Ransomware – kalter Kaffee?

Sicherheit im Internet

Marcel Grand

Information Security Consultant / CISO

Unwahrscheinlicher Fall?

goSecurity
EXPERTEN FÜR IHRE IT-SICHERHEIT

26. März 2017

Dishwasher has directory traversal bug

Thanks a Miele-on for making everything dangerous, Internet of Things firmware slackers

26 Mar 2017 at 23:08, Richard Chirgwin

Don't say you weren't warned: Miele went full Internet-of-Things with a network-connected

Unwahrscheinlicher Fall?

goSecurity
EXPERTEN FÜR IHRE IT-SICHERHEIT

18. Juni 2008

Kaffeemaschine gehackt

18.06.2008, 17:07 Uhr | Sascha Plischke

TEILEN TWITTERN DRUCKEN MAILEN REDAKTION

Internet-Kaffee: Hacker können über Kaffeemaschine für ärger sorgen. (Foto: T-Online)

Kaffeemaschinen des Herstellers Jura lassen sich über das Internet hacken. Das hat nun ein australischer Sicherheitsfachmann herausgefunden. Hacker können offenbar ganz einfach über eine Verbindung zwischen Kaffeeautomat und PC in das Gerät eindringen. Dabei können sie ihren Opfern nicht nur den Kaffee gründlich vermiesen – über die Abwehrschwäche der Kaffeemaschine können Kriminelle gleich auch noch den angeschlossenen Computer kapern.

Unwahrscheinlicher Fall?

goSecurity
EXPERTEN FÜR IHRE IT-SICHERHEIT

16. Oktober 2014

16.10.2014 07:45 Uhr

Achtung: Die Zahnbürste ist gehackt

Risiko Die Vernetzung von Milliarden Geräten wird das Risiko von Hacker-Angriffen im Alltag nach Einschätzung eines Cyber-Sicherheitsexperten rapide erhöhen. "Die Angriffsfläche für Online-Kriminelle weitet sich damit dramatisch aus", betonte Raj Samani vom Antiviren-Spezialisten McAfee. Sicherheit und Datenschutz müssten von Anfang an beim weiter

Unwahrscheinlicher Fall?

goSecurity
EXPERTEN FÜR IHRE IT-SICHERHEIT

20. September 2016

foto: apa
Chinesische Sicherheitsforscher entdeckten Sicherheitslücke in Teslas Model S.

Tesla gehackt: Forscher knacken Auto per Wlan

20. September 2016, 11:56

27 POSTINGS

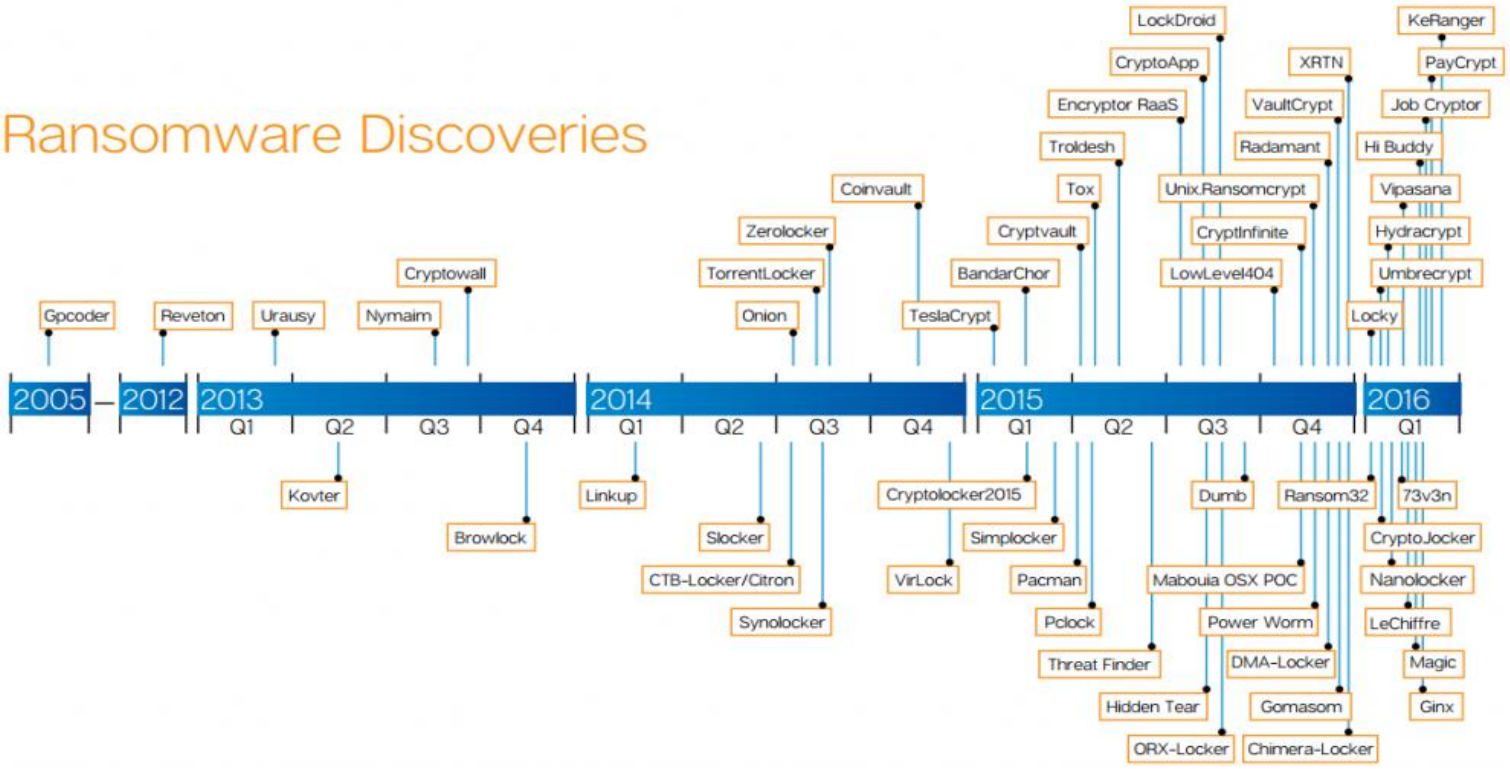
Chinesische Sicherheitsfoscher übernahmen Kontrolle von Bremse und Türverriegelung – Sicherheits-Patch bereits veröffentlicht

Sicherheitsforscher von Keen Lab konnten sich erfolgreich in Teslas Model S über Funk einhacken. Das chinesische Forscherteam machte eine Sicherheitslücke im Kontrollsystem ausfindig, und drang über einen Wlan-Hotspot ins Auto ein. Mit dem Hack konnten sie unter anderem die Bremsen bei voller Fahrt betätigen. Tesla hat auf den Hack reagiert und ein Sicherheitsupdate ausgeschickt.

Hack über Wlan-Hotspot

Hacking – Jeden Tag ein neuer Angriff

Ransomware überall - und immer neue Varianten



Quelle: Symantec Internet Security Threat Report 2016

Ransomware – die jüngsten Betroffenen

10.10.2022	Hacker greifen Webseiten von **US-Airports** an	Link
25.09.2022	IT-Sicherheitslücke bei **Lufthansa:** Chef der Fluglinie selbst betroffen	Link
19.09.2022	**UBER** gehackt: Zugriff auf interne Systeme und Schwachstellenberichte gestohlen	Link
19.09.2022	**"GTA VI"-Leak**: Hacker erpresst **Entwickler Rockstar**	Link
06.09.2022	**Schoggifabrikant Läderach** von Ransomware-Attacke beeinträchtigt	Link
01.09.2022	**TAP Air Portugal** hacked by RagnarLocker Ransomware Gang	Link
23.08.2022	**Krankenhaus bei Paris** weist wegen Cyberattacke Notfallpatienten ab	Link
08.08.2022	Produktion lahmgelegt: **Medi Bayreuth** steht nach Hacker-Angriff mehr oder weniger still	Link
01.08.2022	Nürnberger Elektronikhersteller **Semikron** gehackt	Link
18.07.2022	Cyberangriff auf **Stadt Bülach**	Link
07.07.2022	Wieder Datenleck bei **Hotelkette Marriott**: Firmen- und Kundendaten kompromittiert	Link
30.06.2022	**Baustoffhersteller Knauf** Opfer von Cyberangriff	Link
28.06.2022	**Ransomware-Attacke auf AMD**: 56 GB an Daten abgeflossen	Link
21.06.2022	Cyber-Angriff auf **H+ Die Spitäler** der Schweiz	Link
20.06.2022	Hacker-Angriff auf die **Med-Uni in Innsbruck**	Link
12.06.2022	Cyberangriff beim **Darmstädter Energieversorger Entega**	Link

“Es ist ja noch nie etwas passiert”

Source: Blick Online, 28. Februar 2020

Ransomware

- Conti Pentester Guide Leak
  https://github.com/ForbiddenProgrammer/conti-pentester-guide-leak
- NoMoreRansomware
  https://www.nomoreransom.org/de/index.html
- Aktuelle Zahlen
  https://www.coveware.com/ransomware-quarterly-reports

Average and Median Ransom Payment in Q2 2022

Average Ransom Payment

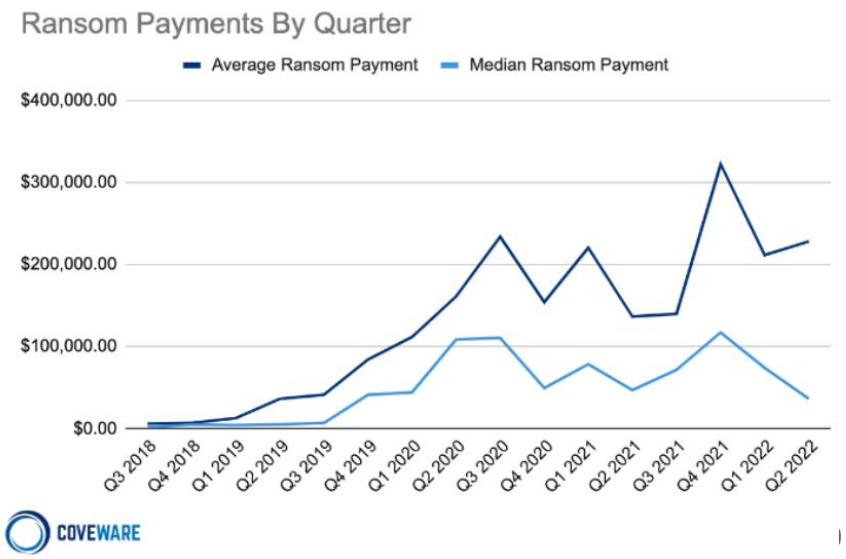
$228,125

+8% from Q1 2022

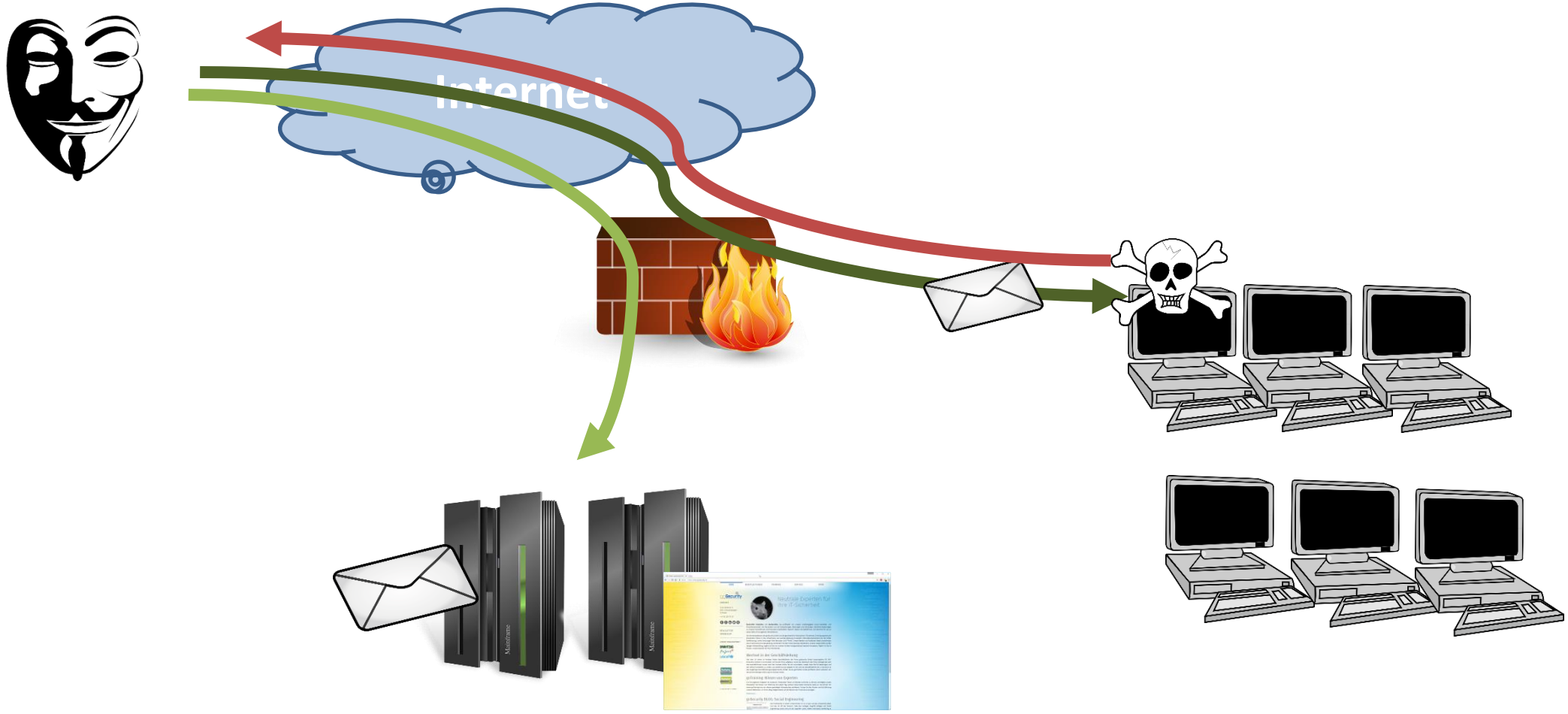
Median Ransom Payment

$36,360

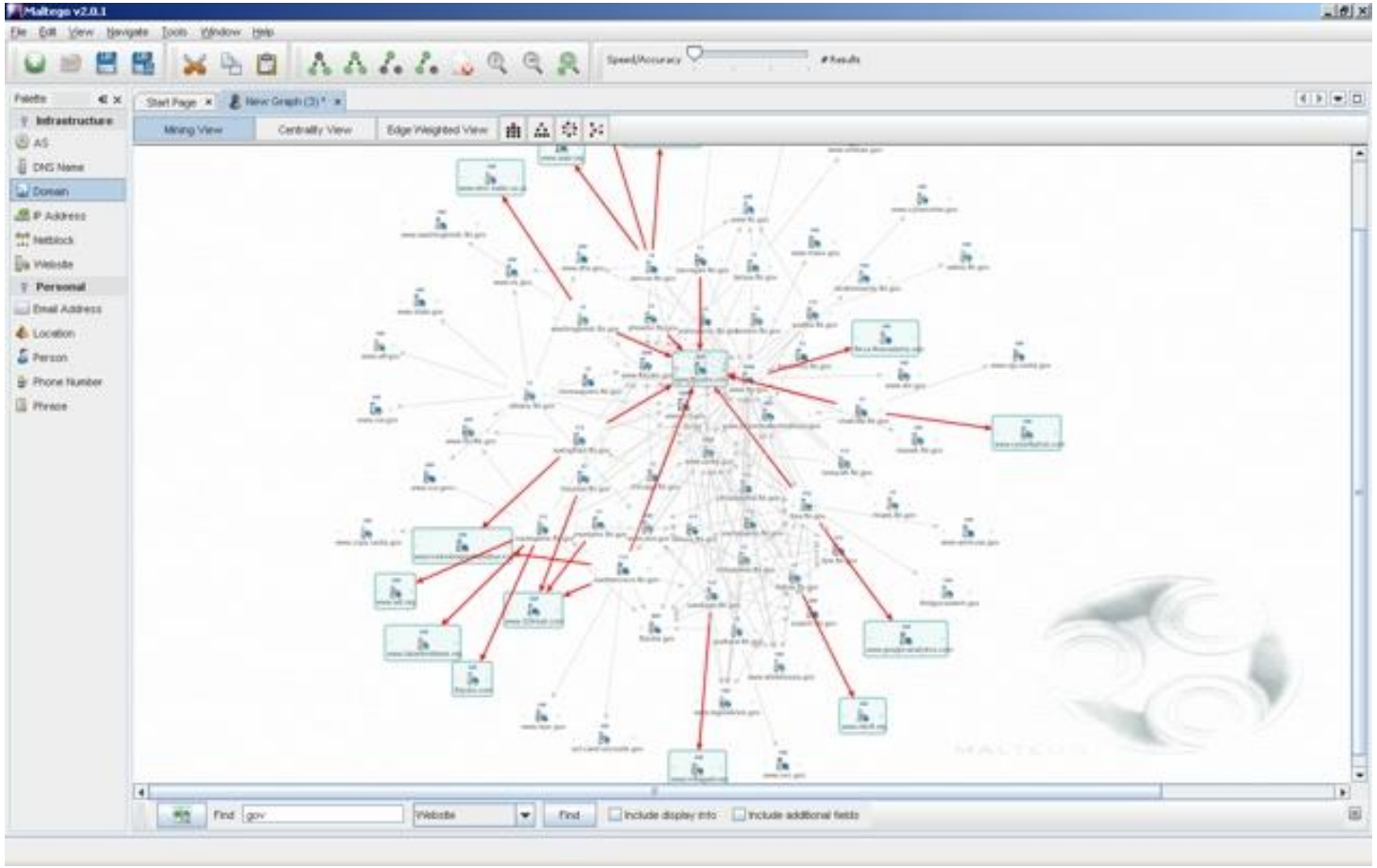
-51% from Q1 2022



Wie gehen Hacker vor?



Informationssuche



Maltego ist eine Analysesoftware, mit der sich Informationen im Internet suchen und verknüpfen lassen.

Phishing

[Spam] PostFinance - Message alert

Swiss Post Security <security@postfinance.ch>

Gesendet: Sa 16.04.2011 05:25

An: undisclosed-recipients:

PostFinance SWISS POST

Important Information Regarding Your PostFinance Account.

Dear member,
We are writing regarding your PostFinance Account
Case ID : (6224-81532-4235-8431)

We have reason to believe that your account was accessed by a third party
Because protecting the security of your account is our primary concern, we have limited access to sensitive PostFinance account features.We understand
that this may be an inconvenience but please understand that this temporary limitation is for your protection.

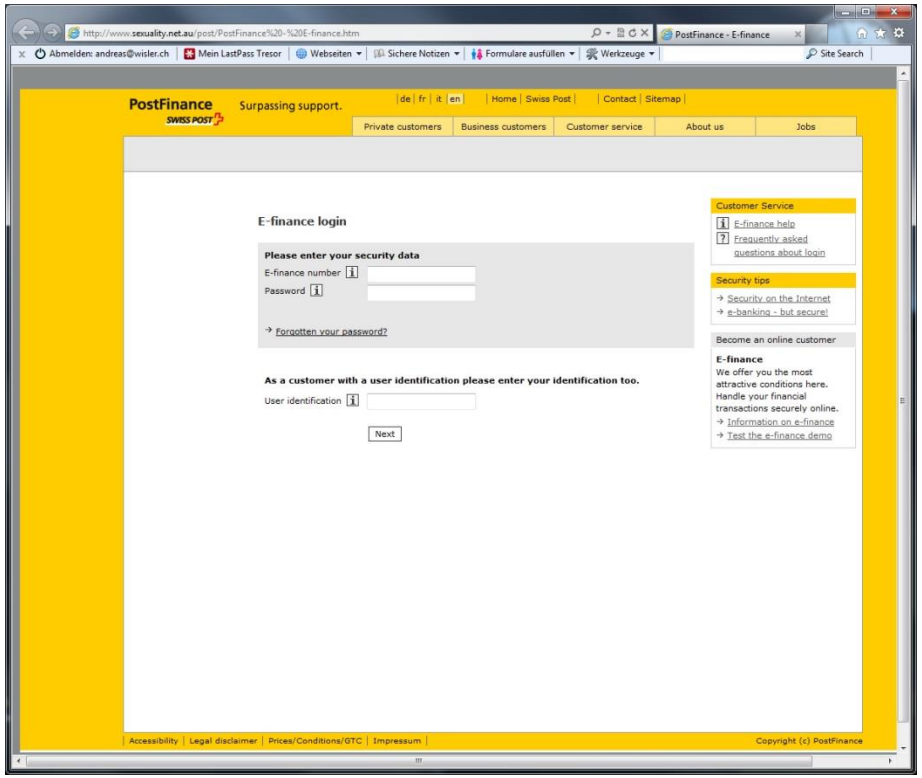
SERVICE : PostFinance SWISS POST.
EXPIRATION : April , 25 , 2010

What you need to do:
Activate your credit card by click on the link bellow and complete the fields :

https://e-finance.postfinance.ch/ef/secure/html/?login&p_spr_cd=4

- Update your information immediately.

Thanks
PostFinance Cards Department.



Phishing

An: Andreas Wisler;

Sehr geehrter Herr Wisler

Der von Ihnen gesuchte Gegenstand wurde im Fundbüro am Flughafen Zürich, Ankunft Terminal 1, abgegeben und ist nun bei uns unter der Referenz-Nummer F-2015/01558 eingelagert und zum Abholen bereit. Die Abholgebühr beträgt CHF 20.-, für HON oder Senator Member ist diese gratis.

Unsere Öffnungszeiten sind täglich von 06:30 – 23:00 Uhr.
Zur Abholung sind Referenz-Nummer sowie ein Personalausweis notwendig.

Sollte es Ihnen nicht möglich sein, den Fundgegenstand am Flughafen abzuholen, bestehen noch untenstehende Varianten. In einem solchen Fall, bitten wir Sie, mit uns Kontakt aufzunehmen.

Für Kunden mit Domizil Schweiz
Ihr Fundgegenstand wird gegen eine Vorauszahlung von CHF 40.-, per Post nach Hause geschickt. Sobald Ihre Zahlung bei uns eingetroffen ist, werden wir Ihnen den Gegenstand zustellen. Einzahlung bitte auf unser Konto:
UBS AG, Bahnhofstrasse 45, 8001 Zürich
Konto: 0230-0018067502V
IBAN: CH91 0023 0230 1806 7502 V
Mitteilung: Referenznummer -> ist zwingend anzugeben

Für Kunden mit Domizil Ausland
Ihr Fundgegenstand wird an einem Flughafen in Ihrer Nähe nachgeschickt, damit Sie ihn dort abholen können. (Nur auf direkten Flügen von Swiss International Air Lines ab Zürich)

Wir möchten Sie darauf aufmerksam machen, dass wir in solchen Fällen keine Haftung für evtl. Beschädigungen/Verluste übernehmen.

Freundliche Grüsse

Swissport International Ltd. Station Zurich
Fundbüro
Postfach
CH - 8058 Zürich-Flughafen

Tel: +41 900 57 10 15 (CHF 1.19/Min)
Email: zrh.lostproperty@swissport.com
www.swissport.com/network/zrh/easyfind

Phishing


I'LL HELP YOU FIND THE HACKERS
...
GIVE ME YOUR PASSWORD
CHAPPATTE
The New York Times

Was können Sie tun?

- ❒ Verwenden Sie aktuelle Antivirenprogramme und eine moderne Firewall.
- ❒ Schulen Sie alle Ihre Mitarbeitenden regelmässig und wiederholt.
- ❒ Bewerten Sie Schwachstellen (Risikoanalyse) und schliessen Sie diese so schnell wie möglich.
- ❒ Machen Sie niemals Systeme ohne VPN zugänglich.
- ❒ Schützen Sie alle Zugänge aus dem Internet mittels MFA.
- ❒ Verwenden Sie immer sichere Passwörter (> 12 Zeichen) und nutzen Sie für jeden Dienst ein anderes.
- ❒ Antworten Sie nicht auf E-Mails, wenn Sie ein ungutes Gefühl haben.

Vielen Dank für Ihre Aufmerksamkeit!

Marcel Grand

Information Security Consultant / CISO