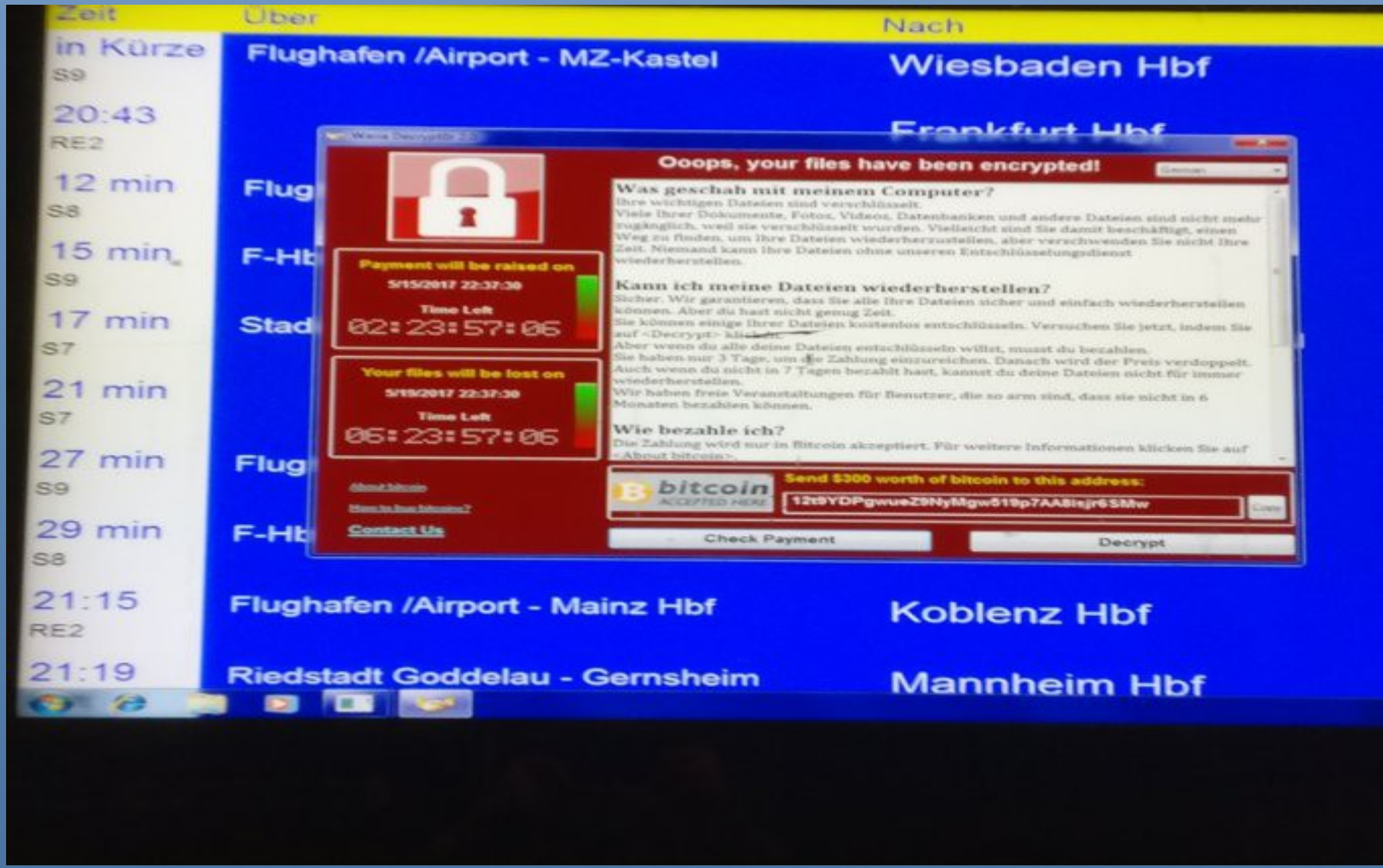
Gängige Angriffe auf den Faktor Mensch

ein Vortrag von Marius Schwarz

im Rahmen des LPD 2017

Ransomware


Zeit
Über
Nach
in Kürze
S9
Flughafen /Airport - MZ-Kastel
Wiesbaden Hbf
20:43
RE2
Frankfurt Hbf
12 min
S8
15 min
S9
17 min
S7
21 min
S7
27 min
S9
29 min
S8
21:15
RE2
Flughafen /Airport - Mainz Hbf
Koblenz Hbf
21:19
Riedstadt Goddelau - Gernsheim
Mannheim Hbf
Ooops, your files have been encrypted!
Was geschah mit meinem Computer?
Kann ich meine Dateien wiederherstellen?
Wie bezahle ich?
Payment will be raised on
5/15/2017 22:37:30
Time Left
02:23:57:06
Your files will be lost on
5/19/2017 22:37:30
Time Left
06:23:57:06
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

Gängige Angriffe auf den Faktor Mensch

„Am häufigsten sitzt das Problem vor dem Monitor.“

Gängige Angriffe auf den Faktor Mensch

Angriff auf menschliche Schwächen:

Phishingmails,
Gewinnversprechen aka. die Nigeria Connection,
Telefonanrufe von Enkeln
Telefonanrufe von falschen Polizisten
Sozialhacking in Firmen

Gängige Angriffe auf den Faktor Mensch

Angriff auf menschliche Schwächen:

Phishingmails,
Gewinnversprechen aka. die Nigeria Connection,
Telefonanrufe von Enkeln
Telefonanrufe von falschen Polizisten
Sozialhacking in Firmen

greifen alle zwei grundlegende menschliche Schwächen an:

Hilfsbereitschaft gegenüber Anderen,

Gängige Angriffe auf den Faktor Mensch

Angriff auf menschliche Schwächen:

Phishingmails,
Gewinnversprechen aka. die Nigeria Connection,
Telefonanrufe von Enkeln
Telefonanrufe von falschen Polizisten
Sozialhacking in Firmen

greifen alle zwei grundlegende menschliche Schwächen an:

Hilfsbereitschaft gegenüber Anderen,
und die reine Habgier.

Gängige Angriffe auf den Faktor Mensch

Schwachstelle : Faktor Mensch

„Die Neugier ist der Katze Tod.“

- Ausführen von Attachments in einer Email
- Anzeigen von gefährlichen Webinhalten ohne Schutzsoftware.
- Schlangenölprodukten aka Antivirensoftware ungeprüft vertrauen
- Installieren von ungeprüften Anwendungen auf dem Handy/PC.
- Einführen von USB Sticks unbekannter Herkunft
- unsichere Passwörter nutzen … „123456“, Geburtsdaten etc.

Gängige Angriffe auf den Faktor Mensch

Gegenmaßnahmen

Die meisten Angriffe auf Menschen kann man durch den Einsatz von gesundem Menschenverstand und Disziplin abwehren.

Gängige Angriffe auf den Faktor Mensch

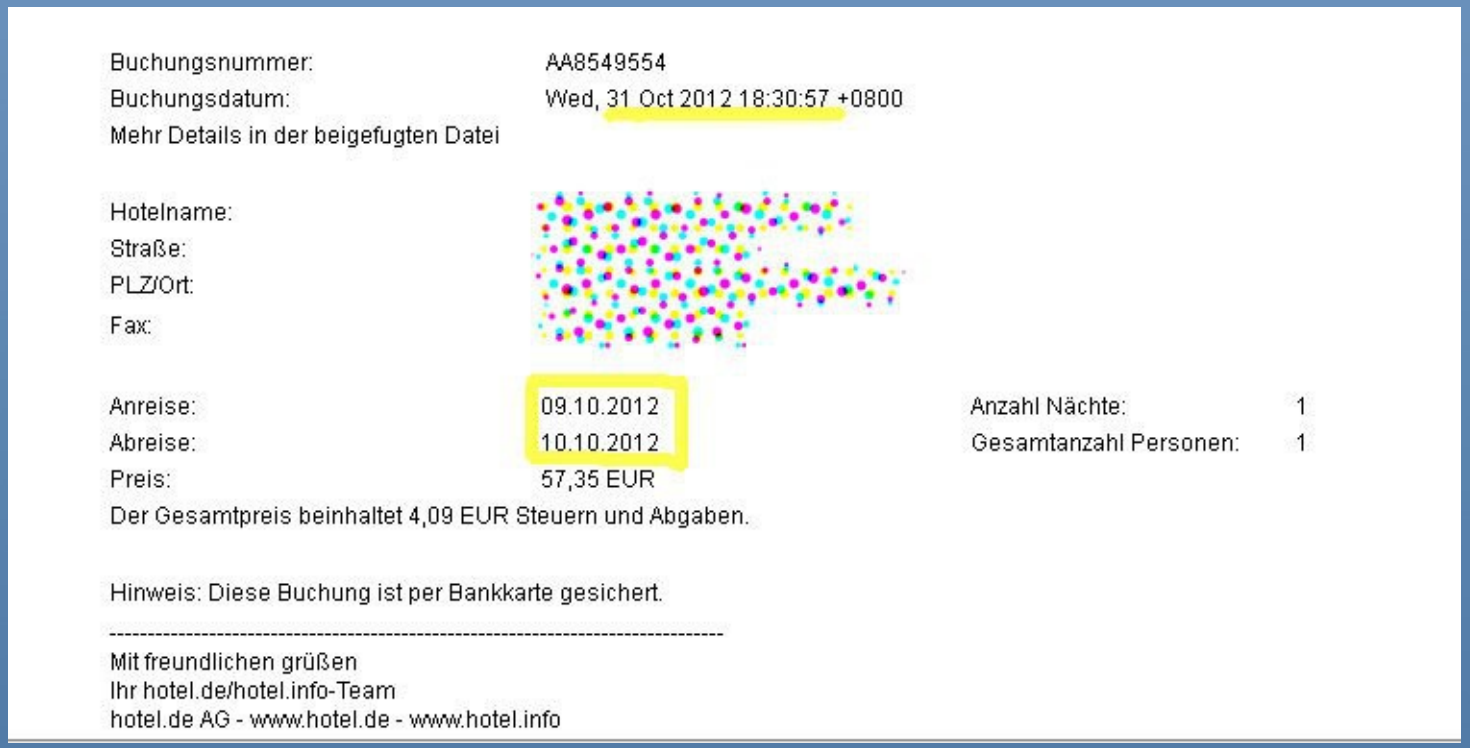
Sozial Spam

„Bitte beachten und verstehen, mein Ziel von e-mailing Sie heute, mein name ist Thomas Wells, Business Relationship Manager bei NatWest Bank plc. London. Ich Fragen Sie Ihre Aufmerksamkeit, um diese Transaktion mit größter Vertraulichkeit.“

Gegenmaßnahme: Einfach löschen.

Gängige Angriffe auf den Faktor Mensch

Verunsicherung, daß etwas zum eigenen Nachteil schief gelaufen ist.



Buchungsnummer: AA8549554
Buchungsdatum: Wed, 31 Oct 2012 18:30:57 +0800
Mehr Details in der beigefugten Datei

Hotelname:
Straße:
PLZ/Ort:
Fax:

Anreise: 09.10.2012
Abreise: 10.10.2012
Preis: 57,35 EUR

Anzahl Nächte: 1
Gesamtanzahl Personen: 1

Der Gesamtpreis beinhaltet 4,09 EUR Steuern und Abgaben.

Hinweis: Diese Buchung ist per Bankkarte gesichert.

Mit freundlichen grüßen
Ihr hotel.de/hotel.info-Team
hotel.de AG - www.hotel.de - www.hotel.info

Gegenmaßnahme: Einfach löschen.

Gängige Angriffe auf den Faktor Mensch

Ausführen von Attachments in einer Email

Gegenmaßnahme: Einfach nicht machen.

Öffnen Sie nur Emailanhänge, die Sie erwarten. Fragen Sie beim vermeindlichen Absender nach, ob er das wirklich geschickt hat.

Einführen von USB Sticks unbekannter Herkunft

Gegenmaßnahme: Einfach nicht machen.

Stecken Sie keine Hardware in Ihren PC, die Sie auf der Straße oder dem Nebentisch im Restaurant gefunden haben. Sie wissen nie, ob der Stick nicht absichtlich platziert wurde.

Gängige Angriffe auf den Faktor Mensch

Anzeigen von gefährlichen Webinhalten ohne Schutzmaßnahmen.

Gegenmaßnahme:

Nutzen Sie Firefox und das Plugin „NoScript“

Vertrauen Sie beim Ausführen von Javascript und Flash nur den Webseiten selbst, aber nie Drittanbieterseiten.

Positiver Nebeneffekt: kaum noch Tracking durch den Webseitenbetreiber möglich.

Gängige Angriffe auf den Faktor Mensch

Installieren von ungeprüften Anwendungen auf dem Handy/PC

Gegenmaßnahme: Einfach nicht machen.

Anwendungen für das Handy, sollte man nur aus sicherer Quelle installieren, z.B. dem Appstore des Anbieters.

Funktioniert die Sicherheitsarchitektur des Handies, kann auch ein Antivirenprogramm nichts finden, womit es überflüssig wird.

Gängige Angriffe auf den Faktor Mensch

Unsichere Passwörter … „123456“

Gegenmaßnahme:

Denken Sie sich einfach ein besseres Passwort aus. Es sollte Groß- und Kleinbuchstaben und Zahlen enthalten und min. 8, besser 12 Stellen lang sein.

Nutzen Sie Eselsbrücken zum Herleiten von Passwörtern.

Gängige Angriffe auf den Faktor Mensch

Eine Warnung aus der Sparte :

„Irgendwelche Hardware an sein Netzwerk anschliessen“

IOT – Internet of Things - Geräte erscheinen vielen Menschen als ein cooles, neues Gerät, daß Ihnen tolle, völlig nutzlose Dinge erlaubt, wie z.b. im Supermarkt daran erinnert werden, daß die Zahnbürste festgestellt hat, daß sie erneuert werden müßte, oder andere Leute ins eigene Haus lassen, wenn man selbst nicht daheim ist.

Sind die zu absoluten Niedrigpreisen produzierten Geräte erst einmal ans heimische Netz angeschlossen, wird der Anwender üblicherweise darauf verzichten, die mitgelieferten Passwörter zu ändern, falls das Geräteinterface überhaupt geschützt ist.

Gegenmaßnahmen: Überlegen Sie vorher, ob Sie das riskieren wollen.

Gängige Angriffe auf den Faktor Mensch

Quellen im Netz zum Nachlesen

https://marius.bloggt-in-braunschweig.de/2013/01/21/sie-sind-wieder-da-lufthansa-und-vodaphone/

www.stern.de/digital/online/internet-betrug-zu-besuch-bei-der-nigeria-connection-543198.html

https://marius.bloggt-in-braunschweig.de/2012/12/16/die-nigeria-connection-stirbt-wohl-nie-aus/

http://www.golem.de/news/thingbot-botnetz-infiziert-kuehlschrank-1401-103978.html