Cyber Security Schulung

Soltermann Stefan

Leiter Interkommunale IT Gemeinden Naters und Brig-Glis

Informatiker HF / NDS Betriebswirtschaft / BASc in Management

Zertifizierung: ISO/IEC 27001 (Informationssicherheit)

Inhalt:

- Bedrohungslage und Risiken
- Viren
- Social Engineering / Datamining / Phishing (Fall Oberwallis)
- Datenlecks / Datendiebstahl (Fall Amazon Züri)
- Sichere Passwörter

Passiert immer nur den anderen

KESB-Daten

Heikle Daten bei Hackerangriff gestohlen - Gemeinde Saxon wird Opfer

Die Vormundschaftsbehörde der Gemeinde Saxon ist Opfer eines Cyberangriffs geworden. Laut der Walliser Kantonspolizei wurden dabei Daten der örtlichen KESB gestohlen und verschlüsselt.

Artikel hören

Teilen

Ein Fall von Erpressung?

Die EnBag wird Opfer eines Hackerangriffs – und schweigt

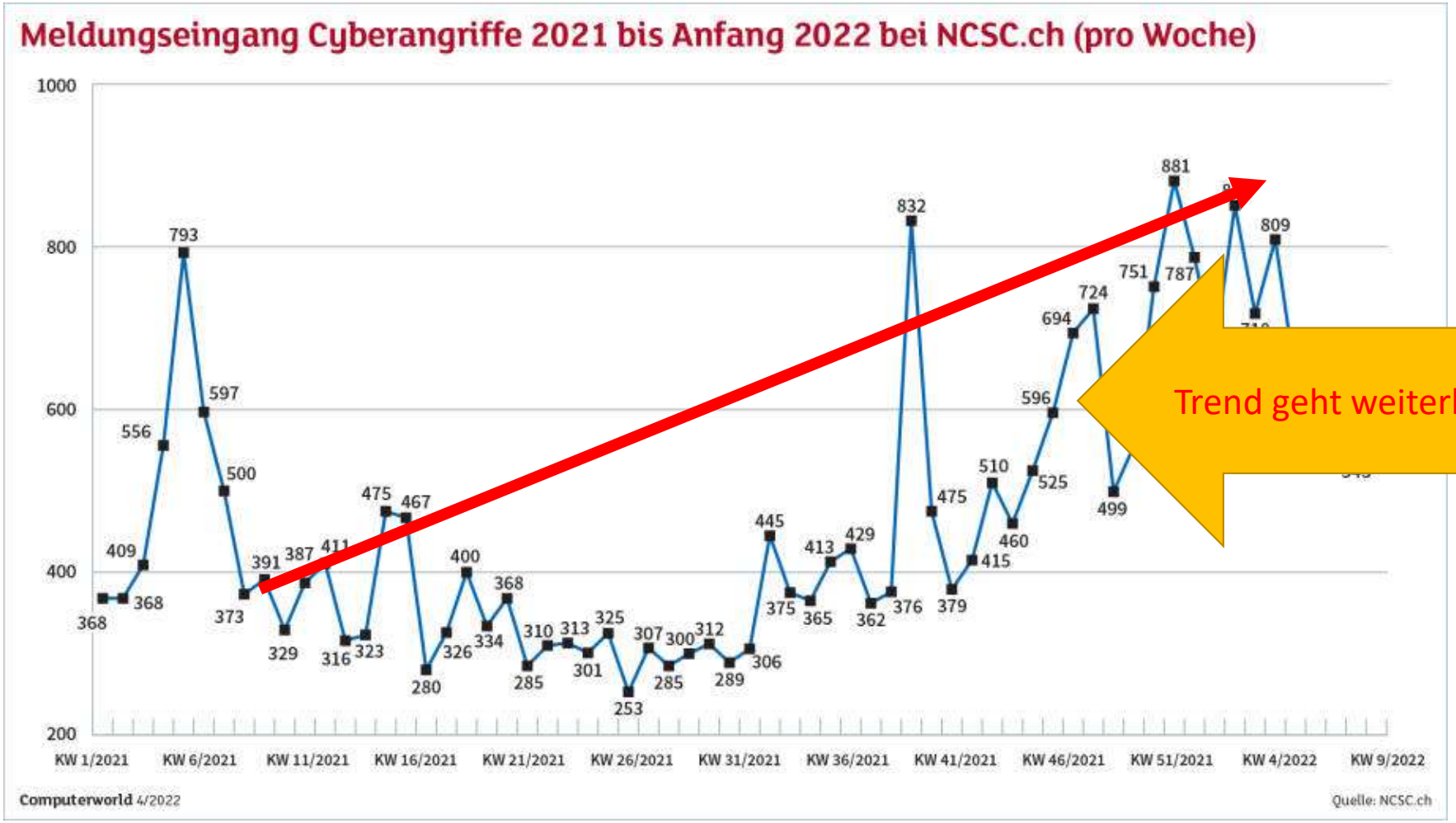
Datenschützer Sébastien Fanti will wissen, ob die grösste Oberwalliser Stromverteilerin ein Lösegeld bezahlt hat.

Fabio Pacozzi

Teilen

Wie erst jetzt bekannt wird, haben Hacker im Sommer 2020 erfolgreich die IT-Systeme der Oberwalliser Energiegesellschaft EnBag attackiert. Der oder die Täter drangen am 26. August 2020 in einen EnBag-Server ein und verschlüsselten tags darauf

Zunahme der Bedrohung:

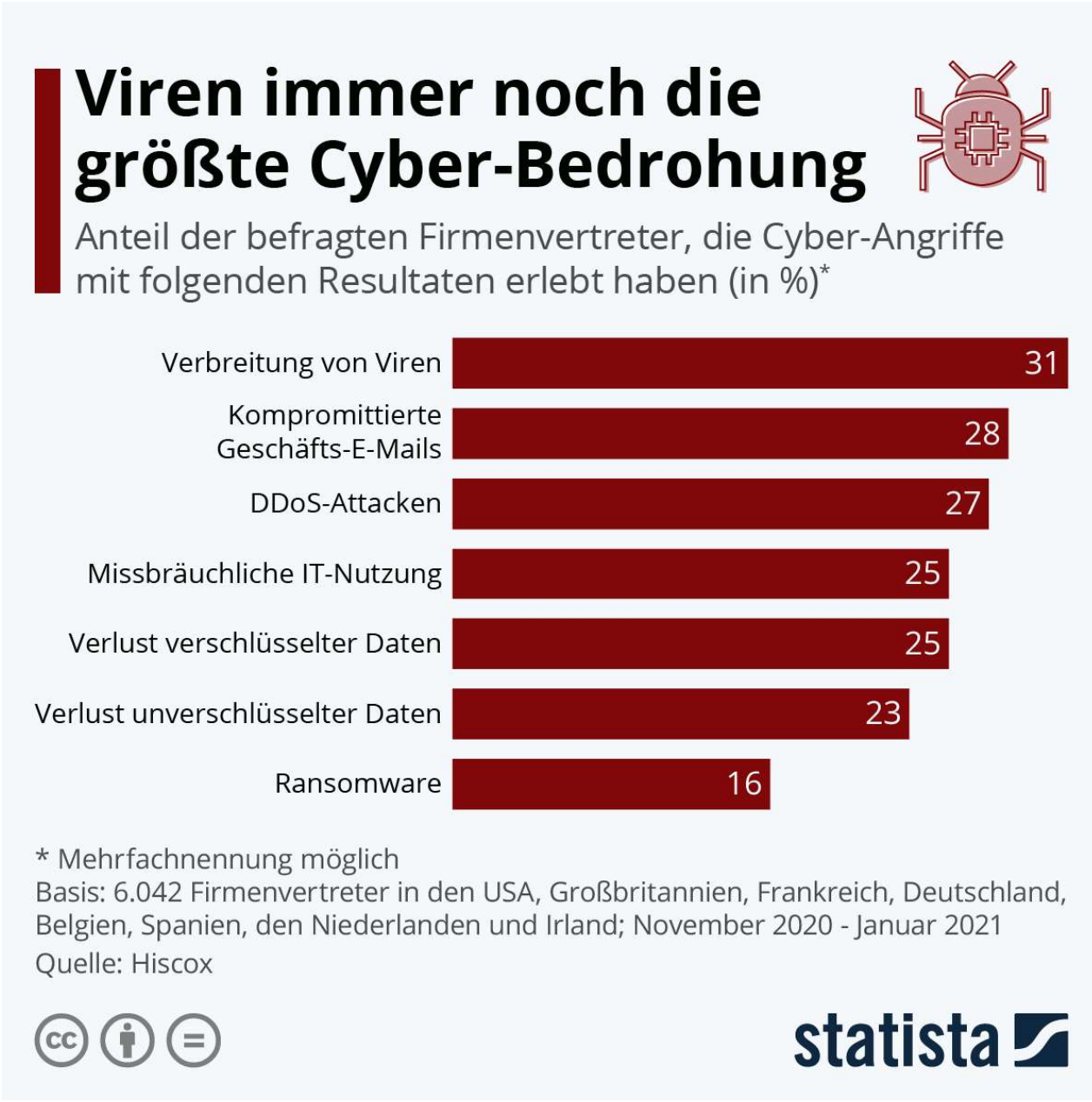


Betriebsrelevant?

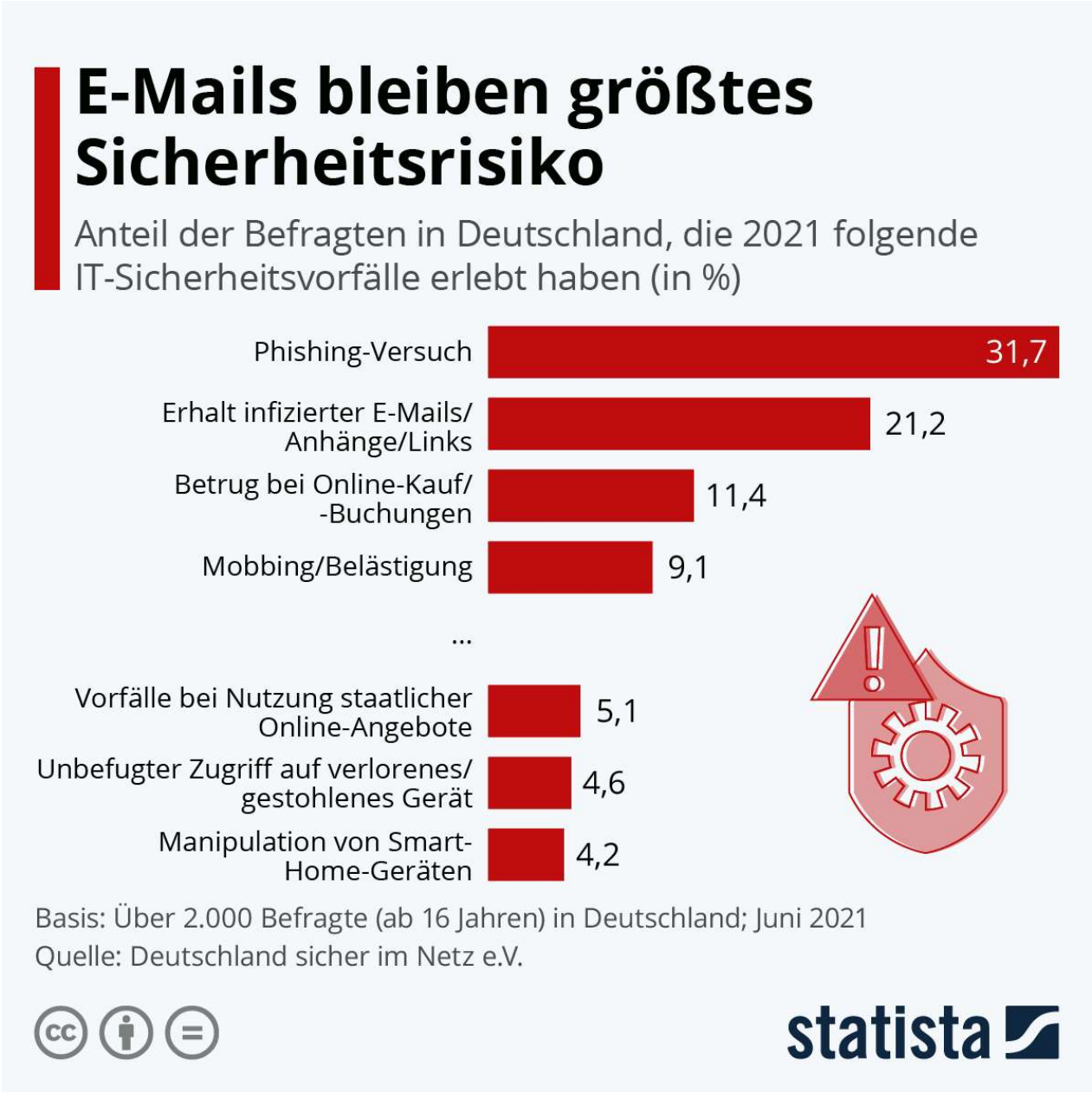
Eine nicht funktionierende IT ist mit hohe Kosten verbunden!

Viren usw.

Viren sind einfach zu programmieren
(Baukasten) und rasch zu verteilen
aber auch recht einfach abzufangen

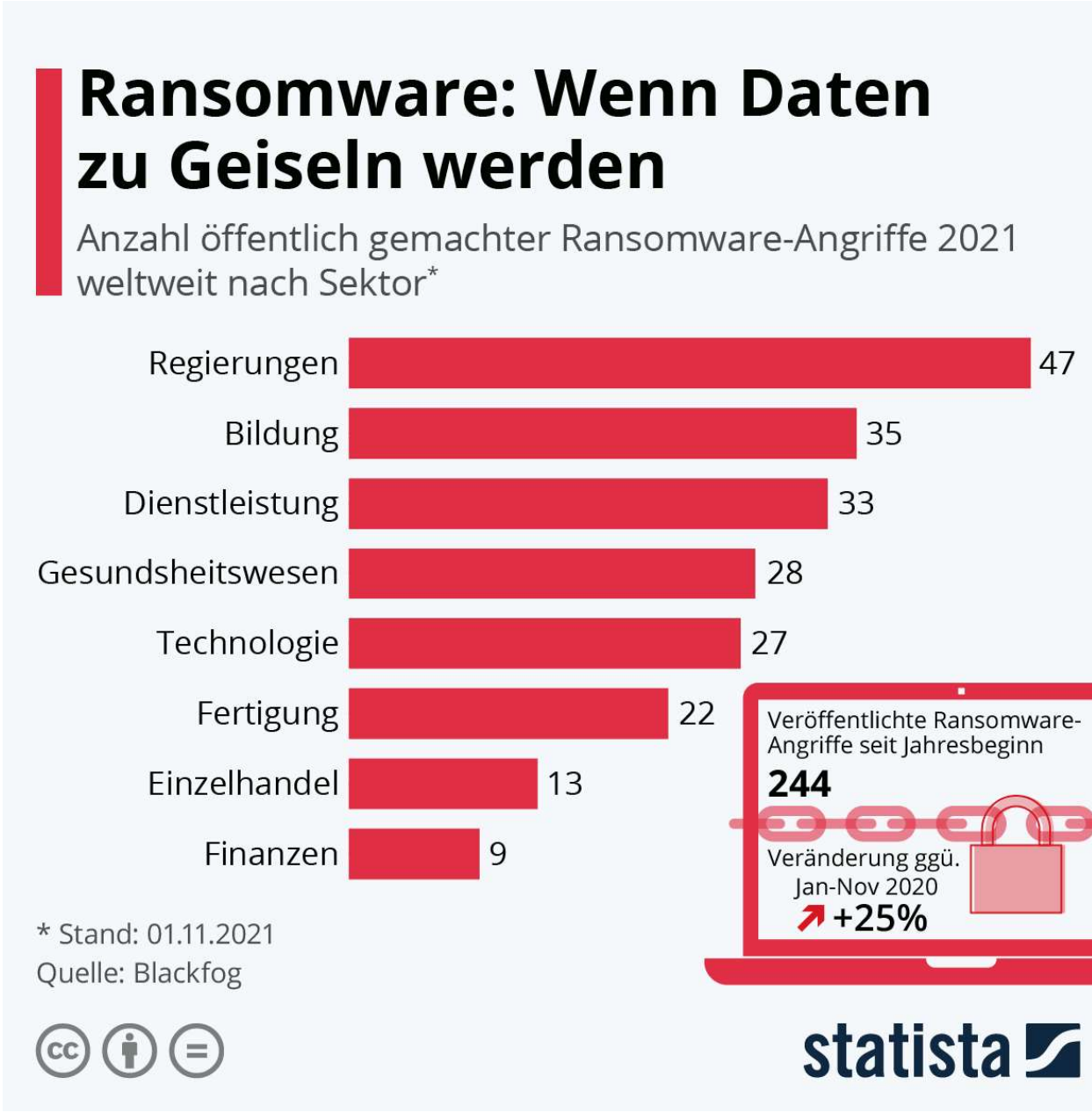


E-Mails:


E-Mails bleiben größtes Sicherheitsrisiko
Anteil der Befragten in Deutschland, die 2021 folgende IT-Sicherheitsvorfälle erlebt haben (in %)
Phishing-Versuch
31,7
Erhalt infizierter E-Mails/ Anhänge/Links
21,2
Betrug bei Online-Kauf/ -Buchungen
11,4
Mobbing/Belästigung
9,1
...
Vorfälle bei Nutzung staatlicher Online-Angebote
5,1
Unbefugter Zugriff auf verlorenes/ gestohlenes Gerät
4,6
Manipulation von Smart-Home-Geräten
4,2
Basis: Über 2.000 Befragte (ab 16 Jahren) in Deutschland; Juni 2021
Quelle: Deutschland sicher im Netz e.V.
statista

Erpressung

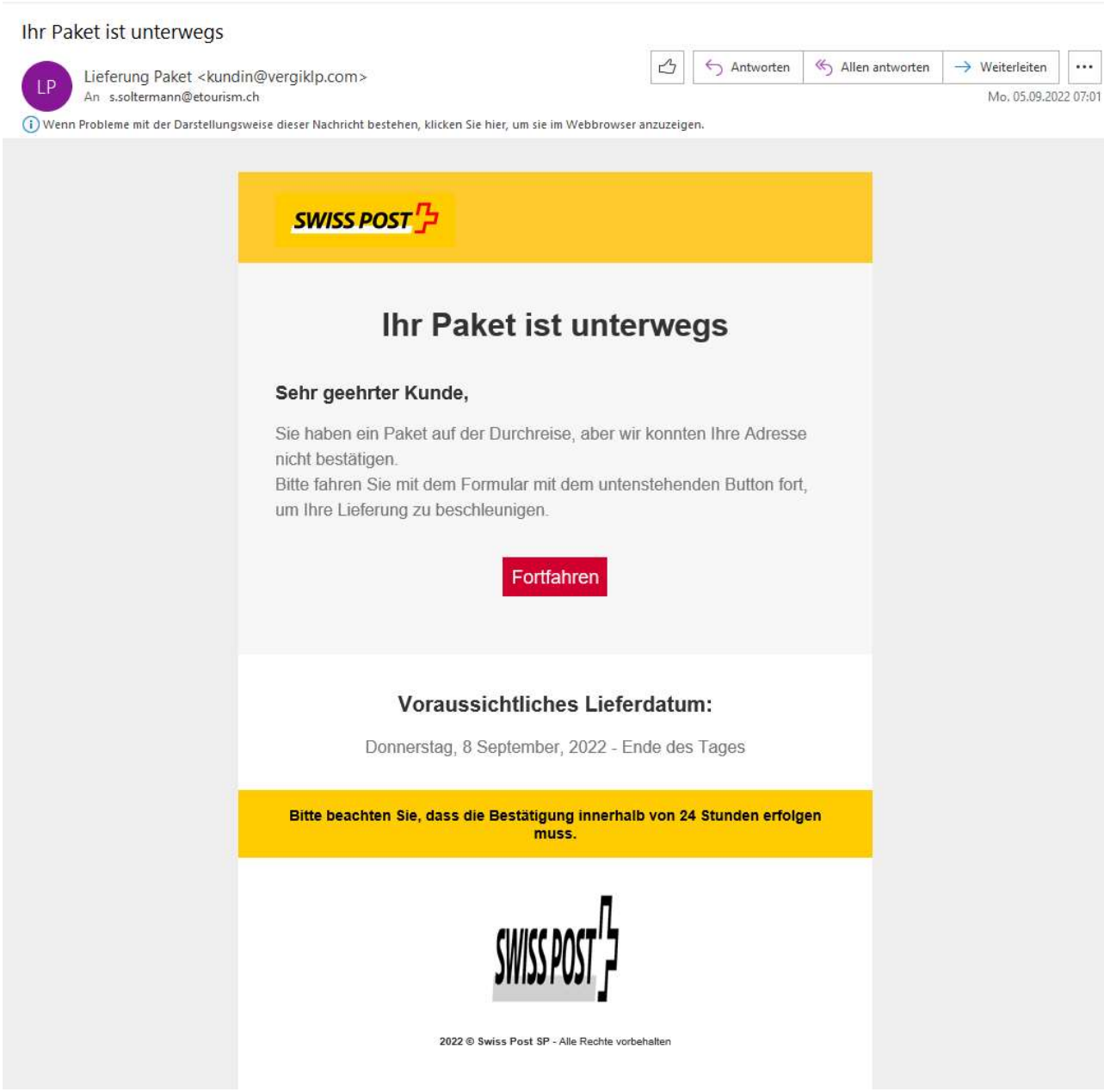
Regierungen und Behörden sind ein attraktives Ziel für Ransomeware



Wie erkennen?

Ransomeware tarnt sich immer besser.
Kopf einschalten und immer zuerst überlegen, bevor man etwas anklickt.

Hier fallen sofort 2 Sachen ins Auge:
Das Logo unten und oben sind nicht gleich und Absender: @vergiklp.com?



Wie erkennen?

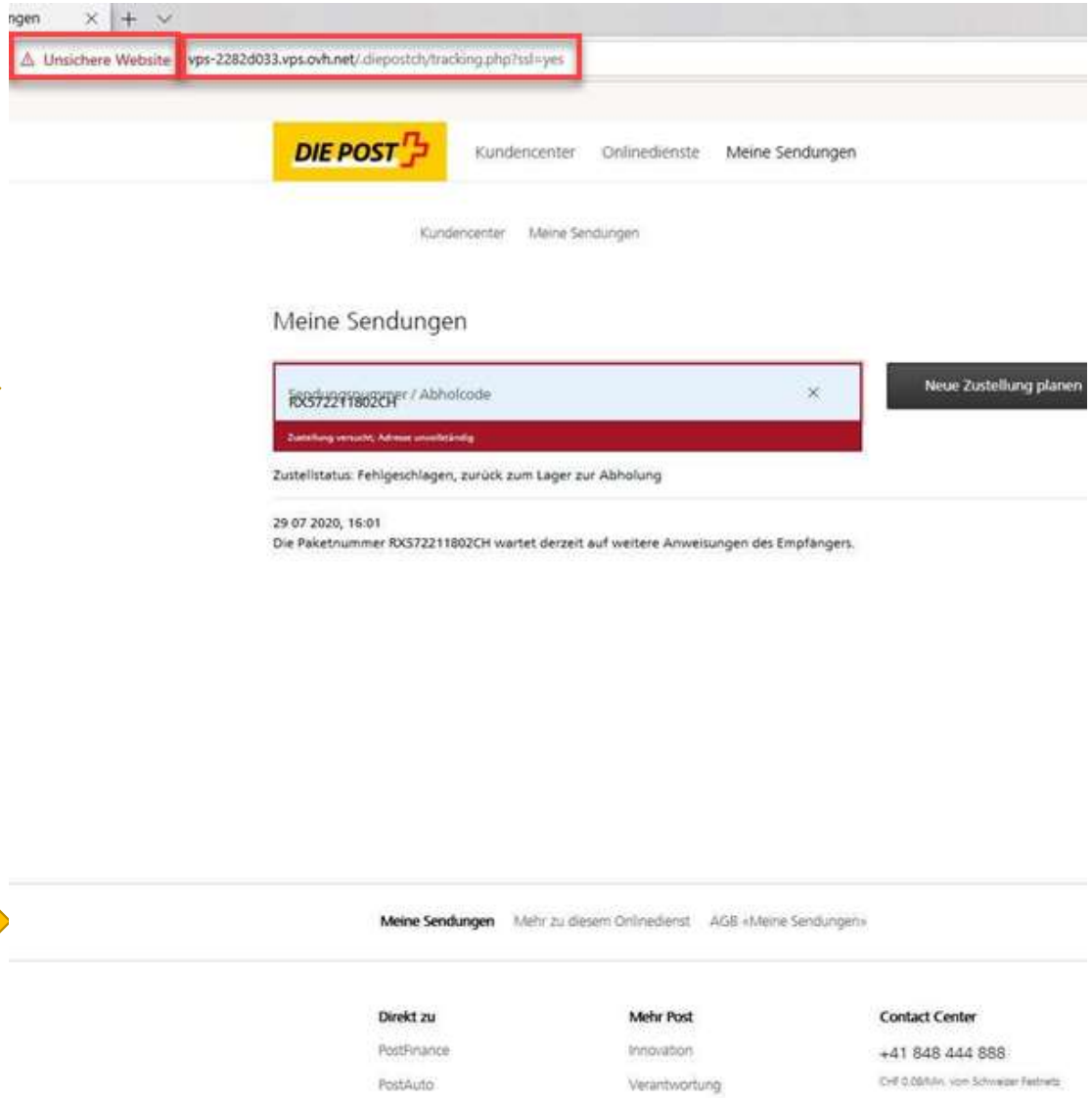
Ransomeware funktioniert immer gleich.
Der Benutzer wird mit Angst und Zeitdruck zu einer Handlung aufgefordert.

Ransomeware funktioniert immer gleich.
Der Benutzer wird mit Angst und Zeitdruck zu einer Handlung aufgefordert.

Was passiert?

Meistens wird man auf eine Webseite geleitet, welche wie in unseren Beispiel gleich der Post aufgebaut ist. Man wird aufgefordert, Daten, Passwörter oder sonstige Informationen abzugeben.

Oft passiert auch gar nichts oder besser gesagt, man merkt nicht dass über den Link versteckt, eine Schadsoftware heruntergeladen und installiert wird. Dazu später mehr.



Aber der Absender war richtig…

Der Absender einer Mail ist so leicht zu fälschen, wie jener auf einem Brief.
Man braucht nur einen Kugelschreiber, im Mail auch nicht viel komplizierter…

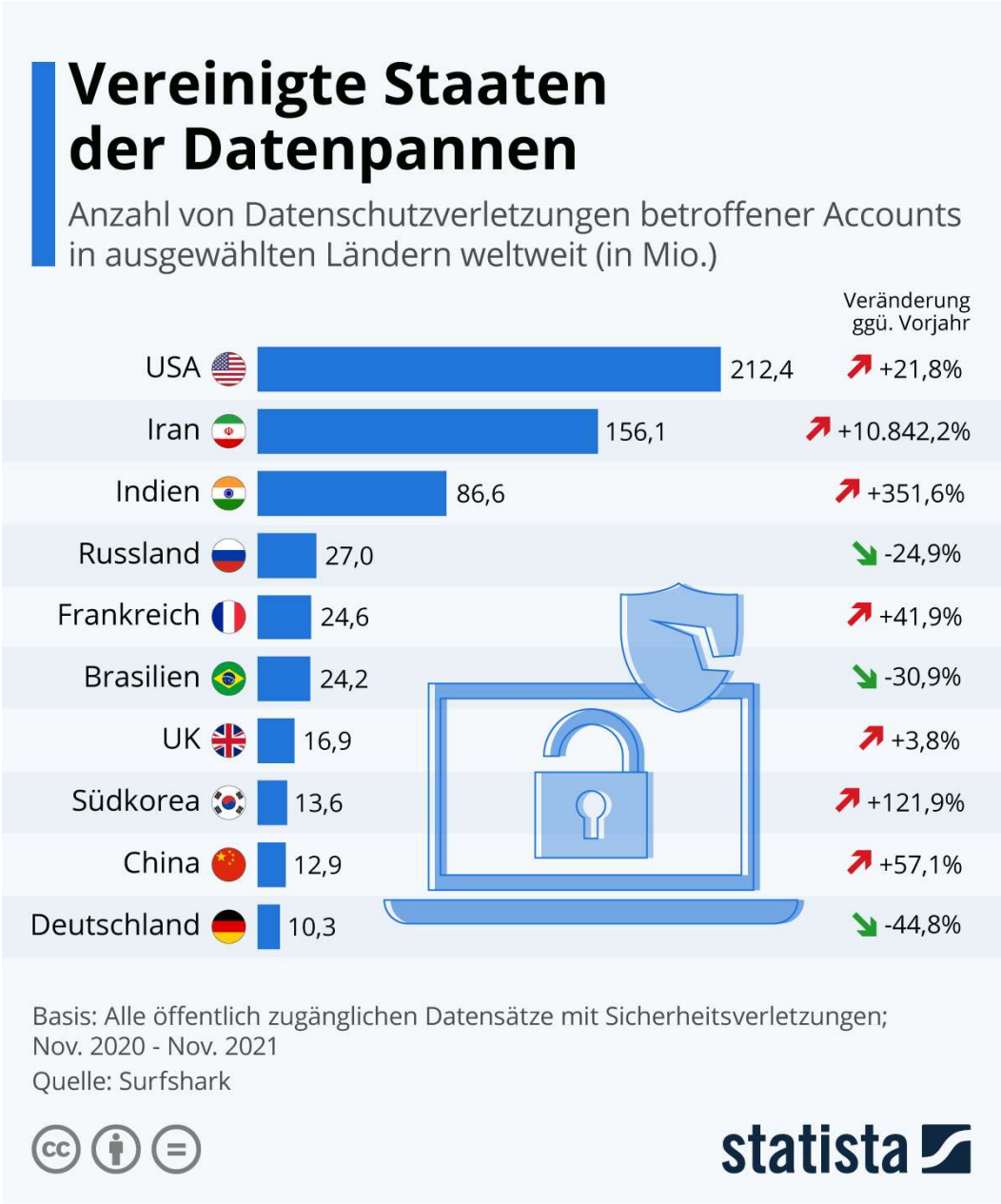
Darwin Award:
Die dümmsten Todesfälle (Wirklich so passiert)
Es war einmal ein Terrorist, der wollte eine Briefbombe verschicken. Nur leider hatte er zu wenig Porto auf den Umschlag geklebt. Der Brief kam zurück – der Terrorist öffnete ihn. Ende der Geschichte.
Fazit: Hätte er nur den Absender gefälscht…

https://www.stern.de/panorama/weltgeschehen/darwin-award--die-duemmsten-arten-zu-sterben-7247784.html

Datenlecks:

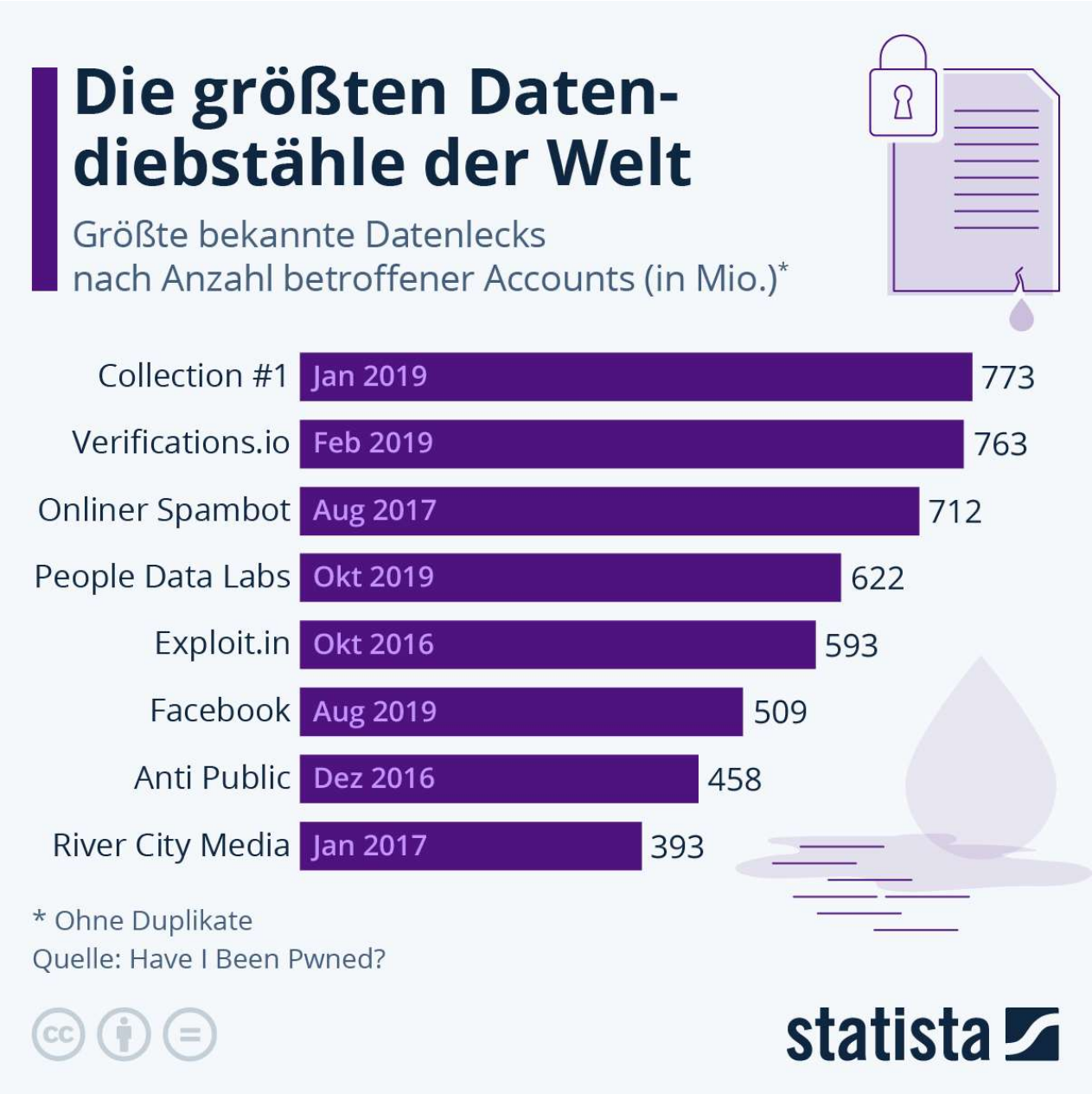
Facebook & Insta, Twitter, WhatsApp, Adobe, Uber, Yahoo sind alle in den USA beheimatet

Achtung: Nicht nur USA ist betroffen…
Swisscom: 0.8 Mio (2020)
Swisspass: 1 Mio (2022)



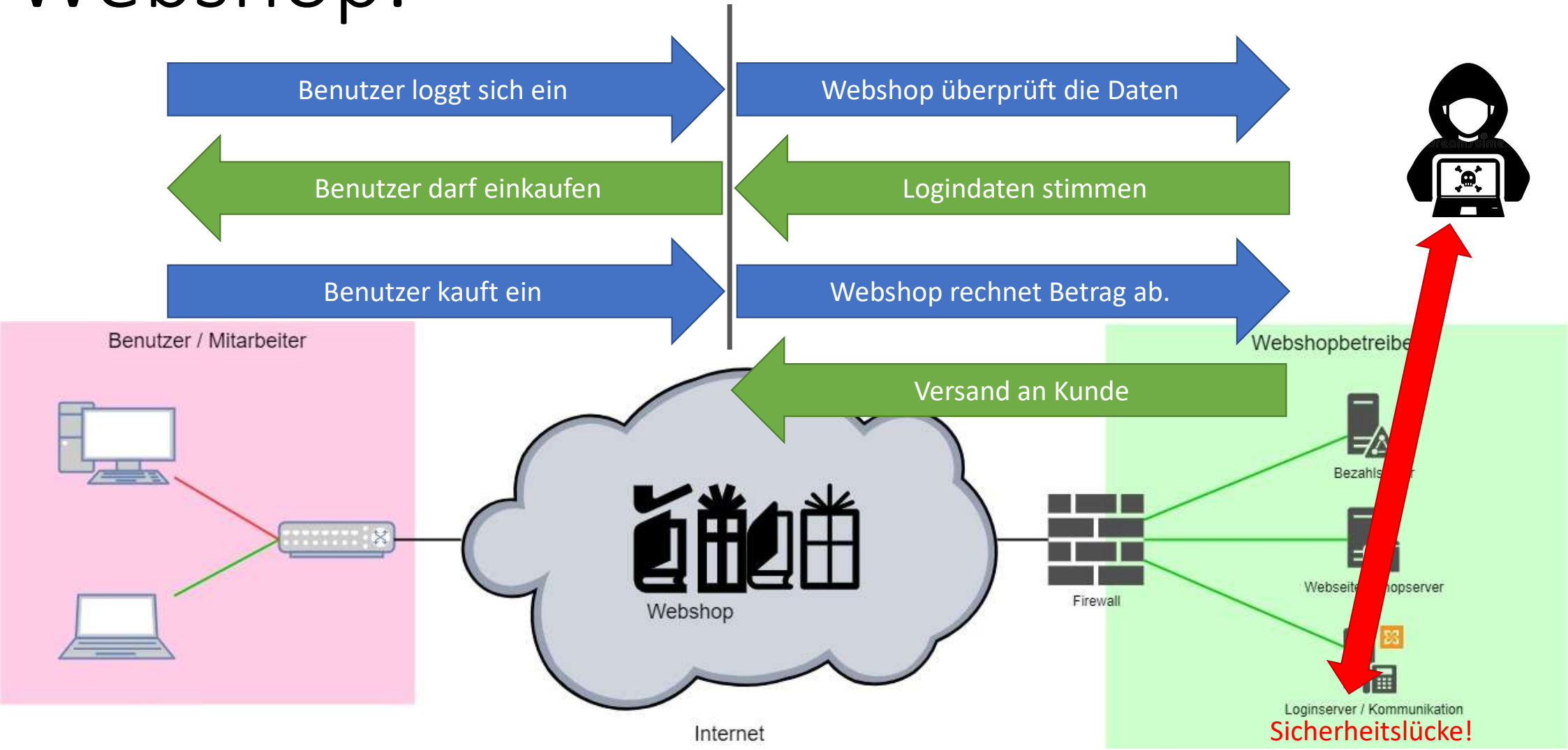
Datendiebstahl:

Seit 2019 wurden über 7 Mia Logins gestohlen!
Tendenz: Steigend

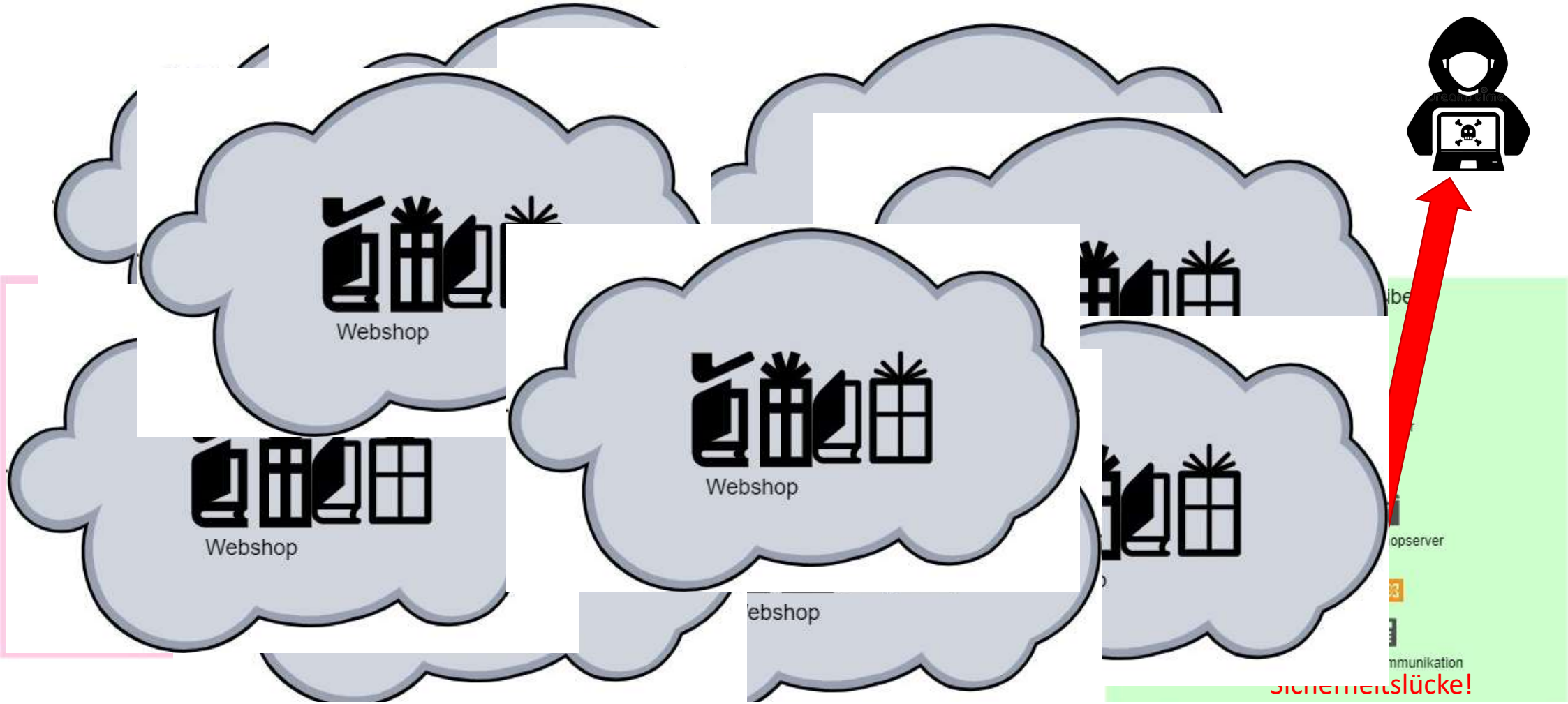


Demo: https://haveibeenpwned.com/

Webshop:


Benutzer loggt sich ein
Webshop überprüft die Daten
Benutzer darf einkaufen
Logindaten stimmen
Benutzer kauft ein
Webshop rechnet Betrag ab.
Versand an Kunde
Benutzer / Mitarbeiter
Webshop
Internet
Firewall
Webshopbetreibe
Bezahls
Webseite
opserver
Loginserver / Kommunikation
Sicherheitslücke!

Gleiche Logindaten überall?/!

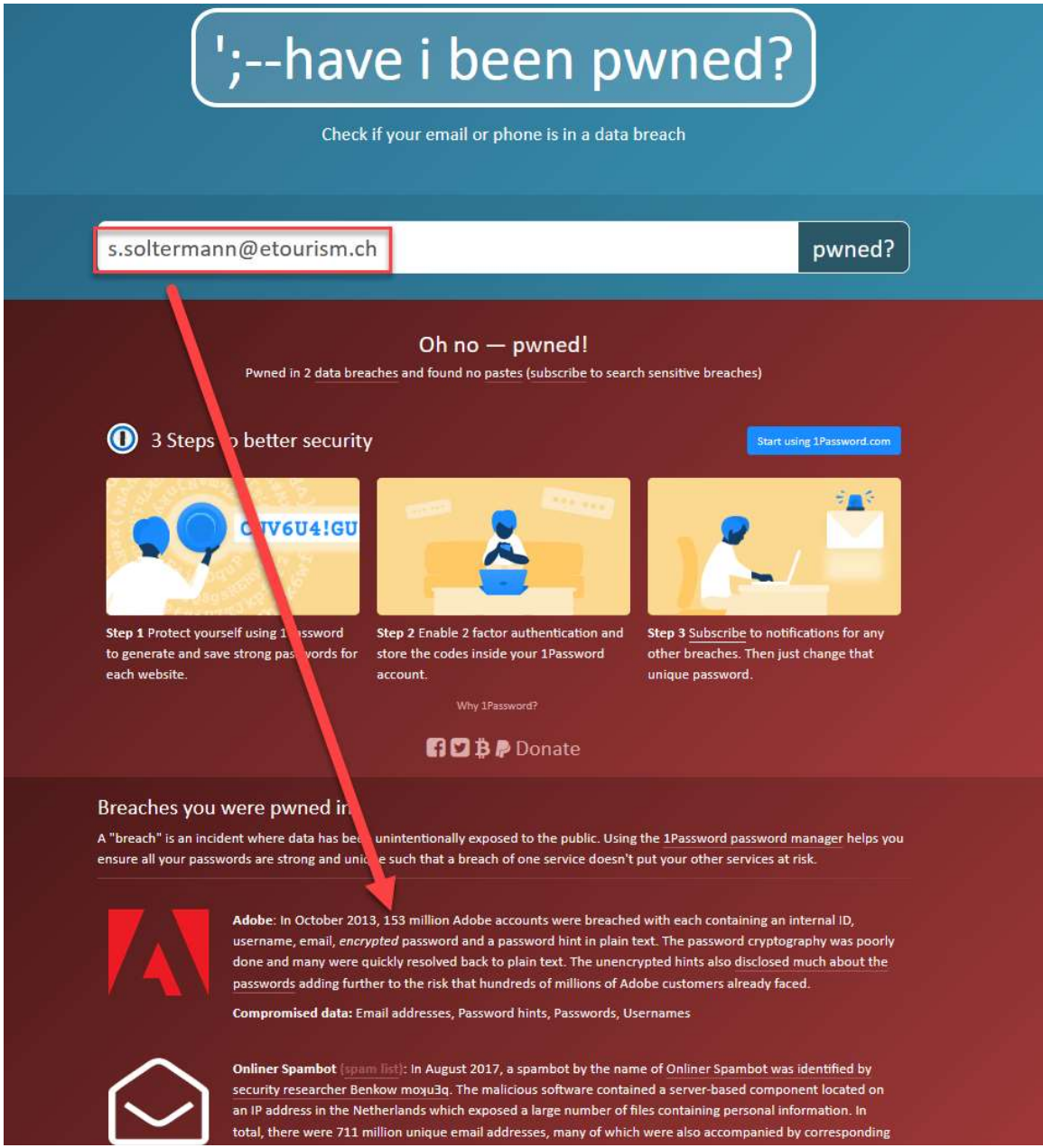


Datendiebstahl:

Adobe hatte 2013 ein Datenleck, wo 153 Mio Daten gestohlen wurde.

Was hilft?
Regelmässiges ändern der Logindaten.
Keine Mehrfachnutzung! **Gleiches Login = Generalschlüssel für den Hacker!**

https://haveibeenpwned.com/



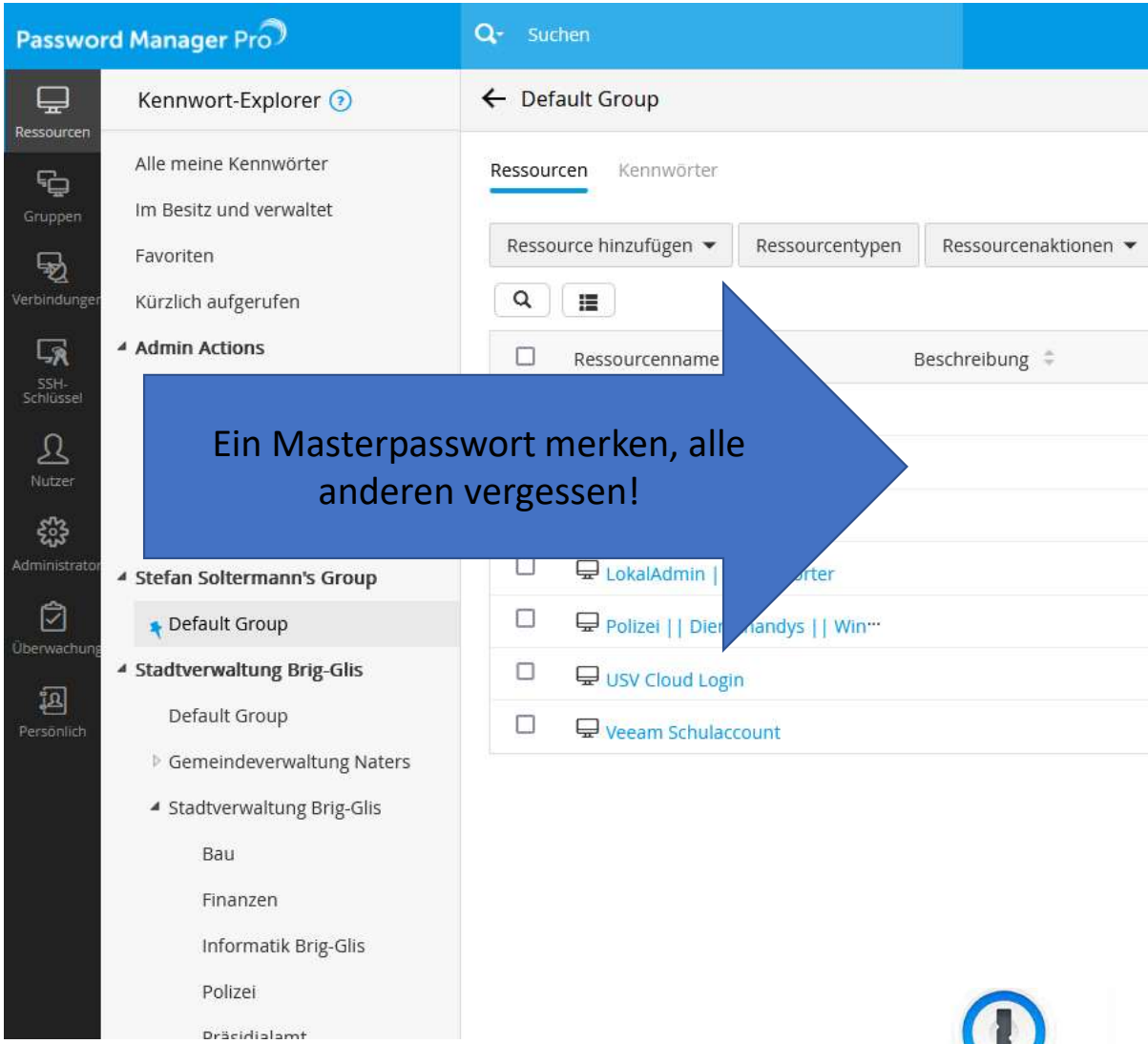
Sichere Passwörter?

Kantonspolizei Zürich

Wie soll ich mir all die Logins merken?

Das kann doch kein Mensch!
Richtig, dafür gibt’s Werkzeuge.

Lösung?
Jeder Mitarbeiter hat einen Password Manager (Brig-Glis-Naters).



Ein Masterpasswort merken, alle anderen vergessen!

Empfehlung (Private):
Über alle Gerätearten nutzbar (Cloudlösung für 5.- pro Monat für 5 Familienmitglieder)

1Password

Ende:

Folien, Links, Schulungen, Fragen usw. bitte über stefan.soltermann@brig-glis.ch

Social Engineering /Data Mining

"Faktor Mensch" als vermeintlich schwächstes Glied

Die Schwindler bauen zum Opfer vertrauen auf. Sie wissen viel mehr über die Opfer, als man selbst denkt denn das Internet ist eine riesige Mine (Data Mining) von persönlichen Daten die man selbst und ohne Not preisgibt und nach denen geschürft wird.

Die Angreifer sammeln solange Daten, bis es reicht damit ein Mensch die Falle stellen kann. Wenn es um das Erschwindeln von Geld geht, sind Menschen hervorragende Lügner und sehr kreativ.

Fall Social Engineering (Anonym)

Ich wurde zu einem meiner früheren Arbeitgeber gerufen. Grund: Die Direktionsassistentin hat eine Mail des besten Freundes ihres Mannes erhalten. Darin Stand, dass ihrem Mann in Spanien die Brieftasche gestohlen wurde und dass sie ihm doch bitte per «Western Union Monney Kurier» dringend Geld zusenden soll. Für Fragen stehe das Hotel als Geldempfänger unter der Spanischen Nummer xy zur Verfügung. Das Mail war mit dem Spitznahmen des besten Freundes unterzeichnet. Die Absendermail stimmte auch.
Da ihr Mann auf Geschäftsreisen war, kam ihr das Vorgehen zunächst nicht suspekt vor. Trotzdem hatte sie Zweifel, dass etwas Faul war und rief mich an.

Sie hat mich gefragt, ob sie mal ins Hotel anrufen soll. Meine Antwort: Nein, eine Festnetznummer kann ohne weiteres Umgeleitet werden und da nimmt dann jemand aus einem Callcenter ab und sagt, dass ihr Mann unter der Dusche ist und sie das Geld nur senden soll.
Meine Empfehlung war: Ruf deinen Mann doch einfach mal an. Er hat ja ein Handy. Sie tat es aber es kam immer das Besetztzeichen. Ein Anruf aufs Handy des Freundes schaffte Klarheit, denn er wusste nichts von der Mail oder der Situation.
Aussage: Ihr Mann sitze im Flieger nach Amerika und können darum wohl nicht telefonieren. Die Mail sei sicher Fake.

Nach der Rückreise von allen Personen haben wir den Fall analysiert:
Woher wussten die Angreifer vom Spitznamen? Auf der Webseite vom Skiklub stand sein Spitzname. Im XING Profil seine Mailadresse und im Facebook hatte ihr Mann seine Reise in die USA angekündigt…

Fall Amazon

11.05.2020 / Quelle SRF

- Dank dem Kauf von gestohlenen Benutzer-Daten eines anderen Webshop-Portals (nicht Amazon) im Darknet , konnten sich die Betrüger mit den identischen Logindaten im Amazon Shop anmelden (Mehrfachnutzung Logindaten).
- Die Betrüger haben die Zahlungsart auf Monatsrechnung und die Lieferadresse umgestellt und für über 20`000.- Material zur neuen Lieferadresse bestellt.
- Die neue Adresse war in einem Wohnblock mit unbewachtem Zugang zu den Briefkästen.
- Die Pakete wurden immer sofort nach Anlieferung der Post von den Betrügern aus dem Milchfach entwendet.
- Der Betrug flog erst auf, als Amazon den eigentlichen Login-Besitzer wegen Zahlungsverzug per Brief mahnte und dieser bei der Durchsicht seines Kontos aus allen Wolken fiel.
- Amazon beharrte auf den Betrag und wies jede Schuld von sich und bekam vom Gericht Recht, denn eine Mehrfachnutzung von denselben Logindaten in mehreren Shops ist fahrlässig. (Risiko des Kunden)
- Der geprellte Amazon Kunde musste den Betrag selbst bezahlen und hat hoffentlich etwas dabei gelernt.
- Von der Ware fehlt nach wie vor jede Spur und diese Art des Betrugs, kommt regelmässiger vor als man denkt.
- Die Betrüger kamen über ein klassisches Datenleck bei einem Webshop (Folie 17) an die Daten.