



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.

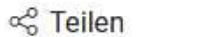
[Ein Fall von Erpressung?](#)

Die EnBag wird Opfer eines Hackerangriffs – und schweigt

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

[Fabio Pacozzi](#)

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 EnRan-Server ein und verschlüsselten darauf

 Artikel hören
 Teilen

Zunahme der Bedrohung:



Betriebsrelevant?

Eine nicht funktionierende IT ist mit hohe Kosten verbunden!

Die größten Geschäftsrisiken 2022

Anteil der Befragten, die folgende Risiken 2022 als besonders relevant einschätzen (in %)



Basis: 2.650 Risikomanagementexpert:innen in 89 Ländern; Okt-Nov 2021
Quelle: Allianz Global Corporate & Specialty



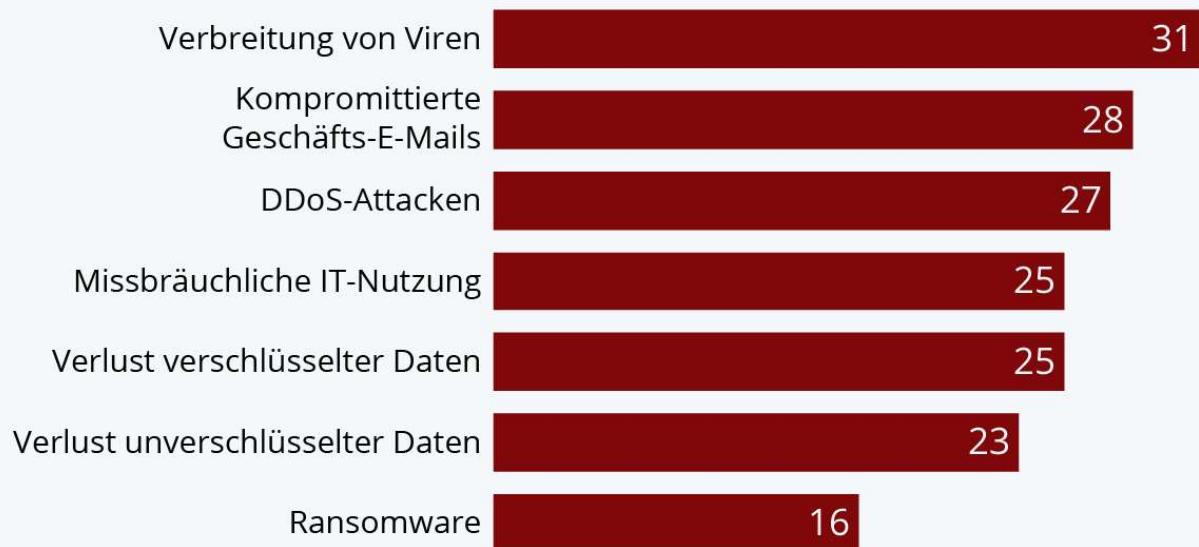
Viren usw.

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

Viren immer noch die größte Cyber-Bedrohung



Anteil der befragten Firmenvertreter, die Cyber-Angriffe mit folgenden Resultaten erlebt haben (in %)*



* Mehrfachnennung möglich

Basis: 6.042 Firmenvertreter in den USA, Großbritannien, Frankreich, Deutschland, Belgien, Spanien, den Niederlanden und Irland; November 2020 - Januar 2021

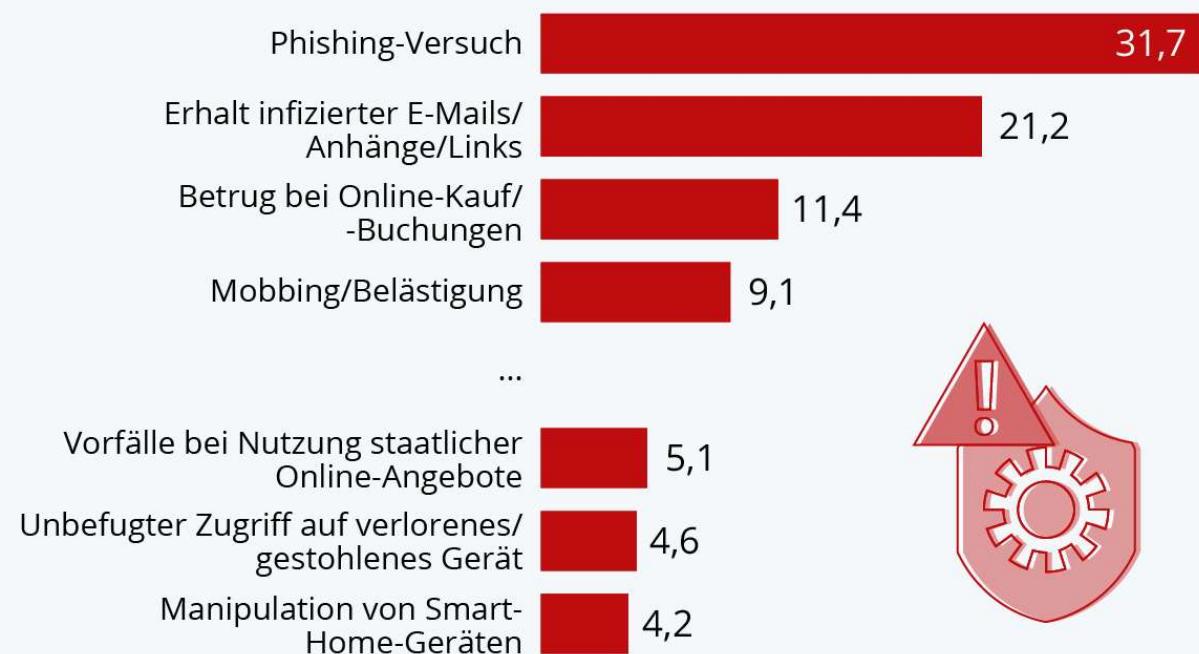
Quelle: Hiscox



E-Mails:

E-Mails bleiben größtes Sicherheitsrisiko

Anteil der Befragten in Deutschland, die 2021 folgende IT-Sicherheitsvorfälle erlebt haben (in %)



Basis: Über 2.000 Befragte (ab 16 Jahren) in Deutschland; Juni 2021

Quelle: Deutschland sicher im Netz e.V.



Erpressung

Regierungen und Behörden sind ein attraktives Ziel für Ransomware

Ransomware: Wenn Daten zu Geiseln werden

Anzahl öffentlich gemachter Ransomware-Angriffe 2021 weltweit nach Sektor*



* Stand: 01.11.2021

Quelle: Blackfog



statista

Veröffentlichte Ransomware-Angriffe seit Jahresbeginn
244
Veränderung ggü. Jan-Nov 2020
 +25%

Wie erkennen?

Ransomware 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?

Ihr Paket ist unterwegs

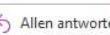


Lieferung Paket <kundin@vergiklp.com>
An s.soltermann@etourism.ch

(i) Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.



Antworten



Allen antworten



Weiterleiten



Mo. 05.09.2022 07:01



Ihr Paket ist unterwegs

Sehr geehrter Kunde,

Sie haben ein Paket auf der Durchreise, aber wir konnten Ihre Adresse
nicht bestätigen.

Bitte fahren Sie mit dem Formular mit dem untenstehenden Button fort,
um Ihre Lieferung zu beschleunigen.

Fortfahren

Voraussichtliches Lieferdatum:

Donnerstag, 8 September, 2022 - Ende des Tages

Bitte beachten Sie, dass die Bestätigung innerhalb von 24 Stunden erfolgen muss.



2022 © Swiss Post SP - Alle Rechte vorbehalten

Wie erkennen?

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

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

SWISS POST

Ihr Paket ist geliefert

Sehr geehrter Kunde,

Sie haben ein Paket auf der Durchgangsstation bestellt und möchten es nicht bestätigen.

Bitte fahren Sie mit dem Formular fort, um Ihre Lieferung zu beschleunigen.

<a href="https://u28898832.ct.sendgrid.net/ls/click?upn=d7c1rjbejngzunfoxdu-2fa6jgwz7uph9u9yslegnoucm9p3dtznjp2z90tuh6y3wd6sujm6ua83-2ft-2f-2b1kscdxa2fx1zryxzbwgwbrpyfergcycjeyxfaxmuj2qnmaiij5j-2f0-2fnnst8peqlksxx7a-3d-3dwvb-a_zzxoych-2bpmrnxzbupewzyq4wpdxfdtjmvm3vceogxbxrugmr3a6krto1bui6ekdrjp1mfthehnmyhawoudjp4vmmmcxa8tyebrt3ndcps5ta1rkpviiyutajwbd8ychz5i6ksa62k6zwmhtdz2jwippdirqgw4u34ssuaoxoflysa2phjx05g962azg0m-2f2dwnztqc5e78pyu1t99dagg238coptqdb4iaeqbziapmeaa1qvdo4dwleboyxvx66ixld1qwqpxsqmitgrtxqoc11iy5zk6ws-2f6efhbqbn3d9ufbvxtu1v1wn57zr3lfszw0ltjkqzgawwy03uk2a0whenv1dhw3obdlcm6ex0va8vv4mmmd945p10tw53ipchmknhjs47vkfzbepufltu-2bcbaokb901xho-2frum3je0yp26hronpqfe4gxn1-2borijqsa8lr-2f7puikxh3h9vza0ihendlbnwo71a103b3tpzvbfajvox-2fsxflyaoq3lwq-2bkpphe1pdkjablk6rooblkdovrdtfa7afunfedqabfwfjpnrokcnwkr7woncywihsen4gg8fbujycqcwtzuvx6wmua3d3yya9iazjmgarcryqb3dvwpngiksbhaxkpw1uqxo-2f8fxh9uyv2nxl283fujpblix-2fp828qn1mra2hqqowlucxcdd28yngscjc3zqnrcth6zzfxhh8jiugxdurisbjbmi1k3cz7qcefomnryfxbpr-2fxrpw-2fiwv98tq2bayzubhhwzebp3v4th9dsn5kkt1dqbytk9csve47jo8ooth7-2b6ww1afa8n0tjqn4d71qjobufspzim1kuw7www-2f2aubcl7z8e-3d

Klicken oder tippen Sie, um dem Link zu folgen.

Fortfahren

Hinter dem Button, versteckt sich viel aber sicherlich nichts von der Post Schweiz.

Voraussichtliches Lieferdatum:
Donnerstag, 8 September, 2022 - Endzeitpunkt

Bitte beachten Sie, dass die Bestätigung innerhalb von 24 Stunden erfolgen muss.

Wichtig: Link nie anlicken, sondern nur mit der Maus darüberfahren, dann wird das Ziel vom Link angezeigt und der Fall ist zu 99% klar.

Achtung: Bsp. post.gugus.com ist keine gültige Postadresse!

Merke: Grossfirmen kommunizieren immer über den bekannten Namen wie post.ch, migros.ch usw.

SWISS POST

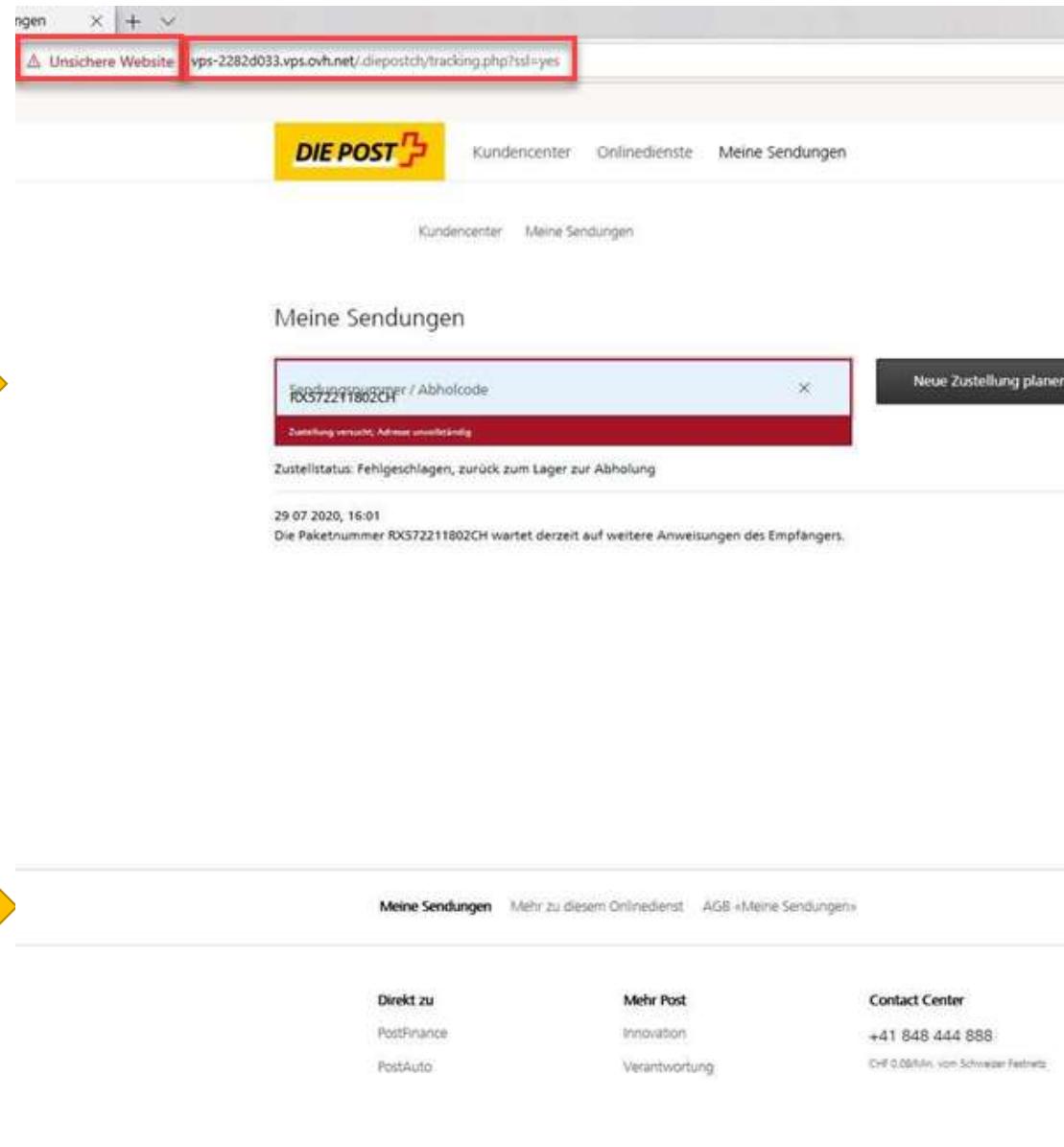
2022 © Swiss Post SP - Alle Rechte vorbehalten

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...

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)

Vereinigte Staaten der Datenpannen

Anzahl von Datenschutzverletzungen betroffener Accounts in ausgewählten Ländern weltweit (in Mio.)



Basis: Alle öffentlich zugänglichen Datensätze mit Sicherheitsverletzungen;
Nov. 2020 - Nov. 2021
Quelle: Surfshark



Datendiebstahl:

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

Demo: <https://haveibeenpwned.com/>

Die größten Daten-diebstähle der Welt

Größte bekannte Datenlecks
nach Anzahl betroffener Accounts (in Mio.)^{*}

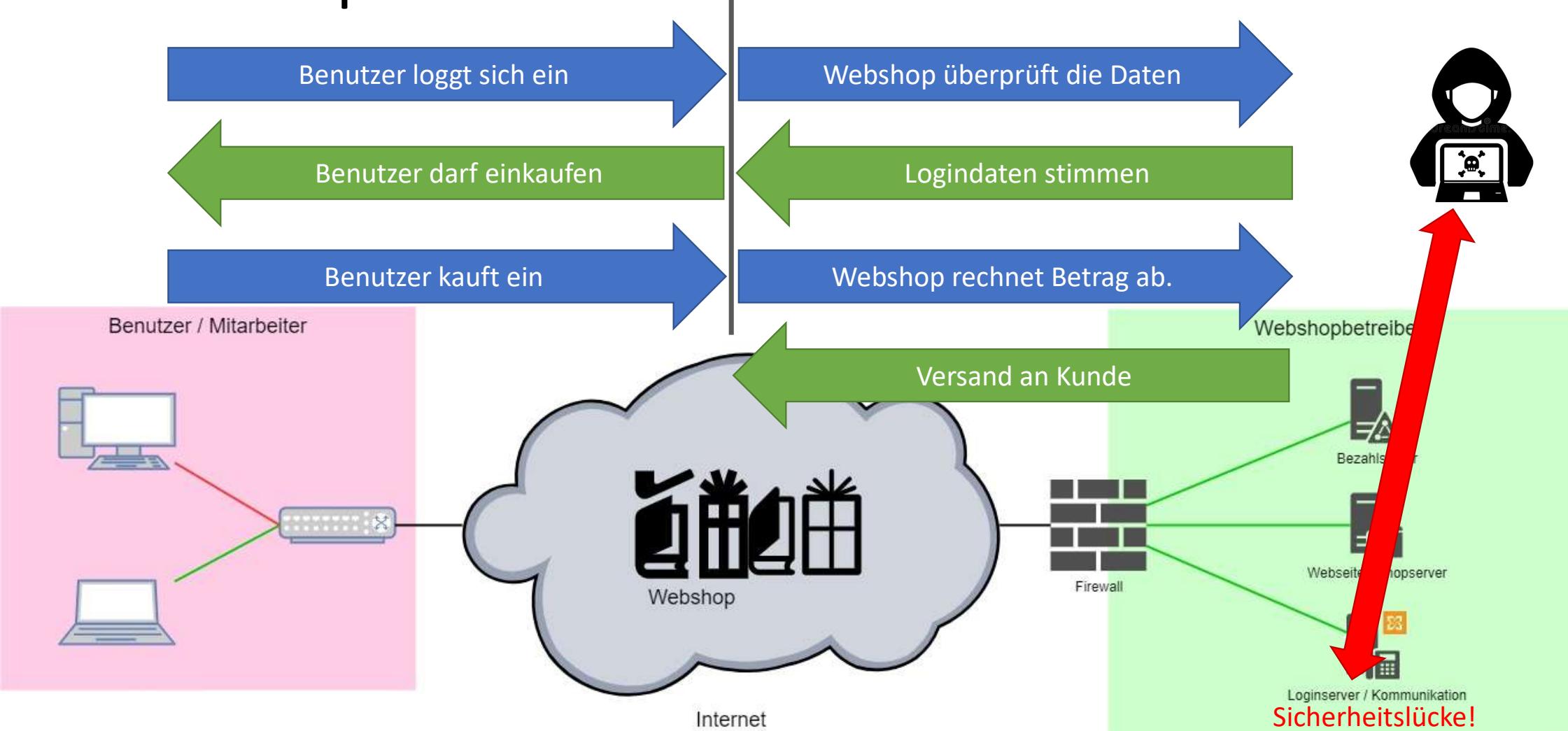


* Ohne Duplikate

Quelle: Have I Been Pwned?



Webshop:



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/>

The screenshot shows the homepage of haveibeenpwned.com. At the top, it asks "Check if your email or phone is in a data breach". A red box highlights the email address "s.soltermann@etourism.ch" in the search bar. To the right, a button says "pwned?". Below the search bar, the text "Oh no — pwned!" is displayed, followed by "Pwned in 2 data breaches and found no pastes (subscribe to search sensitive breaches)". A large red arrow points from the "pwned?" text down to the "Breaches you were pwned in" section. This section lists the "Adobe" breach from October 2013, which compromised 153 million accounts. It includes a red icon of the letter 'A' and a detailed description of the breach. Another red arrow points from the "Compromised data" section of the Adobe entry down to the "Onliner Spambot" entry below it. The "Onliner Spambot" entry includes a red icon of an envelope and a detailed description of the breach.

Sichere Passwörter?



<https://www.passwortcheck.ch/>

Das zu prüfende Password lautet:

.....

Passwort anzeigen

Das eingegebene Passwort ist stark

Das Passwort ist Stark

Alles unter «stark» ist ein Risiko und sollte geändert werden!
Mit künstlicher Intelligenz (ChatGPT) haben die Hacker ein neues top Werkzeug zum Knacken eurer Passwörter erhalten!
Passwörter welche vor Wochen noch Jahre an Rechenzeit benötigten, gehen jetzt in Minuten = Passwörter müssen noch länger und komplexer werden.

Ausgewählte Wörterbücher

Deutsch Französisch Italienisch
 Rätoromanisch Englisch

Teilwörter	Länge	Typ	Raumgrösse	Anzahl Versuche	Entropie	Rechenzeit
***	10	Übrige Zeichen	102	1.219e+20	67 Bit	
Aufwandschätzung				1.219e+20	67 Bit	39 Jahre

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).

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

The screenshot shows the 'Password Manager Pro' application interface. On the left is a sidebar with icons for Ressourcen, Gruppen, Verbindungen, SSH-Schlüssel, Nutzer, Administrator, Überwachung, and Persönlich. The main area has a blue header bar with a search field and a back button labeled 'Default Group'. Below the header, there are tabs for 'Ressourcen' (selected) and 'Kennwörter'. A large blue arrow points from the sidebar towards the right content area. The right side displays a list of saved logins under 'Default Group':

- LokalAdmin | [redacted]
- Polizei || Diensthandys || Win... [redacted]
- USV Cloud Login [redacted]
- Veeam Schulaccount [redacted]

Ende:



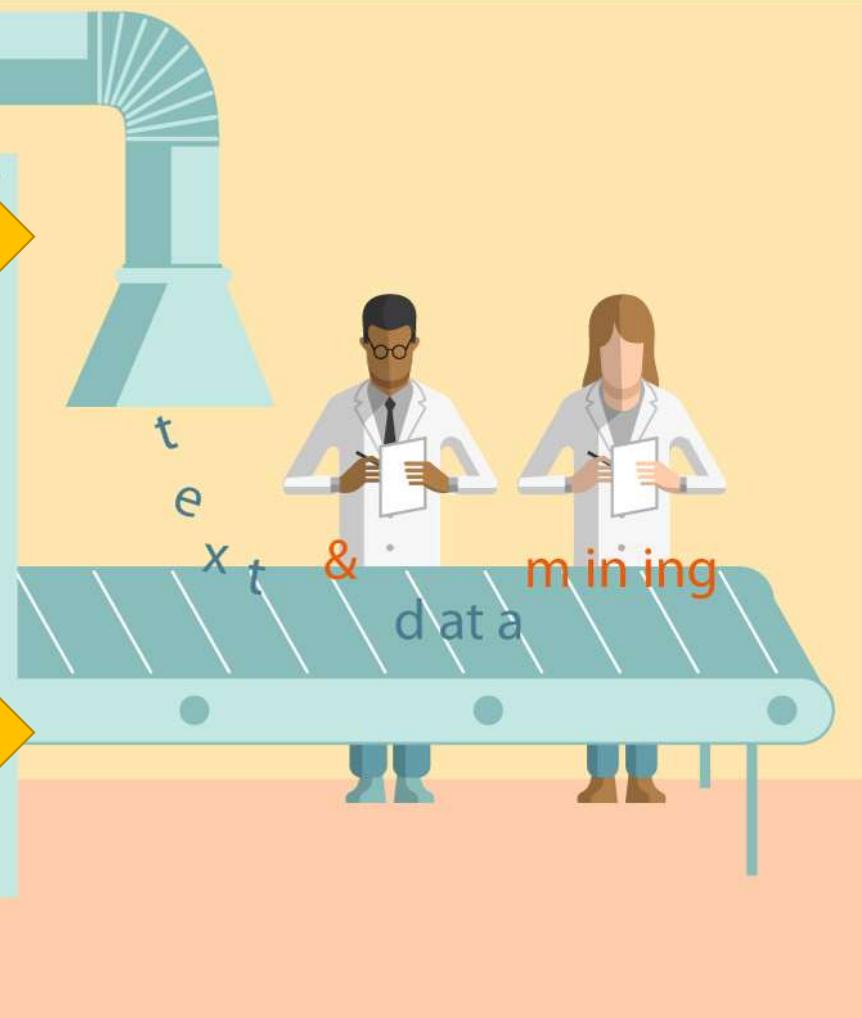
Folien, Links, Schulungen, Fragen usw. bitte über stefan.soltermann@brig-glis.ch

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 Money Kurier» dringend Geld zusenden soll. Für Fragen stehe das Hotel als Geldempfänger unter der Spanischen Nummer xy zur Verfügung. Das Mail war mit dem Spitznamen 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.