

www.pwc.de

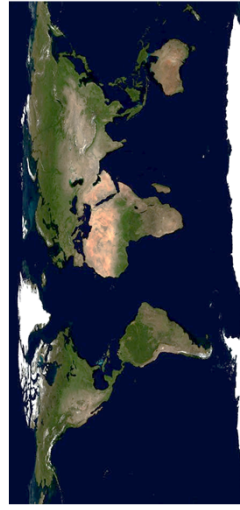
Cybersecurity in der Finanzindustrie



21. September 2018
Mainz

pwc

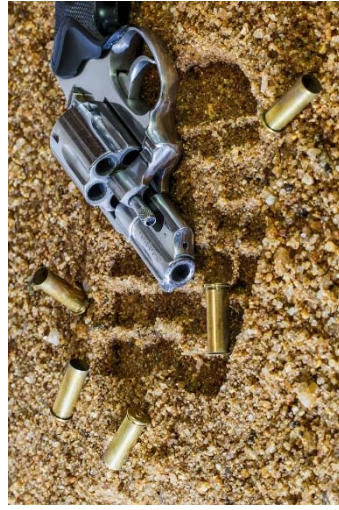
Angreifertypen



Staaten



Haktivisten



Organisierte Kriminalität



Cyber-Terroristen



Insider

Hack the System

Jede Lösung eines Problems ist ein neues Problem. (J.W. von Goethe)





Business Driven Hacking

Eine betriebswirtschaftliche Sicht



Darknet Services

Am Beispiel TDOS (Telephony Denial of Service)



Meistbesucht [Learn more about Tor](#) [The Tor Blog](#) [Hidden Wiki](#) - Tor Wiki... [Seiten-Ladefehler](#) [Mailinator](#)

Suchen

Software & Malware Botnets & Malware **TDOS (Telephony Denial of Service) - ONE HOUR (or ...)**

TDOS (Telephony Denial of Service) - ONE HOUR (or more) CALL FLOOD to any phone number (LANDLINE or MOBILE)

TDOS (Telephony Denial of Service attack): I will FLOOD your LANDLINE phone number target during one hour. If your target pick up the call, my bot will stay on the line until your target hang up or until the time is up. NO WAY TO BLOCK THIS ATTACK because source phone number change on every single call. Even the country source change and sometime the call is private number (no number appear to ...)

Sold by **ameilia75** - f11 sold since Nov 13, 2016 **Vendor Level 5** **Trust Level 5**

Product class	Quantity left	Ends in	Features	Origin country	Ships to	Payment	Features
Digital goods	Unlimited	Never	Bulk Discounts	Worldwide	Worldwide	Escrow	Worldwide
Bulk Discount	From qty 2 to 4	USD 3.77	From qty 2 to 4	0.0037 BTC			Worldwide
Bulk Discount	From qty 5 to 168	USD 2.77	From qty 5 to 168	0.0027 BTC			Escrow

LANDLINE phone number - 1 days - USD +0.00 / item

Purchase price: USD 4.77

Qty: 1

0.0047 BTC / 0.2217 XMR

[Description](#) [Bids](#) [Feedback](#) [Refund Policy](#)

Product Description

TDOS (Telephony Denial of Service attack): I will FLOOD your LANDLINE phone number target during one hour. If your target pick up the call, my bot will stay on the line until your target hang up or until the time is up.

NO WAY TO BLOCK THIS ATTACK because source phone number change on every single call. Even the country source change and sometime the call is private number (no number appear to target).

This price is for one hour call flood (test purpose). Please check bulk discount above for 2 to 4 hours or 5 to more hours! If you order, PLEASE ENCRYPT the target phone number into the international format (using + instead of 00 at the start). Please also inform the date and exact UTC time to start.

IMPORTANT: THIS OFFER IS FOR LANDLINE phone number. If you want to flood a MOBILE phone number, please select MOBILE in the listing above (+ 1.00 USD per hour).

LISTING OPTIONS

- Contact Seller
- Favorite Listing
- Favorite Seller
- Alert when restock
- Report Listing

BROWSE CATEGORIES

- Fraud 39981
- Drugs & Chemicals 216813
- Guides & Tutorials 14137
- Counterfeit Items 8095
- Digital Products 15985
- Jewels & Gold 1630
- Weapons 4017
- Carded Items 3647
- Services 7207
- Other Listings 3567
- Software & Malware 3083
- Security & Hosting 749

SEARCH OPTIONS

Search terms:



Darknet Services

Am Beispiel von Login-Daten zu Bankaccounts

Browser address bar: pwoah7foa6au2pul.onion/listing.php?id=311111 | Suchen

Navigation: Home | Fraud | Accounts & Bank Drops | Bank Drops | HIGH BALANCE DEUTSCHE-BANK.DE LOGINS | Grid

HIGH BALANCE DEUTSCHE-BANK.DE LOGINS

I will provide HIGH QUALITY & HIGH BALANCE Deutsche-bank.de Bank Account Logins, hacked by yours truly. My prices are fair and all my accounts are validated before sale. These accounts are well loved by many customers and cashout is relatively easier with the information provided. This is the format that you will get your Deutsche-bank.de accounts: ===== branch: ac...

Sold by **Artillery** - 0 sold since **Mar 10, 2017** | **Vendor Level 1** | **Trust Level 4**

Product class	Quantity left	Ends in	Features	Origin country	Ships to	Payment	Features
Digital goods	Unlimited	Never	Worldwide	Worldwide	Escrow		

Price list:

- \$76000 - 1 days - USD +140.00 / Item
- \$76000 - 1 days - USD +140.00 / Item
- \$300000 - 1 days - USD +280.00 / Item

Qty: 1 | **Buy Now**

0.0000 BTC / 0.0000 XMR

Buttons: Description | Bids | Feedback | Refund Policy

Product Description

I will provide HIGH QUALITY & HIGH BALANCE Deutsche-bank.de Bank Account Logins, hacked by yours truly. My prices are fair and all my accounts are validated before sale. These accounts are well loved by many customers and cashout is relatively easier with the information provided.

This is the format that you will get your Deutsche-bank.de accounts:
=====

branch:
account:
pin:

LISTING OPTIONS

- Contact Seller
- Favorite Listing
- Favorite Seller
- Alert when restock
- Report Listing

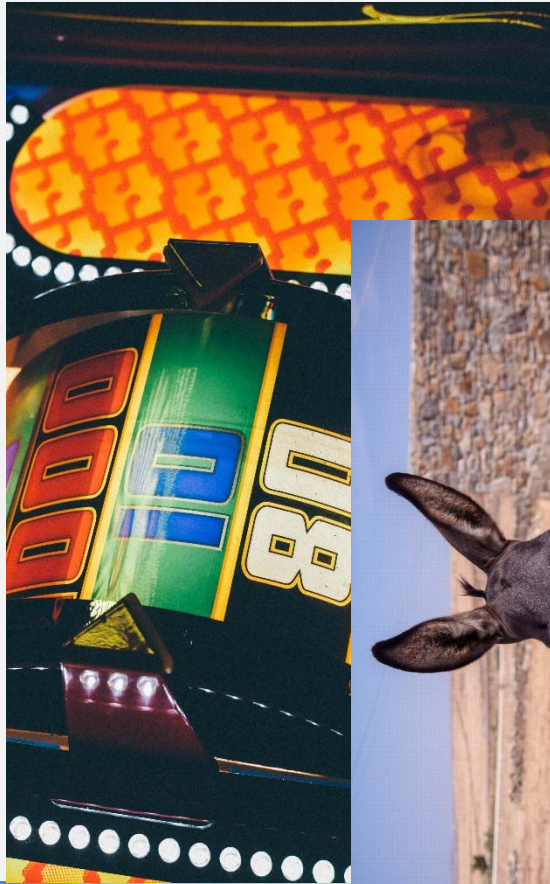
BROWSE CATEGORIES

- Fraud: 39981
- Drugs & Chemicals: 216800
- Guides & Tutorials: 14137
- Counterfeit Items: 8091
- Digital Products: 15983
- Jewels & Gold: 1630
- Weapons: 4016
- Carded Items: 3647
- Services: 7207
- Other Listings: 3566
- Software & Malware: 3083
- Security & Hosting: 749



Wie erhalte ich mein Geld?

Der Übergang von Online zu Offline

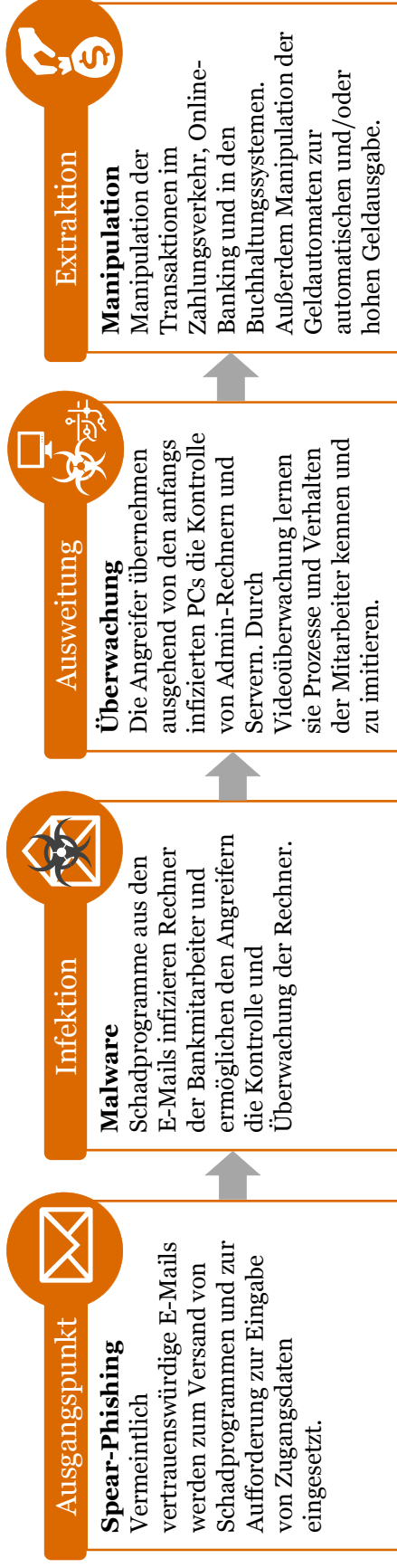




Cyber-Angriffe auf Banken

Beispiel eines modernen Bankraubs durch die „Carbanak“-Gruppe

Seit 2013 entwendete die „Carbanak“-Gruppe bis zu \$ 1 Mrd. durch Hacking

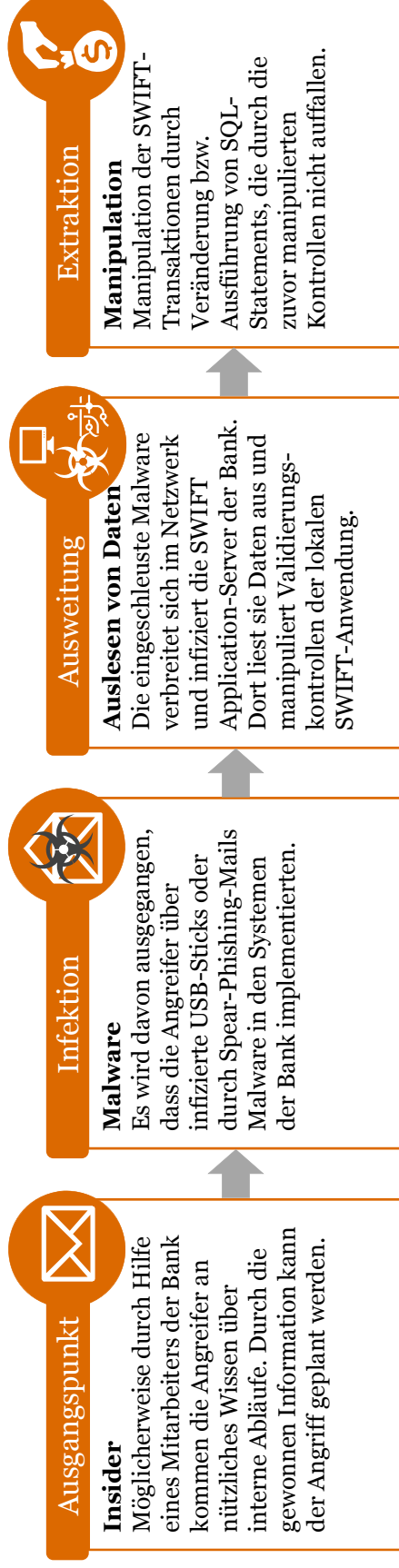




Cyber-Angriffe auf Banken

Beispiel eines modernen Bankraubs mit Hilfe des SWIFT-Netzwerks

Die Angreifer versuchten insgesamt \$ 951 Mio. zu entwenden, \$ 81 Mio. konnten sie erfolgreich stehlen.





Cyber-Angriffe auf Banken

Schutzmaßnahmen



Schutzmaßnahmen

- Multi-Faktor - Authentifizierung
- Moderne Ansätze zum Scanning von E-Mails
- Awareness-Training
- Threat Intelligence

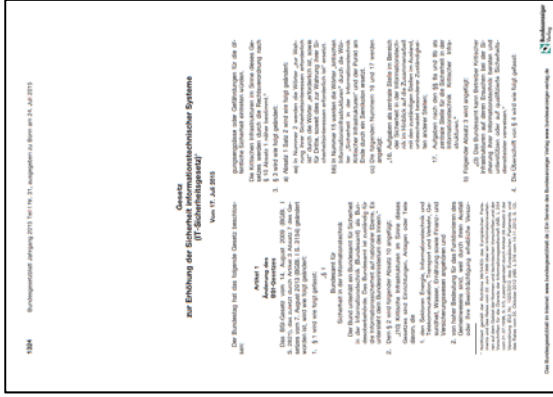
- Patch-Management
- Moderne Security-Software
- Informationsaustausch

- Kontrolle der Systeme und Netzwerke (SIEM)
- Integritätskontrollen für wichtige Dateien (SIEM)
- Netzwerksegmentierung
- Management priv. Berechtigungen und 2FA

- Erhöhter Schutz für „Kronjuwelen“
- Überwachung der Datenbankfehler (SIEM)
- Überwachung der Datenflüsse auf Anomalien

Fazit: Angemessene technische sowie organisatorische Maßnahmen erhöhen die Wahrscheinlichkeit deutlich, solche ausgeklügelten Angriffe erkennen und abwehren zu können.

Gesetzliche & regulatorische Maßnahmen



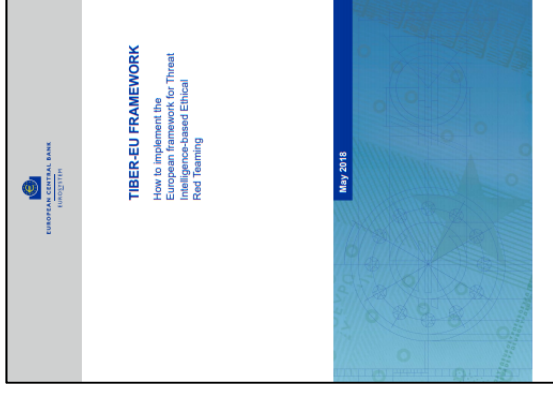
IT-Sicherheitsgesetz



NIST CSF



Datenschutz-Grundverordnung



TIBER-EU Framework



***“Logik bringt dich von A nach B.
Phantasie bringt dich überall hin.”***
(Albert Einstein)

Vielen Dank für die Aufmerksamkeit...



***“Logik bringt dich von A nach B.
Phantasie bringt dich überall hin.”
(Albert Einstein)***

...und weiterhin viel Spaß und spannende Erkenntnisse.

All in this presentation used pictures are under the Creative Commons CCo licence.

Kontakt

*PricewaterhouseCoopers GmbH
Wirtschaftsprüfungsgesellschaft
Friedrich-Ebert-Anlage 35-37
60327 Frankfurt am Main
Telefon: +49 (0)69 9585-3481
Mobil: +49 (0) 170 9445200
klir.thomas@pwc.com*



Thomas Klir
Master of Science (IT Security)