blick authentisch, da sie direkt von der echten Gemeindeadresse versendet wurden.

Überwachung?

- Auf den Vorfall aufmerksam wurde die Gemeinde durch ihre externe IT-Betreuung, die ungewöhnliche Aktivitäten registrierte und sofort Alarm schlug.
- „In enger Abstimmung“ wurden umgehend technische Maßnahmen gesetzt, das betroffene Konto gesperrt und weitere Aussendungen unterbunden.

Bitte gehen sie weiter!

- Parallel informierte die Gemeinde die Bevölkerung über soziale Medien
- Wir dürfen uns höflich entschuldigen, jedoch liegt dieser Hackerangriff nicht in unserer Verantwortung.

Kosten und Verluste

- Zahlreiche Bürgerinnen und Bürger meldeten sich telefonisch im Amt
- Die Verunsicherung war groß
- Laut Bürgermeisterin Regina Schrittwieser wurden keine Daten abgegriffen

Vorsorge der Gemeinde

- Man habe jedoch vorgesorgt:
  - Schulungen für Mitarbeiter
  - Cyber-Versicherung

Lerneffekt

- Sichere Passwörter
- Zwei-Faktor Authentifizierung
- Microsoft schützt vor Hackern nicht
  - `$ dig krieglach.gv.at MX`
    `10 krieglach-gv-at.mail.protection.outlook.com.`

Sichere Passwörter

- Was ist ein GUTES Passwort gemäß Zivilschutz Steiermark?
  - 8-10 Zeichen
  - Groß- und Kleinbuchstaben
  - Sonderzeichen und Ziffern
  - KEIN Bezug zu Namen, Geburtsdaten, Kindern usw.
  - KEINE Muster (12345, qwertz, 123321 usw.)

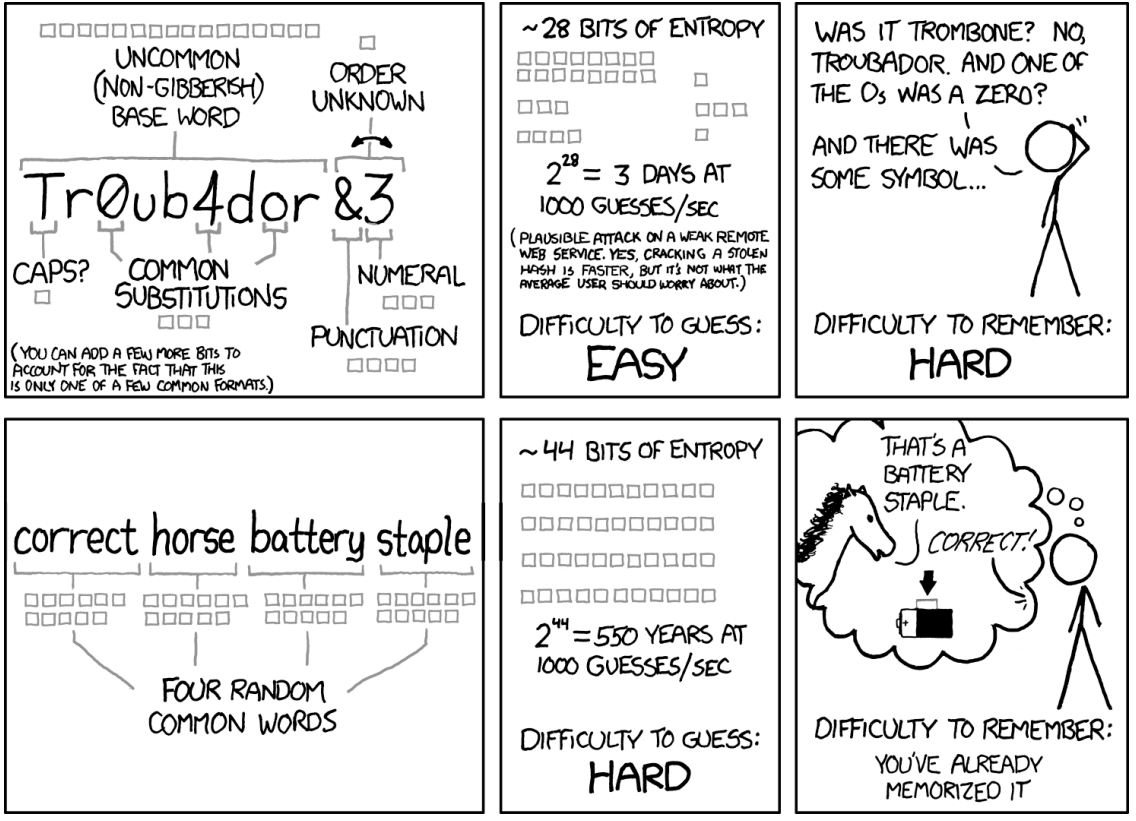
https://www.zivilschutz.steiermark.at/thema/cybercrime/

Sichere Passwörter

- Was ist ein GUTES Passwort gemäß Zivilschutz Steiermark?
  - 8-10 Zeichen
  - Groß- und Kleinbuchstaben
  - Sonderzeichen und Ziffern
  - KEIN Bezug zu Namen, Geburtsdaten, Kindern usw.
  - KEINE Muster (12345, qwertz, 123321 usw.)

https://www.zivilschutz.steiermark.at/thema/cybercrime/

Länge schlägt Komplexität



https://xkcd.com/936/

2-Faktor Authentifizierung

CHRONIK

Hackerangriff legt Feldbacher EDV lahm

Am Wochenende ist die Stadt Feldbach Opfer eines Hackerangriffs geworden: Das EDV-System wurde übernommen; sollte die Stadt ihre Daten wiederhaben wollen, müsse Lösegeld bezahlt werden.

Initiiert wurde der Angriff am Freitag – nach derzeitigem Wissensstand über einen Homeoffice-PC. Am Samstag traten erste Probleme auf, als eine Mitarbeiterin Vorarbeiten für die Präsidentenwahl erledigen wollte; sie alarmierte daraufhin die IT-Verantwortlichen.

Gemeinde ist versichert

Laut dem Feldbacher Bürgermeister Josef Ober wurde auch eine Lösegeldforderung gestellt – nur nach Zahlung würden die Daten wieder freigegeben. Da die Stadt versichert ist, sei ihr nun ein Expertenteam aus Deutschland zu Hilfe geschickt worden, so Ober: „Es ist eine Forderung da, die Versicherung ist informiert."

„Hackerangriff“

- Am Wochenende ist die Stadt Feldbach Opfer eines Hackerangriffs geworden
- Das EDV-System wurde übernommen; sollte die Stadt ihre Daten wiederhaben wollen, müsse Lösegeld bezahlt werden.

Ihre Sorgen möchten wir haben

- Da die Stadt versichert ist, sei ihr nun ein Expertenteam aus Deutschland zu Hilfe geschickt worden
- Finanzieller Schaden würde der Stadt nicht entstehen, denn die Systeme seien auf dem modernsten Stand, und man sei ja versichert

Könnt Ihr noch „Analog“?

- Zurzeit werde analog gearbeitet – also via Telefon, Post und persönlichem Kontakt.

Alles neu - auch das kostet

- Die Stadtgemeinde will das Lösegeld nicht bezahlen, die Systeme werden komplett neu aufgesetzt
- 5. September: die IT-Systeme werden bis 12. September komplett heruntergefahren.

Vorbereitet

- Viel Geld in eine "äußerst fundierte EDV-Lösung" investiert
  - samt umfangreichem Virenschutz
  - und Datensicherung mit Back-ups.
- Versicherung gegen Hackerangriffe
- Ein simulierter Angriff im April 2022 habe keine Mängel zutage gebracht
  - Hat im September 2022 nicht geholfen

Überwachung?

- Die Cyberattacke dürfte auf den Freitag, 2. September zurückgehen.
- Jedenfalls seien einer Mitarbeiterin am Samstag, 3. September "erste Probleme" aufgefallen.
- Am Montag sei es dann klar gewesen, dass ein Verschlüsselungstrojaner eingesetzt worden war

https://www.derstandard.at/story/2000138860690/steirische-bezirkshauptstadt-feldbach-von-hackerangriff-betroffen

Schäden? Schäden!

- „Finanzieller Schaden würde der Stadt nicht entstehen, denn die Systeme seien auf dem modernsten Stand, und man sei ja versichert“
- Kostenlos?
  - 1 Woche offline, nur analoges Arbeiten → Daten nachtragen
  - Aufwand für die Wiederherstellung - Neu Aufsetzen aller Systeme; Überstunden, Burn-Out
  - Kommunikationskosten

CHRONIK

Hackerangriff auf Therme Waltersdorf

In der Steiermark haben erneut Computerhacker zugeschlagen. Nachdem vergangene Woche die Stadt Feldbach Ziel einer Attacke geworden war, wurde nun die Therme Bad Waltersdorf zum Opfer.

Wie in Feldbach – mehr dazu in **Hackerangriff legt Feldbacher EDV lahm** (6.9.2022) – schlugen die Hacker auch in der Therme Bad Waltersdorf an einem Wochenende zu: Seit vergangenem Sonntag geht nichts mehr, die eigenen Mitarbeiter sind aus dem System ausgesperrt.

„Es handelt sich um einen gezielten Angriff einer internationalen Gruppe, und das hat eine Tragweite, dass sich mittlerweile sogar das Bundeskriminalamt eingeschaltet hat“, sagt Waltersdorf-Geschäftsführer Gernot Deutsch.

Therme ist offline

Die Hacker fordern Lösegeld, um die Rechner und Daten wieder freizugeben. Die Therme schaltete nun Experten ein, die das genaue Ausmaß des Schadens und Wege zur Lösung ausarbeiten sollen: „Es ist

ORF

„Hackerangriff“

- Die Hacker fordern Lösegeld, um die Rechner und Daten wieder freizugeben.
- Es ist jede Konsumation entweder in bar oder mit Karte zu bezahlen
- Nachdem die Therme offline ist, seien auch keine Buchungen über das Internet möglich.

Trennung Admin und Betrieb?

- Gastronomiebereich: nur bar oder mit Bankomatkarte bezahlen, da das Chipkarten-System ausgefallen ist
- Auch die Zimmerschlüssel funktionieren in der Therme per Chip. „Hier mussten wir wieder auf die herkömmlichen, altmodischen Schlüssel zurückgreifen.“

https://futurezone.at/digital-life/cyberangriff-therme-waltersdorf-steiermark-erpresser-ransomware/402146586

HOPE IS NOT A PLAN

IV: Erkenntnisse und Ableitungen aus Cyber-Attacken auf steirische Industriebetriebe

https://steiermark.iv.at/news/detail/cyberattacken-erfahrungen-der-steirischen-industrie/

Highlights Monitoring & Backup

- Aktives Monitoring über sog. Security Operations Center (SOC) einführen
  - Herausforderung im Einrichten eines SOC: 24/7 verfügbar sein. Dies ist intern personell kaum erreichbar
- Das bei allen befragten Unternehmen wesentlichste technische Element zur Schadensbegrenzung war das Backup-Konzept.
  - Eine vollständige und funktionierende Sicherungskopie wurde von einigen Unternehmen als Rettung vor dem Totalverlust beschrieben
  - während bei anderen das Fehlen einer solchen die Wiederherstellung der Systeme schmerzhaft verzögerte

Highlights Prävention

- Einige betroffene Unternehmen berichten, seit einem Angriff das Rechtesystem mit Domain Administratoren im Active Directory zu überdenken
- Security ist kein isoliertes Thema der IT-Abteilung.
- Jeder[1] ist Security.

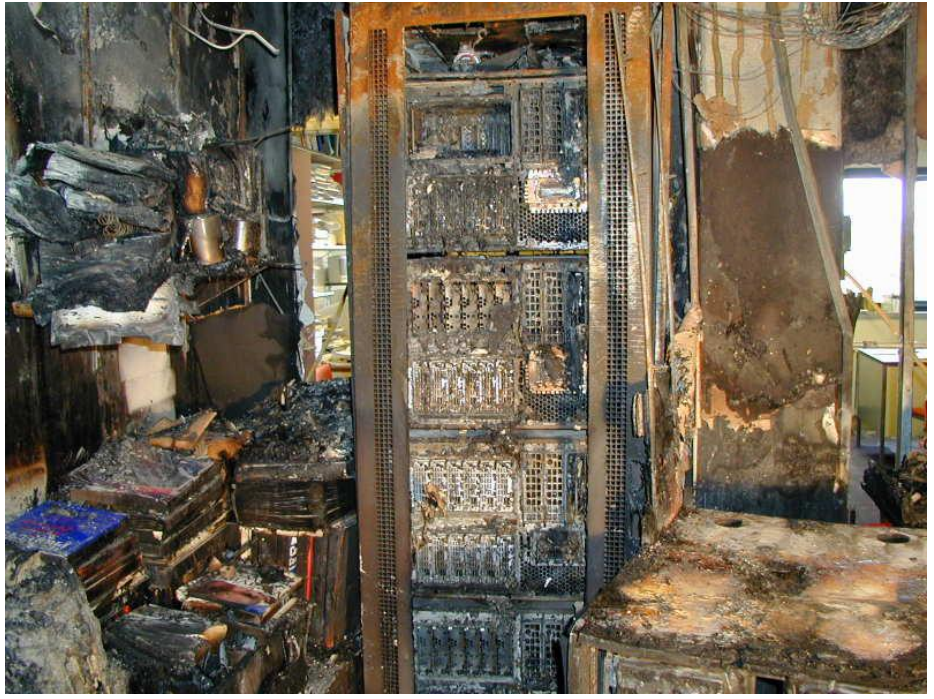
[1] … das mit dem Gendering übt die IV noch

Highlights – Die Überraschung

- Betroffene Unternehmen berichten auch, dass die extreme Arbeitslast über mehrere Wochen oft schleichende mentale Effekte auf die IT-Belegschaft hat
- Nach Abschluss der Initialtriage ist auf entsprechende Pausen und Rasttage zu achten
- insbesondere auch auf Führungsniveau

Wie kann es besser werden?

Backup und Restore



Branko
@brankopetric00

A backup isn't a backup until you have successfully restored from it. Until then, it is just a very expensive file upload called 'Schrödinger's Data'.

Cloud?

IT-Security

- “Sicherheit” ist mehr als Firewalls, installierte Sicherheitssoftware und Passwort-Regeln
- „Sicherheit ist ein Prozess“
- Awareness
- Backups, Backups, Backups !!! (und Restore!)
- Planspiele und Wiederanlauftests

Förderungen!

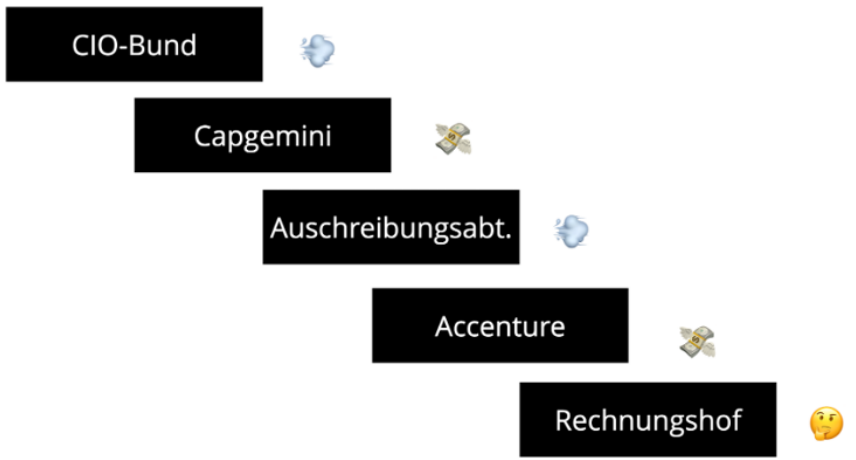
- Die Steirische Wirtschaftsförderung SFG fördert – mit Unterstützung der Wirtschaftskammer Steiermark – Cyber!Sicher Klein- und Mittelunternehmen bei Investitionen in ihre IT-Sicherheit.
- https://www.sfg.at/f/cyber-aber-sicher/

Journalismus ++

- Mehr & bessere IT/Sec Kompetenzen auch in den Lokalredaktionen
- Konsequentes Hinterfragen von Ausreden wie “Hackerangriffen” und DDoS Attacken

Inhousing statt Beratertreppe

- Inhouse-Kompetenzen aufbauen und dann auch einbinden
- Eigenes Personal ist besser als Consultants & Mietkräfte



https://www.heise.de/meinung/Kommentar-GovTech-Campus-ist-fatales-Signal-fuer-Digitalisierung-der-Verwaltung-6740007.html

Fragen ?

- Martin Leyrer
- https://martin.leyrer.priv.at
- leyrer@23.social

Solange man selbst redet, erfährt man nichts.

– Marie Freifrau Ebner von Eschenbach, österreichische Schriftstellerin