ZILLNER IT SECURITY

ÖGWT IHR SERVICE-NETZWERK

Internetsicherheit für die WT-Kanzlei

Tobias Zillner, BSc MSc MSc

ÜBER MICH

- Tobias Zillner, BSc MSc MSc
  - Selbstständiger IT-Sicherheitsexperte
    - Beratung, Überprüfung, Begleitung, Training
  - Ethical Hacker
  - Fokus KMUs
  - Sicherheitsforscher
    - Internet of Things, Smart Homes

- Vortragender auf Konferenzen/FH
  - Blackhat - Las Vegas, Singapur
  - Gastvortragender FH St.Pölten
  - CRESTcon – London
  - DeepSec, Bsides – Wien
  - Security Forum – Hagenberg

ZILLNER IT SECURITY

AGENDA

- Aktuelle Bedrohungen für Wirtschaftstreuhand-Kanzleien
- Risikofaktor Mensch
- Wie schütze ich meine Kanzlei?
- Notfallpläne zur Datenwiederherstellung
- Sichere Email Kommunikation und Datenübertragung im Alltag

ZILLNER IT SECURITY

AKTUELLE BEDROHUNGEN

WIE GEHEN HACKER VOR?

ZILLNER IT SECURITY

16.05.2016 10:46 **Ira Schaible, dpa** 157

Als Chef getarnt fordern Internet-Kriminelle Geld von Firmen

Bild: dpa, Soeren Stache

Mit psychologischen Tricks machen sich Straftäter im Internet an zuvor gezielt ausgesuchte Mitarbeiter von Firmen heran. Es geht um Geld oder Geschäftsgeheimnisse. Das Social Engineering hat aber noch mehr Facetten.

ZILLNER IT SECURITY

WASSERWAAGEN-APP

Android-Trojaner im Play Store installiert ungewollt Apps

Malware für Android existiert meist außerhalb des Play Store. Doch in einem aktuellen Fall hat Google eine Schadsoftware übersehen, die das Gerät rootet und innerhalb von 30 Minuten 14 weitere Apps installiert.

Eine Schadsoftware für ältere Versionen von Googles Android-Betriebssystem installiert ungewollt Apps auf den Geräten der Nutzer. Die Malware mit dem Namen Level Dropper findet sich nach Angaben der Sicherheitsfirma Lookout, die sich auf mobile Geräte spezialisiert hat, auch in Apps in Googles Play Store, in dem es im Vergleich mit alternativen Appstores eigentlich weniger Schadsoftware gibt. Level Dropper rootet das Gerät ohne Eingreifen der Nutzer, die App maskiert sich dabei als nützliches Wasserwaagen-Tool.

Diese Wasserwaage hat keine Malware. (Bild: Igge/Wikimedia Commons/CC-BY-SA 3.0)

Datum: 30.6.2016, 14:18

Autor: Hauke Gierow

Themen: Security, Android, Android 4.4, App, Google Play, Malware, Software, Trojaner

Teilen: 0 44 32 5

ZILLNER IT SECURITY

18. Mai 2016, 15:04 Uhr Gehacktes Karrierenetzwerk

Kriminelle verkaufen 117 Millionen gehackte Linkedin-Passwörter

ZILLNER IT SECURITY

DATENNETZ

Hackerangriffe sorgen für Ausfälle bei A1

von Gregor Gruber 01.02.16, 16:53 Mail an Autor

Das mobile Datennetz von A1 litt unter Störungen aufgrund von Cyberangriffen

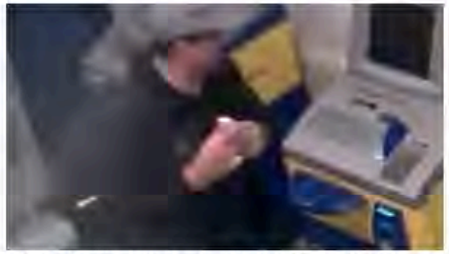
Das mobile Datennetz von A1 litt unter Störungen aufgrund von Cyberangriffen - Foto: APA/HERBERT PFARRHOFER

ZILLNER IT SECURITY

JACKPOTTING

Geldautomaten in Deutschland mit USB-Stick ausgeräumt

Seit 2010 ist das Plündern von Geldautomaten per USB-Stick bekannt. In Deutschland wurde nun erstmals ein Täter dabei gefilmt, wie er zwei Automaten an einem Tag ausräumte.



Der Täter vor dem Ausräumen des Geldautomaten in Berlin (Bild: Polizei Berlin)

Datum: 29.10.2015, 12:06

Autor: Friedhelm Greis

Themen: Security, Black Hat, Geldautomat, Sicherheitslücke, Internet

Teilen: 3 125 58 13

Tools: Drucken

Was der legendäre Hacker Barnaby Jack vor fünf Jahren auf der Black-Hat-Konferenz präsentierte, wird von Kriminellen auch in Deutschland weiter praktiziert: das Ausräumen von Geldautomaten mit Hilfe eines USB-Sticks.

ZILLNER IT SECURITY

SCHADSOFTWARE

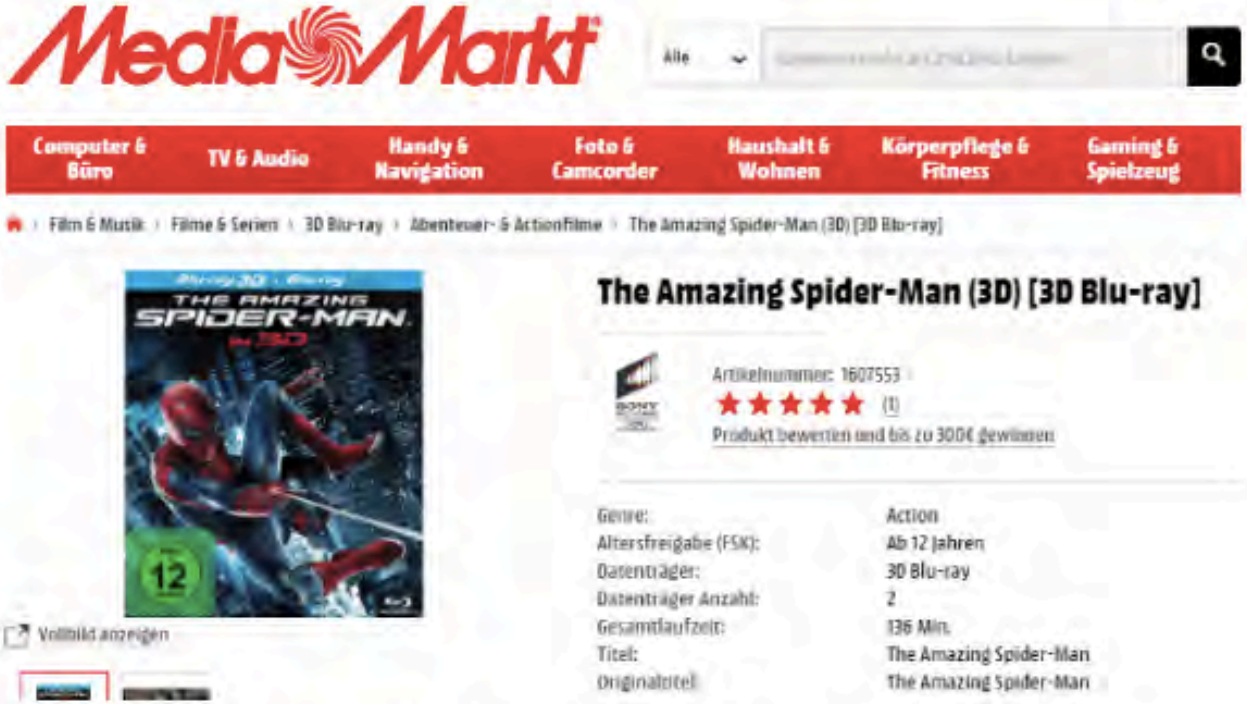
- Früher
  - Scherzprogramme
  - Datenzerstörung
  - Wichtigstes Kriterium**: Auffälligkeit!**
- Heute
  - Datendiebstahl
  - Aufbau großer Netzwerke (für Spam, Angriffe, …)
  - Wichtigstes Kriterium: **Unauffälligkeit!**
- Neue Methoden
  - Erpressung
  - Finanzieller Nutzen
  - Ausnutzung der größten Schwachstelle in jedem Unternehmen: **dem Menschen!**

ZILLNER IT SECURITY

Krypto-Trojaner Cerber: Angebliche Mediamarkt-Bestellung kommt Empfänger teuer zu stehen

23.06.2016 13:58 Uhr – Ronald Eikenberg

vorlesen



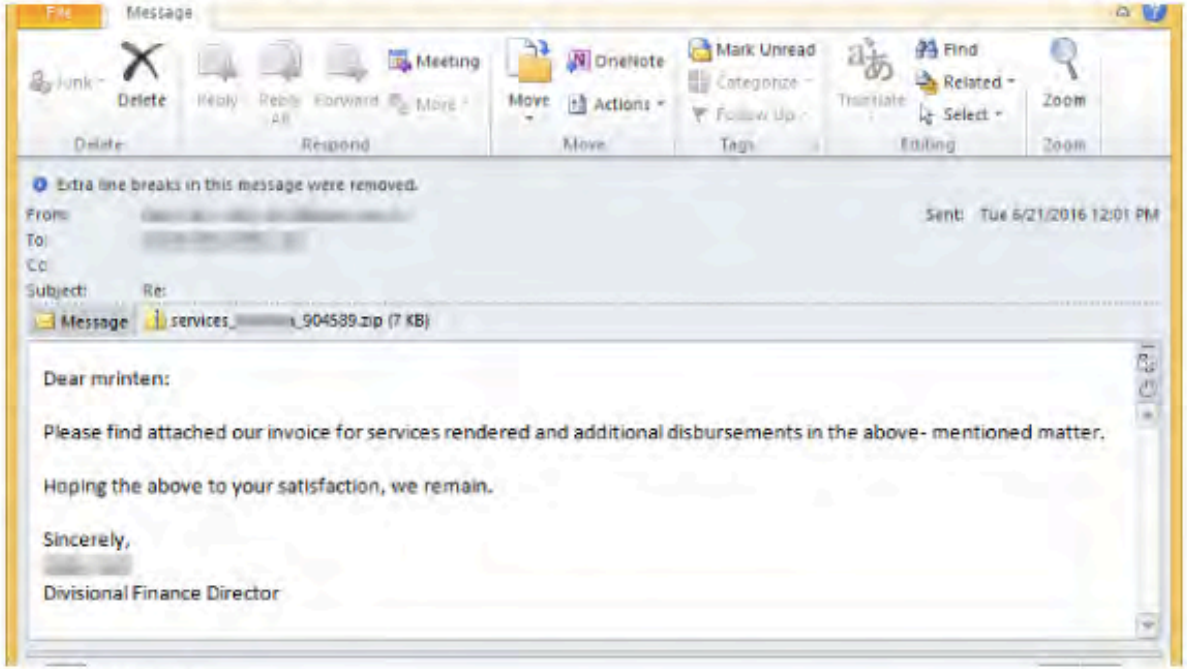
Online-Erpresser verschicken derzeit Mails, die vorgeben, dass ein bei Mediamarkt.de besteller Artikel in Kürze geliefert wird. Wer die Bestellung einsehen oder stornieren möchte, fängt sich einen Krypto-Trojaner ein.

ZILLNER IT SECURITY

Erpressungs-Trojaner: Neue Locky-Welle infiziert Computer

24.06.2016 11:46 Uhr – Dennis Schirrmacher

vorlesen



(Bild: Proofpoint)

Wer dieser Tage eine E-Mail mit Dateianhang bekommt, sollte diese noch kritischer als sonst beäugen: Aktuell verbreitet sich der Verschlüsselungs-Trojaner Locky erneut vornehmlich über vermeintliche Bewerbungs-Mails in Deutschland.

ZILLNER IT SECURITY

RANSOMWARE

- Häufigste Infektionswege
  - Mail mit Link oder Anhang
  - Verseuchte oder gehackte Webseiten
- Besonders betroffen: Personalabteilungen
  - Bewerbungen mit Anhang oder Link auf Cloud-Service
- Unterschiedliche Vorgehensweisen
  - Locky: System infizieren, warten, verschlüsseln
  - Petya: Infizieren des MBR, Neustart erzwingen, verschlüsseln mit manipuliertem chkdsk
  - Samsa: Umgebung evaluieren, Lösegeldforderung anpassen

ZILLNER IT SECURITY

RISIKOFAKTOR MENSCH

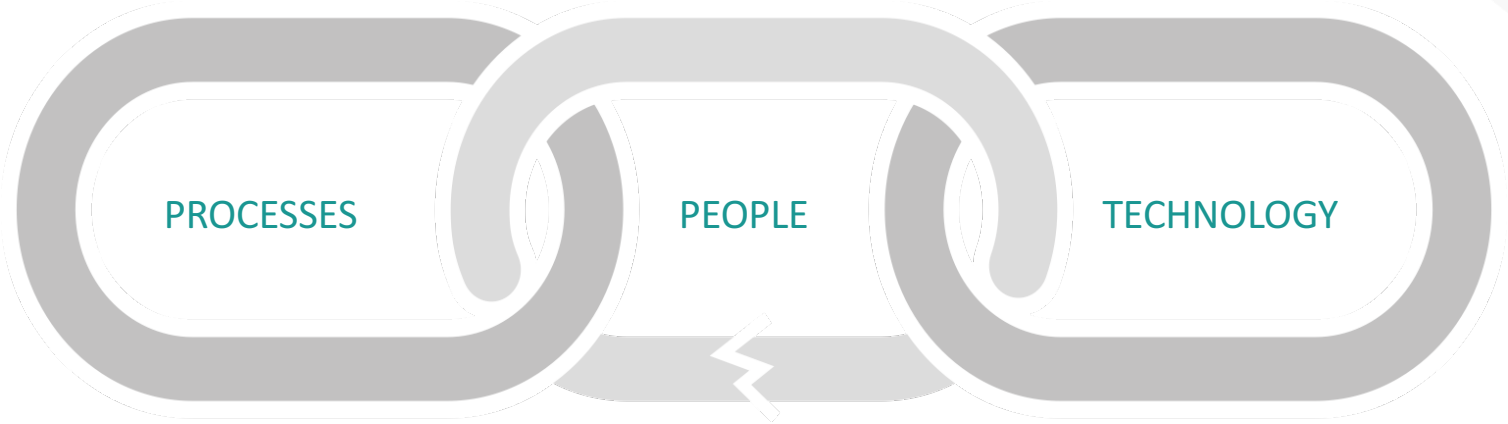
ZILLNER
IT SECURITY

https://ibmcai.files.wordpress.com/2014/06/iot-infographic-212-billion.jpg

ZILLNER IT SECURITY

MITARBEITER, PROZESSE, TECHNOLOGIE

- Welches is das schwächste Glied in der Kette?



ZILLNER IT SECURITY

ANGRIFFE AUF MITARBEITER

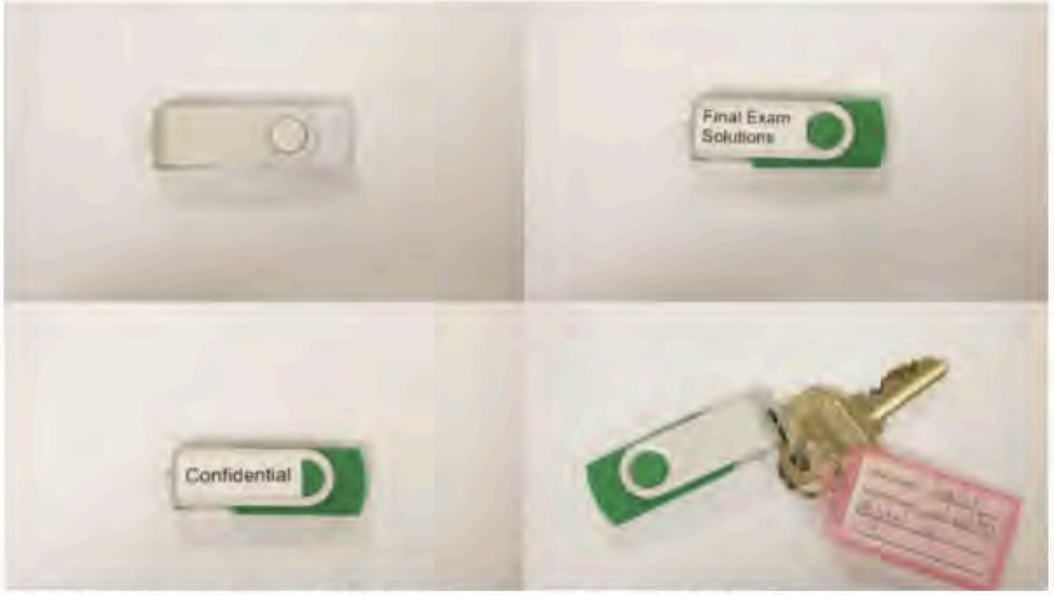
DER FAKTOR MENSCH IST DAS GRÖSSTE SICHERHEITSRISIKO

- Fehler (unabsichtlich / absichtlich)
- Bequemlichkeit
- Phising
- Social Engineering
- Spear Phishing
- Telephone Spoofing
- SMS Spoofing
- Watering Holes
- Malware
- QR Codes
- Keylogging Devices
- “Bad” USB
- Evil AP

ZILLNER IT SECURITY

07.04.2016 11:47 **Dennis Schirrmacher** 390

Studie: Würden Sie einen gefundenen USB-Stick anschließen?



Für ein Experiment wurden verschiedene USB-Sticks auf einem Campus-Gelände verteilt.

Bild: Screenshot

Auf dem Campus-Gelände der Universität Illinois lagen 297 USB-Sticks als Köder aus. Das Ergebnis einer Studie zeigt, wie viele eingesammelt und angeschlossen wurden.

48 Prozent der Finder eines USB-Stick nehmen diesen mit, schließen ihn an einen Computer an und öffnen Dateien. Das ist das Ergebnis einer Studie der Universitäten Illinois und Michigan und Google (PDF-Download). Mit Malware infizierte USB-Sticks sind ein durchaus denkbarer Weg, um Computer anzustecken und etwa Daten abzuziehen.

ZILLNER IT SECURITY

Studie: Viele User geben Passwort für Schokolade her

28. Juni 2016, 17:15

71 POSTINGS

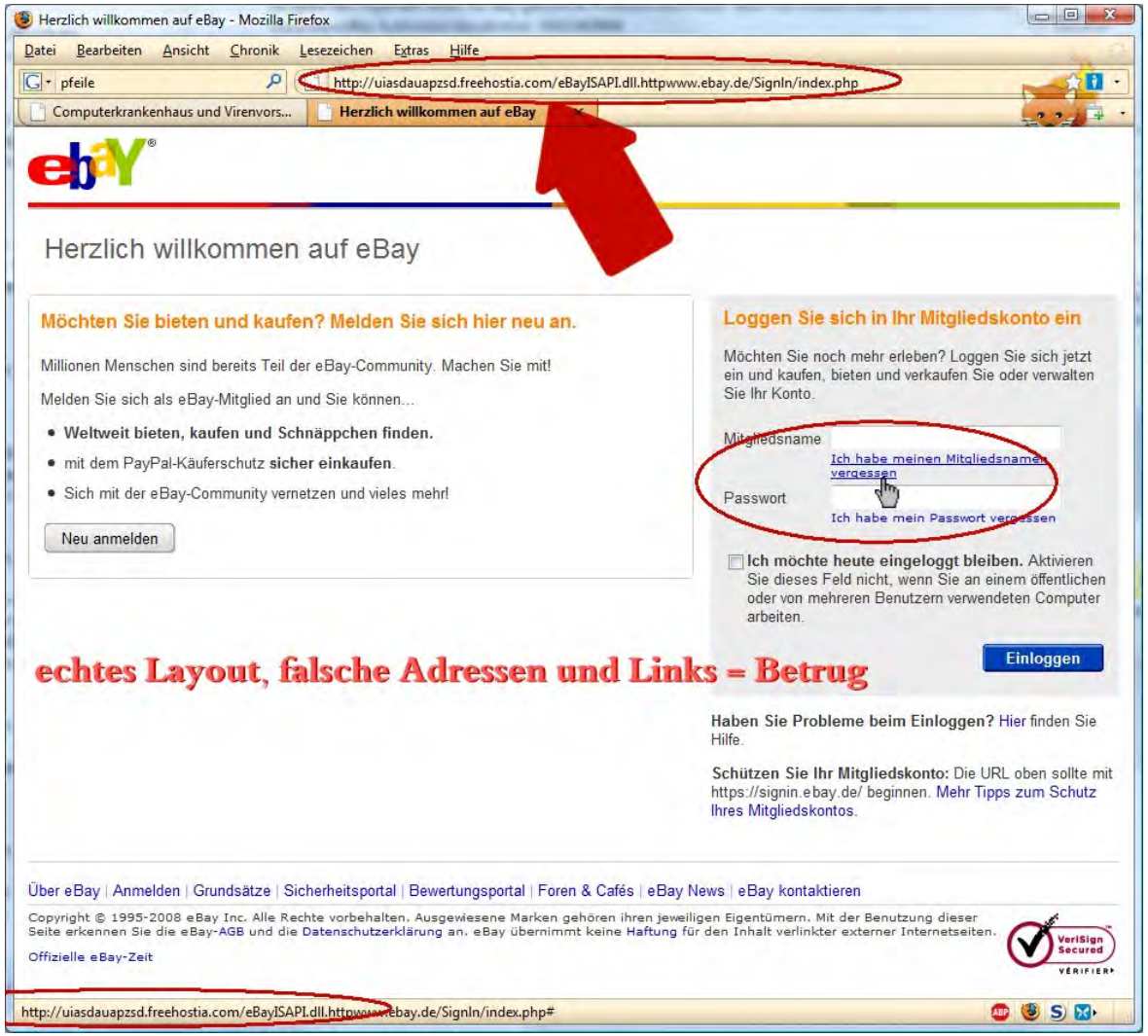
foto: dst.at/ntg3nza1 / wikimedia commons (CC-Lizenz)
Erstaunlich viele Teilnehmer waren bereit, ihr Passwort bekanntzugeben – insbesondere dann, wenn sie davor Schokolade bekamen.

Hohe Nennbereitschaft bei süßem Geschenk unmittelbar vor Frage

Sichere Passwörter zu erstellen, stellt für viele Nutzer immer noch eine Herausforderung dar. Regelmäßig landet etwa "123456" vorn in der Topliste der am häufigsten genutzten Kennwörter. Dass viele Surfer auch gern das gleiche Passwort für mehrere Dienste nutzen, sorgt regelmäßig für Kollateralschäden, wenn Hacker Datenbanken von einem Anbieter knacken.

Der Mangel an Sicherheitsbewusstsein geht aber über diese Problematiken hinaus. Das legt zumindest eine Untersuchung von Forschern der Universität Luxemburg und der International School of Management in Stuttgart

ZILLNER IT SECURITY



ZILLNER IT SECURITY

SCHUTZ VOR PHISING

- E-mails aufmerksam lesen
- Kritisch hinterfragen, warum man bestimmte Mails bekommt
- Sensible Inforamtionen werden nciht per Mail abgefragt
- Absender-Adresse prüfen
  - Angezeigter Name ist nicht der tatsächliche Name
- Link-Adresse kontrollieren
  - Z.B. über Link fahren, aber nicht klicken
- Unbekannte Anhänge nicht öffnen (z.B. Rechnungen)
- Hausverstand!!!

ZILLNER IT SECURITY

SICHERE PASSWÖRTER

GIBT ES ÜBERHAUPT "SICHERE" PASSWÖRTER?

- Anforderungen an ein sicheres Passwort
  - Mindestlänge: 10 Zeichen
  - Komplexität (Kombination aus Groß-, Kleinbuchstaben, Ziffern und Sonderzeichen)
  - Regelmäßiges Ändern der Passwörter
  - Vermeidung von Privatbezug (z.B. Geburtstag)
  - Vermeidung von Wörtern aus dem Wörterbuch
  - Trennung zwischen Provat- und Firmenpasswörter
  - Unterschiedliche Passwörter bei allen Diensten

- Fazit
  - In Regel nicht praxistauglich!
  - Daher Umgang mit Passwörtern meist sehr unsicher

ZILLNER IT SECURITY

ALTERNATIVEN ZU PASSWÖRTERN

2 FAKTOR-AUTHENTIFIZIERUNG

- Was habe ich?
  - Besitz
  - Z.B. Karte, Hardware Token
- Was weiß ich?
  - Wissen
  - Z.B. PIN, Passwort
- Was bin ich?
  - Z.B. Fingerabdruck, Iris

ZILLNER IT SECURITY

WAS ALSO MACHEN?

PRAXISTAUGLICHE LÖSUNGEN

- Passwort Safes
  - Zufällig generierte Passwörter für jeden Dienst
  - Nur ein Masterpasswort
  - Ändern nur im Verdachtsfall
- Wichtige Passwörter immer merken
  - Email Accounts
  - Windowspasswort
  - Online Banking
- Merkhilfen verwenden
  - Sätze bauen und nur Anfangsbuchstaben verwenden
  - Ich esse gerne Schnitzel bei meinem Lieblingslokal im 9.Bezirk!
  - Passwort: IegSbmLi9.B!

ZILLNER IT SECURITY

WIE SCHULE ICH MITARBEITER?

- Seien Sie kreativ!
  - Goodies mit Hinweisen
  - Plakate
  - Workshops
  - Kurse
  - E-Learning
- Praktisch erlerntes bleibt besser hängen als Frontalvorträge!
- Versuchen Sie Verständnis für die eigentliche Problematik zu erlangen

ZILLNER IT SECURITY

WIE SCHÜTZE ICH MEIN UNTERNEHMEN?

ZILLNER
IT SECURITY

KENNEN SIE IHRE RISIKEN?

WAS IST FÜR MEIN UNTERNEHMEN WICHTIG?

- Verfügbarkeit?
  - Welche Daten brauche ich?
  - Wie lange zurück brauche ich Sie?
- Vertraulichkeit?
  - Wer darf meine Daten einsehen?
  - Was machen wenn etwas passiert?
- Integrität?
  - Dürfen meine Daten verfälscht werden?
  - Wie stelle ich die Echtheit sicher?

ZILLNER IT SECURITY

WIE KANN ICH MICH VOR VIREN SCHÜTZEN?

- Virenscanner ist Pflicht!
  - Aber kein Allheilmittel
- Regelmäßig updaten
  - Windows
  - Virenscanner
  - Sonstige Programme (Browser, Office,…)
- Regelmäßige Backups
  - Datenverlust kommt immer unangekündigt
- Alternative Browser nutzen
- Hausverstand!!
  - Keine unbekannten Links / Anhänge öffnen
  - Bei unklaren/komischen Emails einfach nachfragen

ZILLNER IT SECURITY

WIE KANN ICH DATEN AUF MOBILEN GERÄTEN SCHÜTZEN?

- Herausforderungen
  - Mobilität steigt
  - Always on wird standard
  - Vernetzungsgrad steigt
  - Oft einfaches Ziel

- Lösungsansätze
  - Laptopverschlüsselung
  - Smartphones und Tablets verschlüsseln
  - Einrichten von Fernlöschungsmöglichkeiten

ZILLNER IT SECURITY

Bankenaufsicht schlägt Tests gegen Hacker vor

Bild: (c) REUTERS (BOBBY YIP)

Die Behörden sorgen sich nach Attacken um die Sicherheit der Finanzsysteme.

23.06.2016 | 18:17 | (Die Presse)

Brüssel/Washington. Im Kampf gegen Hacker schlagen die Behörden ungewöhnliche Maßnahmen vor. Der oberste europäische Bankenaufseher empfiehlt Stresstests zur Absicherung gegen Hackerangriffe. Die nationalen Regulierer sollten sich stärker mit dem Thema beschäftigen und spezielle Prüfungen erwägen, sagte der Chef der Europäischen Bankenaufsichtsbehörde (EBA), Andrea Enria.

ZILLNER IT SECURITY

ETHICAL HACKING

- Lassen Sie Ihr Unternehmen hacken!
- Mit aktuellen Methoden von Hackern überprüfen wie weit man kommen würde
- Angriffsfläche aus dem Internet im Auge behalten

ZILLNER IT SECURITY

NOTFALLPLÄNE ZUR DATENWIEDERHERSTELLUNG

WAS MACHE ICH GEGEN RANSOMWARE?

ZILLNER IT SECURITY

RANSOMWARE SCHUTZKONZEPTE

- Backups
  - Backups nach dem Pull Verfahren
    - Server holt Daten vom Client
    - Clients können Backup nicht ändern oder löschen
  - Backups außerhalb der Reichweite der Nutzer aufbewahren
  - Mehrere Versionen von Backups vorhalten

- Awareness – Mitarbeitersensibilisierung
  - Erkennung von verseuchten Mails
  - Keine Anhänge öffnen, wenn geringster Zweifel besteht
  - Im Zweifel beim Absender nachfragen

ZILLNER IT SECURITY

RANSOMWARE SCHUTZKONZEPTE

- Makros deaktivieren
- Patch Management
- Aktueller und flächendeckender Virenschutz
  - Email Gateway
  - Unterschiedliche Hersteller
- Browser Plugins nur bei Bedarf
  - Flash deaktiviren, Java,…
  - NoScript als sinnvoller Schutz
- Berechtigungskonzept
  - Zugriff nur auf das notwendige
  - Kein Schreibzugriff auf Backup Ordner
- Benutzerkontensteuerung (UAC) aktivieren
- Verdächtige Aktivitäten melden und untersuchen

ZILLNER IT SECURITY

ZAHLEN ODER NICHT ZAHLEN?

- Keine Garantie für Wiederherstellung
- Grundsätzlich gilt lieber Unterstützung durch Behörden oder private Unternehmen suchen
- Erste Anlaufstelle: Webdienst ID-Ransomware
  - https://id-ransomware.malwarehunterteam.com

ZILLNER IT SECURITY

RANSOMWARE ATTACKERS REFUSE TO DECRYPT HOSPITAL'S FILES AFTER BEING PAID OFF

By **Justin Pot** — May 24, 2016

2 132 Subscribe to this topic

ZILLNER IT SECURITY

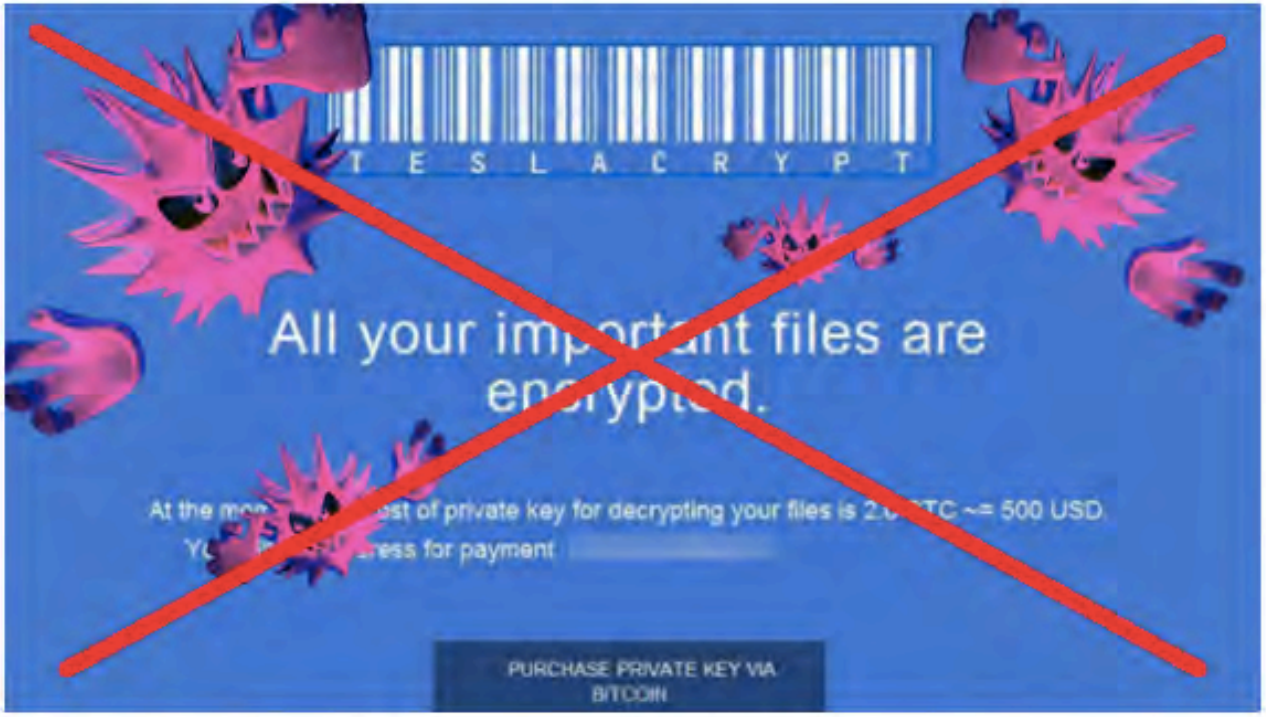
WAS KANN MAN RETTEN?

- Kopie anlegen
  - Niemals am Original arbeiten
- Verschlüsselte Daten aufheben
  - Eventuell in Zukunft knackbar
- Schattenkopien verwenden
- Wiederherstellungspunkte verwenden

ZILLNER IT SECURITY

Erpressungs-Trojaner TeslaCrypt gibt auf: Master-Schlüssel veröffentlicht

19.05.2016 10:44 Uhr – Dennis Schirrmacher vorlesen



Die Drahtzieher hinter TeslaCrypt haben den Stecker gezogen und den Master-Schlüssel in Umlauf gebracht: Opfer der Ransomware können nun ohne Lösegeld zu zahlen wieder Zugriff auf ihre Daten bekommen.

ZILLNER IT SECURITY

SICHERE EMAIL KOMMUNIKATION, PASSWORT MANAGEMENT UND DATENÜBERTRAGUNG IM ALLTAG

EIN AUSFLUG IN DIE PRAXIS

ZILLNER IT SECURITY

ZILLNER IT SECURITY

Kontakt

Tobias Zillner
tobias@zillner.tech
www.zillner.tech
+43 664 8829 8290