www.pwc.de

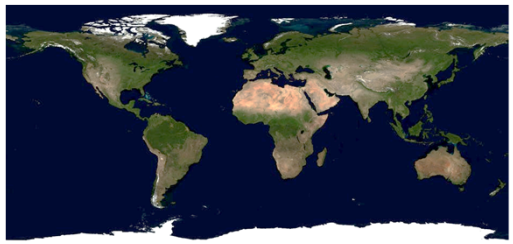
Cybersecurity in der Finanzindustrie

21. September 2018

Mainz

pwc

Angreifertypen

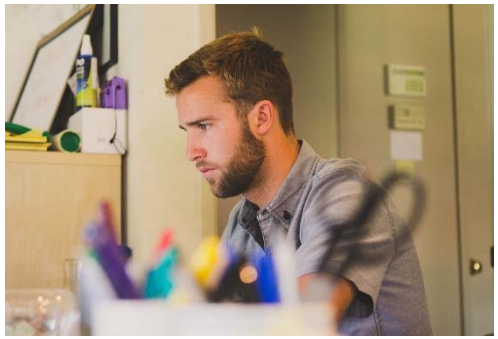


Staaten

Hacktivisten

Organisierte Kriminalität

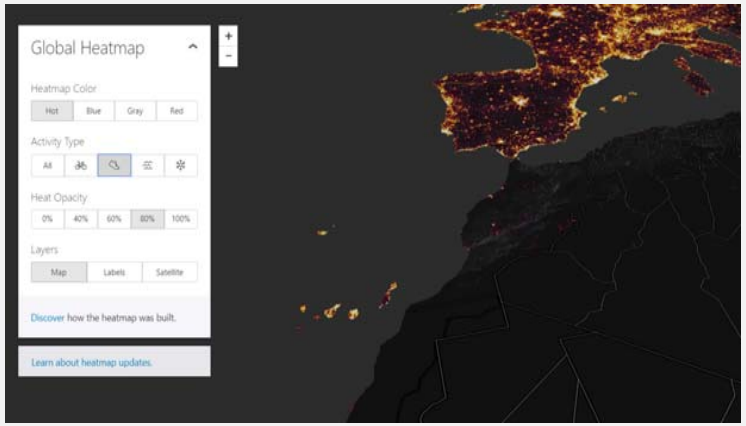
Cyber-Terroristen

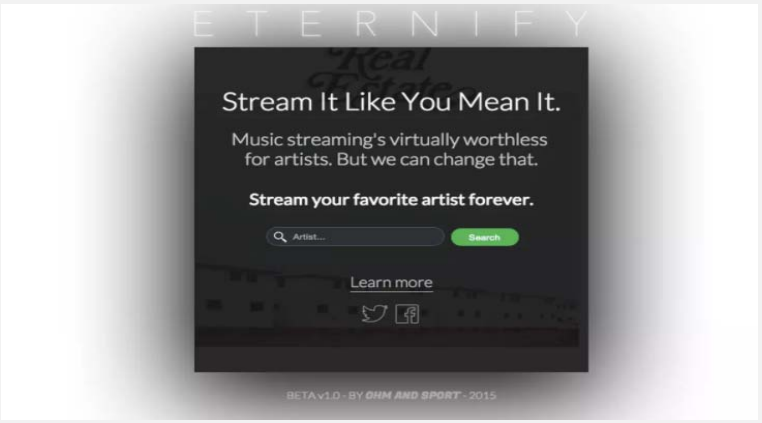


Insider

Hack the System

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

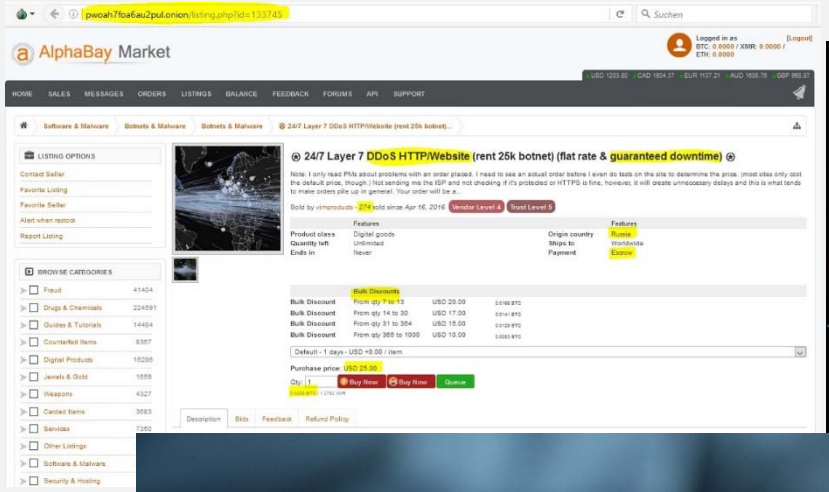


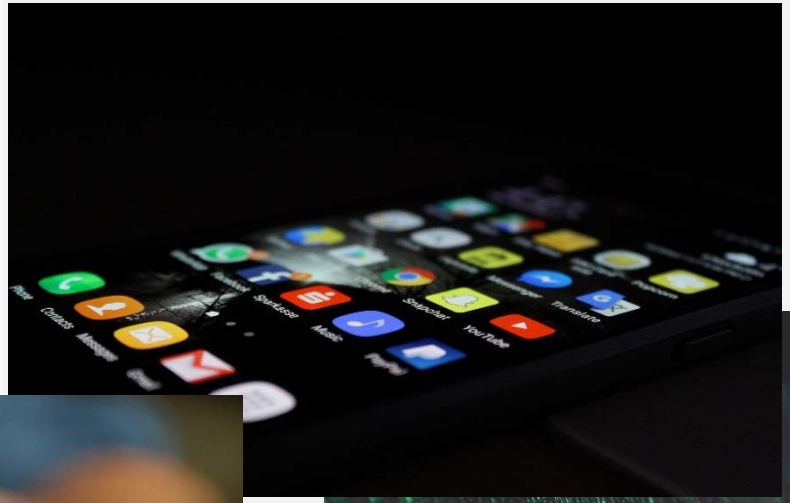


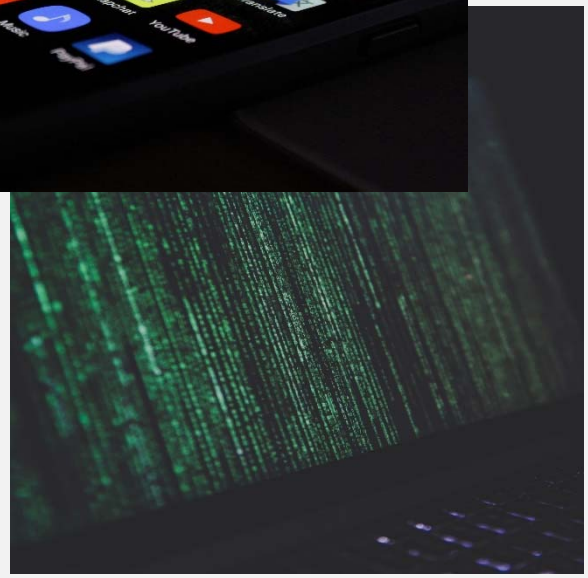
Business Driven Hacking
Eine betriebswirtschaftliche Sicht

Darknet Services

Ein Schlaraffenland für faule Hacker

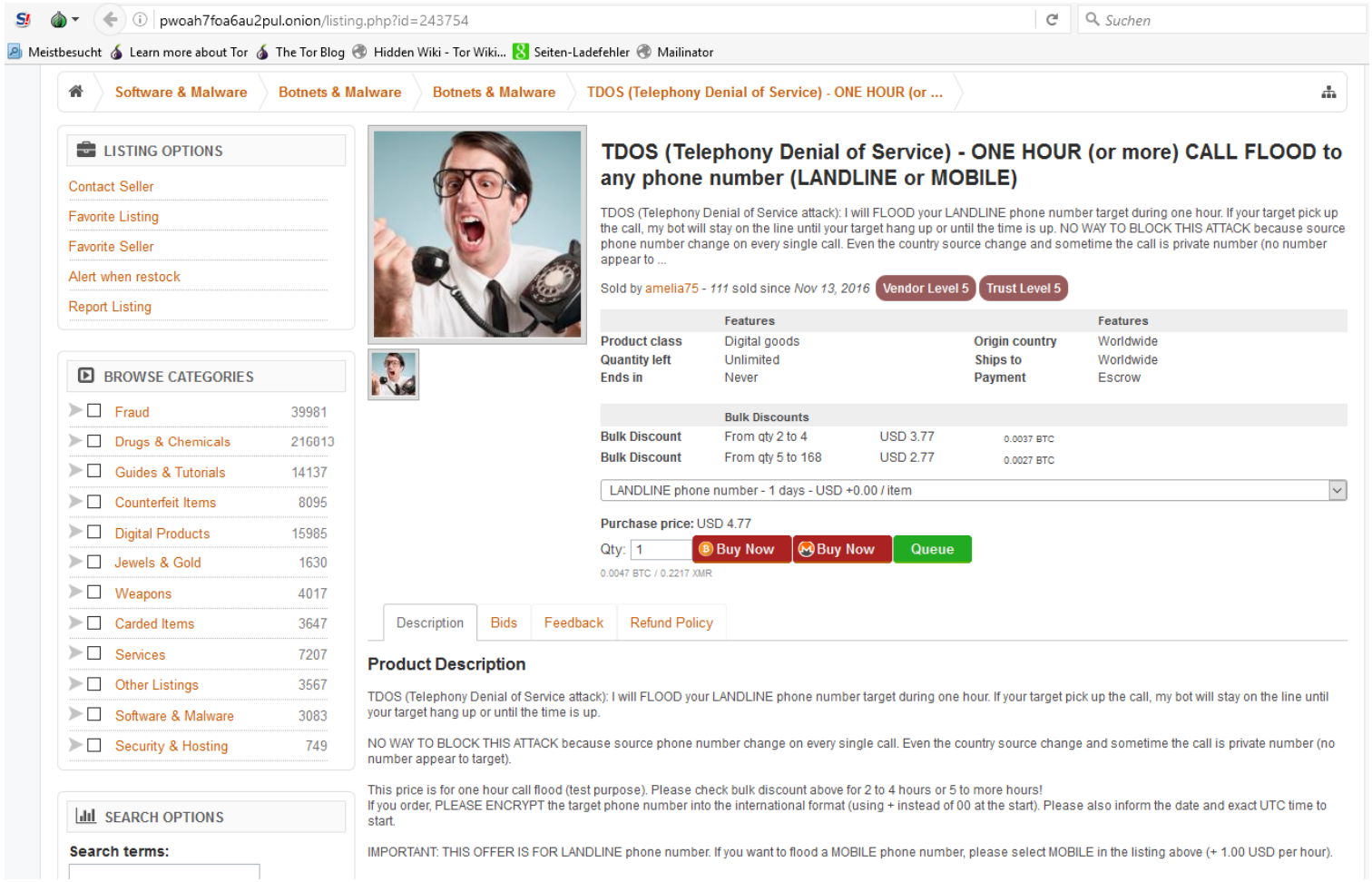






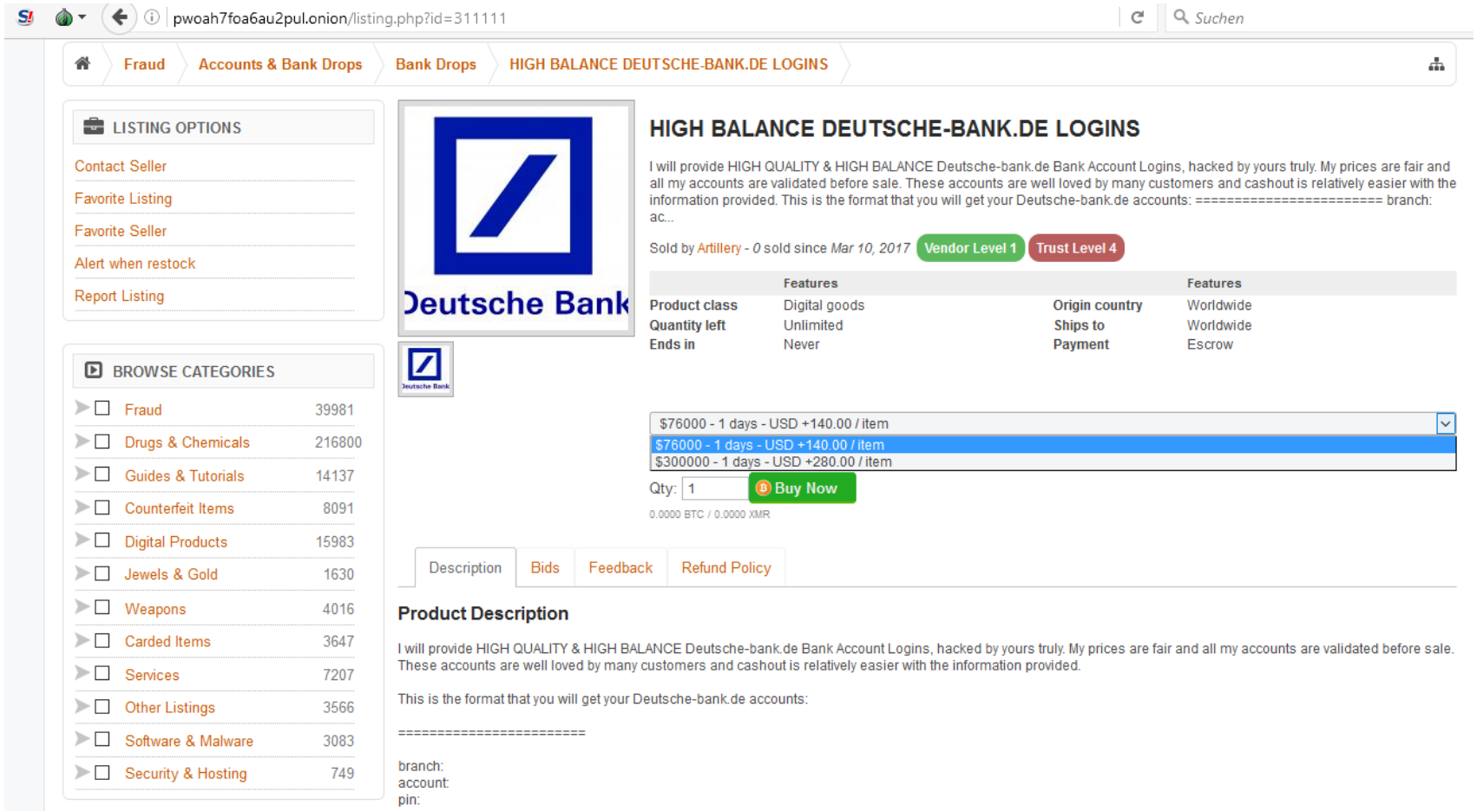
Darknet Services

Am Beispiel TDOS (Telephony Denial of Service)



Darknet Services

Am Beispiel von Login-Daten zu Bankaccounts



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

Ausgangspunkt

Spear-Phishing
Vermeintlich vertrauenswürdige E-Mails werden zum Versand von Schadprogrammen und zur Aufforderung zur Eingabe von Zugangsdaten eingesetzt.

Infektion

Malware
Schadprogramme aus den E-Mails infizieren Rechner der Bankmitarbeiter und ermöglichen den Angreifern die Kontrolle und Überwachung der Rechner.

Ausweitung

Überwachung
Die Angreifer übernehmen ausgehend von den anfangs infizierten PCs die Kontrolle von Admin-Rechnern und Servern. Durch Videoüberwachung lernen sie Prozesse und Verhalten der Mitarbeiter kennen und zu imitieren.

Extraktion

Manipulation
Manipulation der Transaktionen im Zahlungsverkehr, Online-Banking und in den Buchhaltungssystemen. Außerdem Manipulation der Geldautomaten zur automatischen und/oder hohen Geldausgabe.

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.

Ausgangspunkt

Insider
Möglicherweise durch Hilfe eines Mitarbeiters der Bank kommen die Angreifer an nützliches Wissen über interne Abläufe. Durch die gewonnen Information kann der Angriff geplant werden.

Infektion

Malware
Es wird davon ausgegangen, dass die Angreifer über infizierte USB-Sticks oder durch Spear-Phishing-Mails Malware in den Systemen der Bank implementierten.

Ausweitung

Auslesen von Daten
Die eingeschleuste Malware verbreitet sich im Netzwerk und infiziert die SWIFT Application-Server der Bank. Dort liest sie Daten aus und manipuliert Validierungs-kontrollen der lokalen SWIFT-Anwendung.

Extraktion

Manipulation
Manipulation der SWIFT-Transaktionen durch Veränderung bzw. Ausführung von SQL-Statements, die durch die zuvor manipulierten Kontrollen nicht auffallen.

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 Datenbankbefehle (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

Gesetz
zur Erhöhung der Sicherheit informationstechnischer Systeme
(IT-Sicherheitsgesetz)

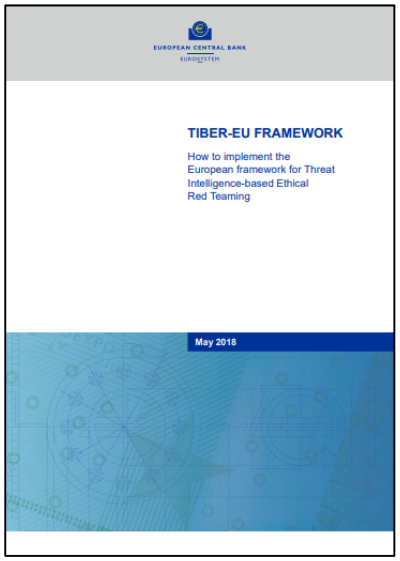
Vom 17. Juli 2015

IT-Sicherheitsgesetz

VERORDNUNGEN

Datenschutz-Grundverordnung

NIST CSF



TIBER-EU Framework

“Logik bringt dich von A nach B. Phantasie bringt dich überall hin.”

(Albert Einstein)

Vielen Dank für die Aufmerksamkeit…

…und weiterhin viel Spaß und spannende Erkenntnisse.

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)