Social Engineering

Dennis Schröder

TÜV Informationstechnik GmbH

IT SICHERHEITSTAG NRW

01. DEZEMBER 2016

WORLD CONFERENCE CENTER BONN

DER FACHKONGRESS FÜR DATEN-, INFORMATIONS- & IT-SICHERHEIT

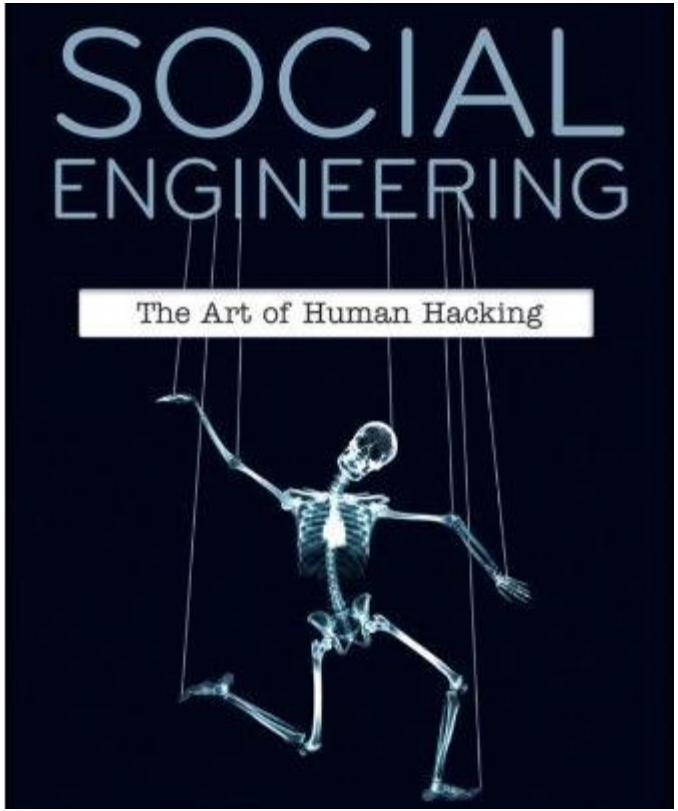
#ITSIHK

TÜVIT®

TÜV NORD GROUP

AGENDA

- Ziele und Motivation
- Exemplarische Angriffskategorien
- Best Practices
- Lessons Learned



Quelle: Buchcover, Social Engineering: The Art of Human Hacking von Christopher Hadnagy

SOCIAL ENGINEERING IN DER PRESSE

NEWS

Investment fund loses $6 million in BEC scam, suspends operations

Victim says fund administrator ignored internal policies and assisted scammers by fixing errors

Credit: iStockphoto

CSO | Sep 19, 2016 3:30 AM PT

MORE LIKE THIS

New tech can help catch spearphishing attacks

The frustrating aftermath of a data breach at American Type Culture Collection

How to keep IT security at the forefront during a merger

on IDG Answers

What is the support life cycle from Google for the Chromebook?

RELATED TOPICS

Security

Data Protection

A lawsuit filed on Friday by Tillage Commodities Fund alleges that SS&C Technology showed an egregious lack of diligence and care, when they fell for an email scam that ultimately led to hackers in China looting $5.9 million.

Quelle:
http://www.csoonline.com/article/3121684/security/investment-fund-loses-6-million-in-bec-scam-suspends-operations.html

SOCIAL ENGINEERING IN DER PRESSE

"Chef-Masche": Kriminelle klauen wohl per Social Engineering 40 Millionen Euro

heise online 16.08.2016 16:45 Uhr vorlesen

Am Ende fehlten auf den Unternehmenskonten 40 Millionen Euro - um diese Summe haben unbekannte Kriminelle jüngst den Autozulieferer Leoni erleichtert. Manches deutet daraufhin, dass auch Leoni Opfer der "Chef-Masche" wurde.

Der Autozulieferer Leoni ist nach eigenen Angaben Opfer eines millionenschweren Betrugs geworden. Unter Verwendung gefälschter Dokumente und Identitäten sowie unter Nutzung

Quelle:
http://www.heise.de/newsticker/meldung/Chef-Masche-Kriminelle-klauen-wohl-per-Social-Engineering-40-Millionen-Euro-3296847.html

SOCIAL ENGINEERING IN DER PRESSE

JAN 15, 2016 @ 09:29 AM 1,145 VIEWS

The Little Black Book of Billionaire Secrets

When Social Engineering Hacked The Director Of National Intelligence

Kalev Leetaru, CONTRIBUTOR

I write about the broad intersection of data and society. FULL BIO

Opinions expressed by Forbes Contributors are their own.

Attendees at the 2015 Black Hat computer security conference Las Vegas. (AP Photo/John Locher)

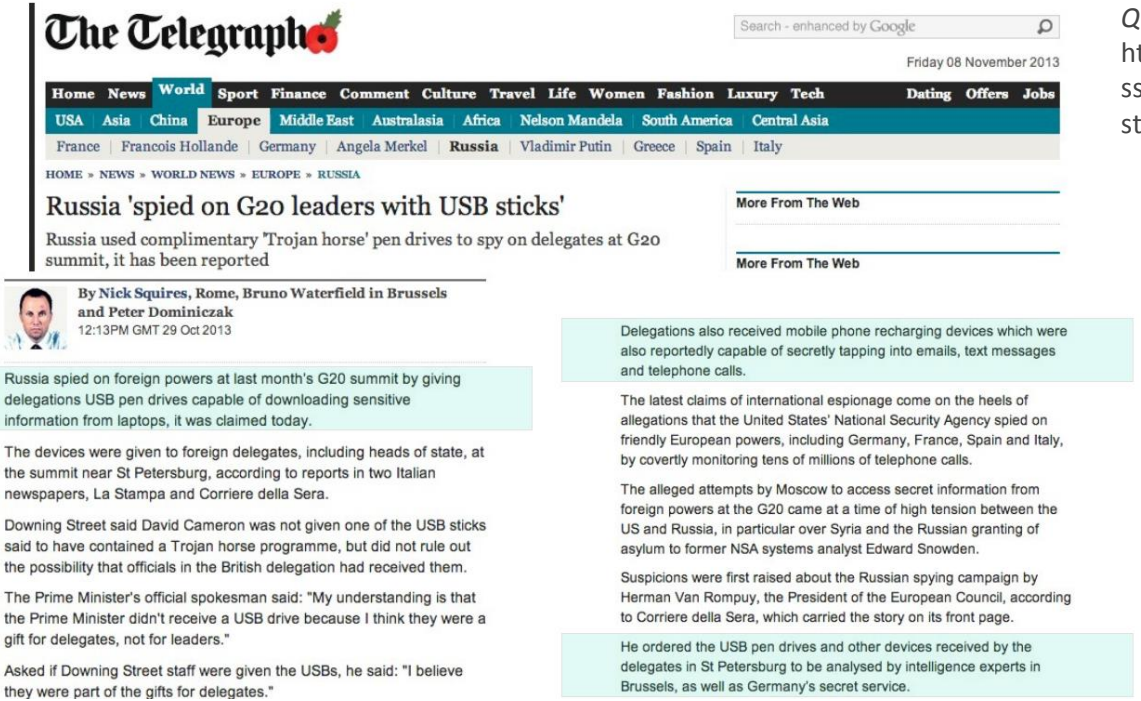
Earlier this week Motherboard reported that the same teenage hacker(s) who hacked into the CIA Director's email last October has been at it again, this time breaching the most senior US intelligence official, the Director of National Intelligence himself, James Clapper. In a world where our most senior intelligence officials are falling victim to computer breaches, what hope is there for the rest of us?

According to the hackers, breaching CIA Director John Brennan's email account last year was a simple act of social engineering. After identifying his ISP as Verizon, they claim to have called Verizon and identified themselves as another Verizon customer support department and eventually received his social security number, which they then turned around and used to request a password reset.

While little is known about how the hackers breached DNI Clapper's accounts, Motherboard suggests that it too was the result of social engineering. The fact that the hackers were able to access not only Clapper's email, but also his wife's email and his home telephone and internet connections

Quelle:
http://www.forbes.com/sites/kalevleetaru/2016/01/15/when-social-engineering-hacked-the-director-of-national-intelligence/#7a2f99d8617e

SOCIAL ENGINEERING IN DER PRESSE



The Telegraph

Search - enhanced by Google

Friday 08 November 2013

Home News World Sport Finance Comment Culture Travel Life Women Fashion Luxury Tech Dating Offers Jobs

USA Asia China Europe Middle East Australasia Africa Nelson Mandela South America Central Asia

France Francois Hollande Germany Angela Merkel Russia Vladimir Putin Greece Spain Italy

HOME » NEWS » WORLD NEWS » EUROPE » RUSSIA

Russia 'spied on G20 leaders with USB sticks'

Russia used complimentary 'Trojan horse' pen drives to spy on delegates at G20 summit, it has been reported

More From The Web

More From The Web

By Nick Squires, Rome, Bruno Waterfield in Brussels and Peter Dominiczak
12:13PM GMT 29 Oct 2013

Russia spied on foreign powers at last month's G20 summit by giving delegations USB pen drives capable of downloading sensitive information from laptops, it was claimed today.

The devices were given to foreign delegates, including heads of state, at the summit near St Petersburg, according to reports in two Italian newspapers, La Stampa and Corriere della Sera.

Downing Street said David Cameron was not given one of the USB sticks said to have contained a Trojan horse programme, but did not rule out the possibility that officials in the British delegation had received them.

The Prime Minister's official spokesman said: "My understanding is that the Prime Minister didn't receive a USB drive because I think they were a gift for delegates, not for leaders."

Asked if Downing Street staff were given the USBs, he said: "I believe they were part of the gifts for delegates."

Delegations also received mobile phone recharging devices which were also reportedly capable of secretly tapping into emails, text messages and telephone calls.

The latest claims of international espionage come on the heels of allegations that the United States' National Security Agency spied on friendly European powers, including Germany, France, Spain and Italy, by covertly monitoring tens of millions of telephone calls.

The alleged attempts by Moscow to access secret information from foreign powers at the G20 came at a time of high tension between the US and Russia, in particular over Syria and the Russian granting of asylum to former NSA systems analyst Edward Snowden.

Suspicions were first raised about the Russian spying campaign by Herman Van Rompuy, the President of the European Council, according to Corriere della Sera, which carried the story on its front page.

He ordered the USB pen drives and other devices received by the delegates in St Petersburg to be analysed by intelligence experts in Brussels, as well as Germany's secret service.

Quelle:
http://www.telegraph.co.uk/news/worldnews/europe/russia/10411473/Russia-spied-on-G20-leaders-with-USB-sticks.html

Quelle: https://www.youtube.com/watch?v=lc7scxvKQOo

DEFINITION

- *„Social Engineering ist eine Methode, um unberechtigten Zugang zu Informationen oder IT- Systemen durch „Aushorchen“ zu erlangen. Beim Social Engineering werden menschliche Eigenschaften wie z.B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität* ausgenutzt.“

Kevin Mitnick

Quelle:
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g00/g00042.html

ZIELE UND MOTIVATION

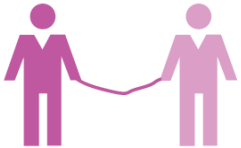
Ziele:

- Nutzt (positive) menschliche Eigenschaften aus.

Zugehörigkeit

Neugierde

Vertrauen



Hilfsbereitschaft

Autorität

- Ziel können Einzelpersonen, Gruppen, Unternehmen sein.

Motivation:

- Finanzielle Gewinne
- Eigeninteresse
- Rache
- Außendruck

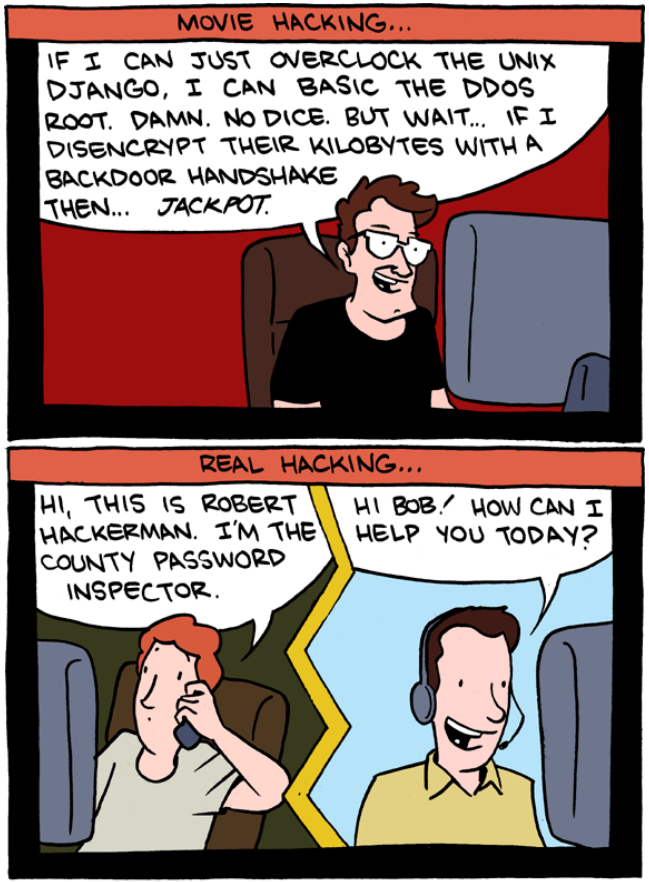
Problem:

- Das Bewusstsein für Angriffe ist niedrig.
- Abwehr nicht einfach und mit großem Aufwand verbunden.

SOCIAL ENGINEERING - KATEGORISIERUNG

Grundlegend zu unterscheiden:

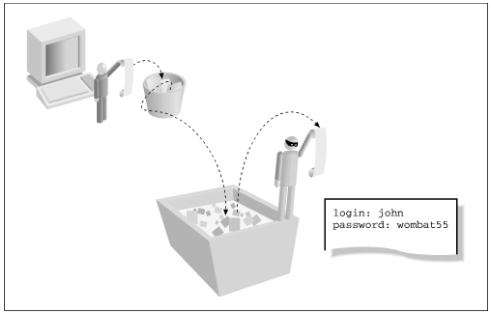
- Passive Angriffe (keine Interaktion mit dem Opfer)
  - Belauschen von Gesprächen
  - Beim Tippen „über die Schulter schauen“ (**shoulder surfing**)
  - Durchsuchen von Papiertonnen (**dumpster diving**)
  - Liegenlassen präparierter USB-Sticks (**baiting**)
- Aktive Angriffe
  - Am Telefon als Mitarbeiter der IT-Abteilung oder guter Bekannter/Assistent des Chefs ausgeben (**pretexting**)
  - Kontaktaufnahme per E-Mail (**phishing**)
  - Internet-Bekanntschaften, z. B. über fingiertes Facebook-Konto



Quelle: http://www.smbc-comics.com/?id=2526

HUMAN-BASED SOCIAL ENGINEERING (1/2)

- **Dumpster Diving**



Quelle: https://hackerstribe.com/

- **Shoulder Surfing**

Quelle: https://secureverifyconnect.info

- **Tailgating**

Quelle: https://commons.wikimedia.org/

HUMAN-BASED SOCIAL ENGINEERING (2/2)

- **Pretexting**
  - Angreifer präsentiert sich als jemand anderen, um private Informationen zu erhalten.
  - z. B. durch Schaffung neuer Identitäten.
  - Der Angreifer benötigt für diesen Angriff gute Informationen.
    - persönliche Informationen der Mitarbeiter
    - Informationen über Dienstleister
    - Freigabemechanismen in dem Unternehmen
- **Quid pro quo**
  - Schokolade gegen Passwort?

- **People Watching**

Quelle: https://de.fotolia.com

COMPUTER-BASED SOCIAL ENGINEERING (1/2)

- **Phishing**
  - Clone phishing — “Update” echter E-Mails
  - Spear phishing — personalisiertes Phishing
  - Whaling — Phishing z. B. gegen hochrangigen Mitarbeiter
  - Vishing — Voice Phishing; Ziel: Opfer ruft Angreifer an
  - Evil Twins — z. B. rogue WiFi access points

Quelle: http://www.telewerkstatt.at/Bilder/Insider/11_phishing/db01.htm

COMPUTER-BASED SOCIAL ENGINEERING (2/2)

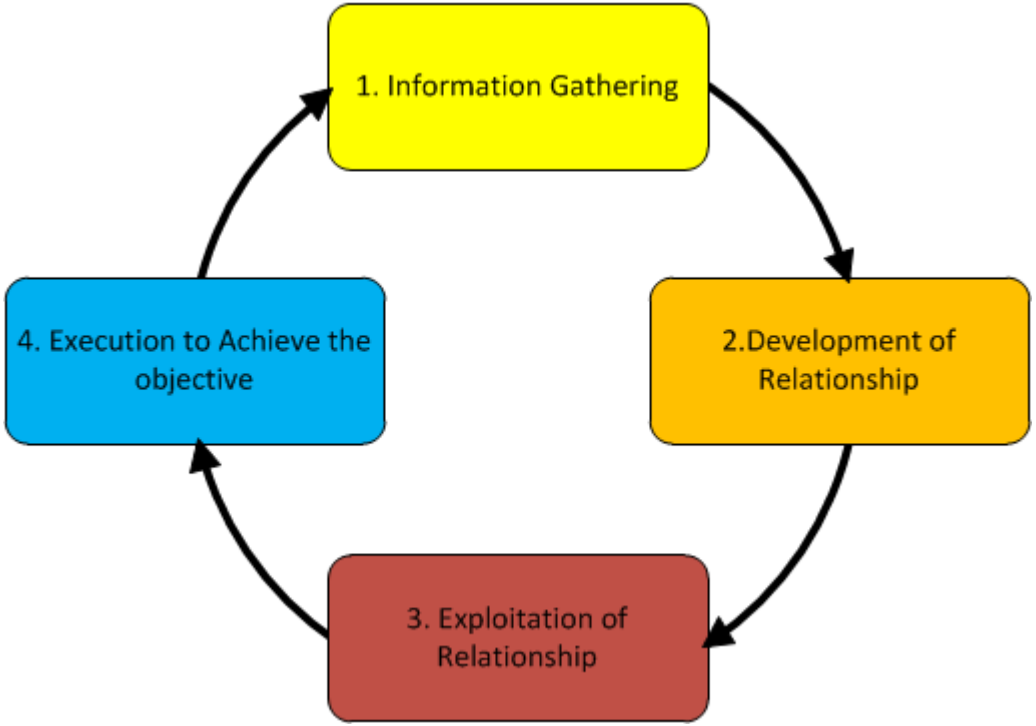
- **Baiting**

Quelle: https://www.zentralesfundbuero.com/assets/img/bildmaterial/geldbeutel_usb_stick_verloren.jpg

- **Forensic analysis** “Dumpster diving” für Elektronik

- **Electronic badges** Duplizieren elektronischer Schlüssel

DER ANGRIFFS KREISLAUF



SOCIAL ENGINEERING IM KONTEXT DES BSI

- „Social Engineering und Phishing“ steht an erster Stelle der ICS Top 10 Bedrohungen vom BSI.

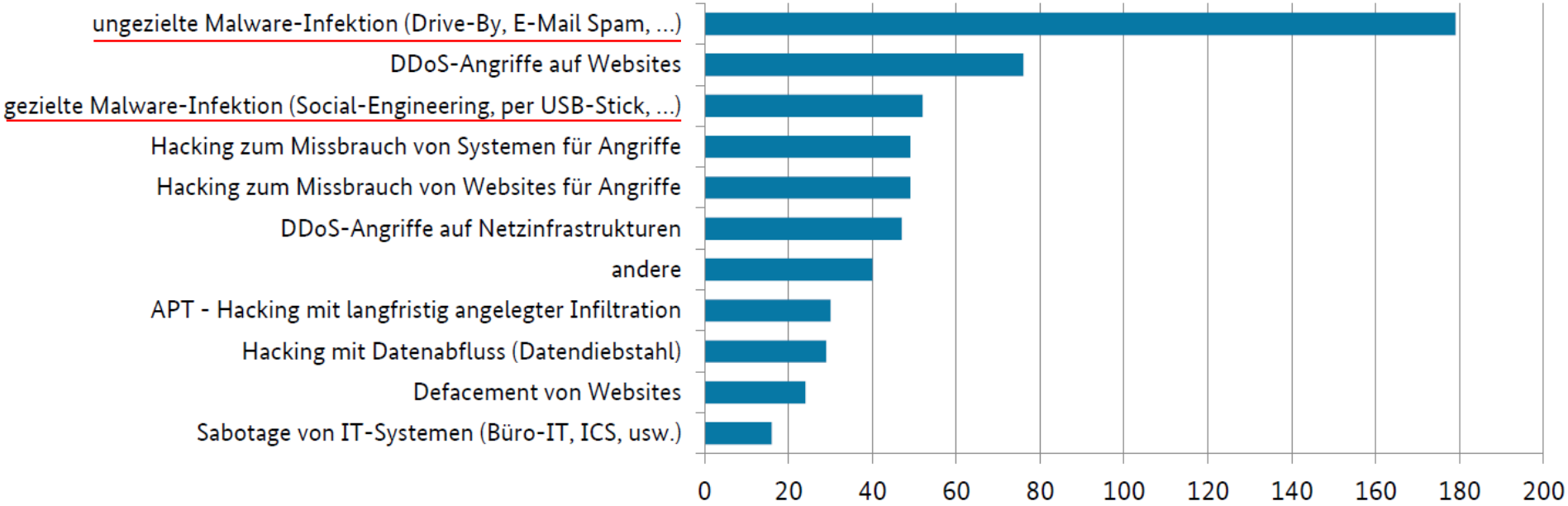
- Zur Bewertung der Bedrohung können die folgenden Kriterien angewandt werden:
  - Verbreitung: Wie verbreitet ist die potenzielle Schwachstelle in Unternehmen?
  - Exposition: Wie leicht ist die Schwachstelle zu lokalisieren und zu erreichen?
  - Ausnutzbarkeit: Wie einfach ist es, die Schwachstelle auszunutzen?
  - Detektion: Wie einfach ist es, eine Kompromittierung zu bemerken?

- Die Bewertungskriterien für Social Enigneering vom BSI:

Verbreitung	Exposition	Ausnutzbarkeit	Detektion
HÄUFIG (3)	HOCH (3)	EINFACH (3)	MODERAT (2)

WELCHER ART WAREN DIE 2014/2015 FESTGESTELLTEN ANGRIFFE?

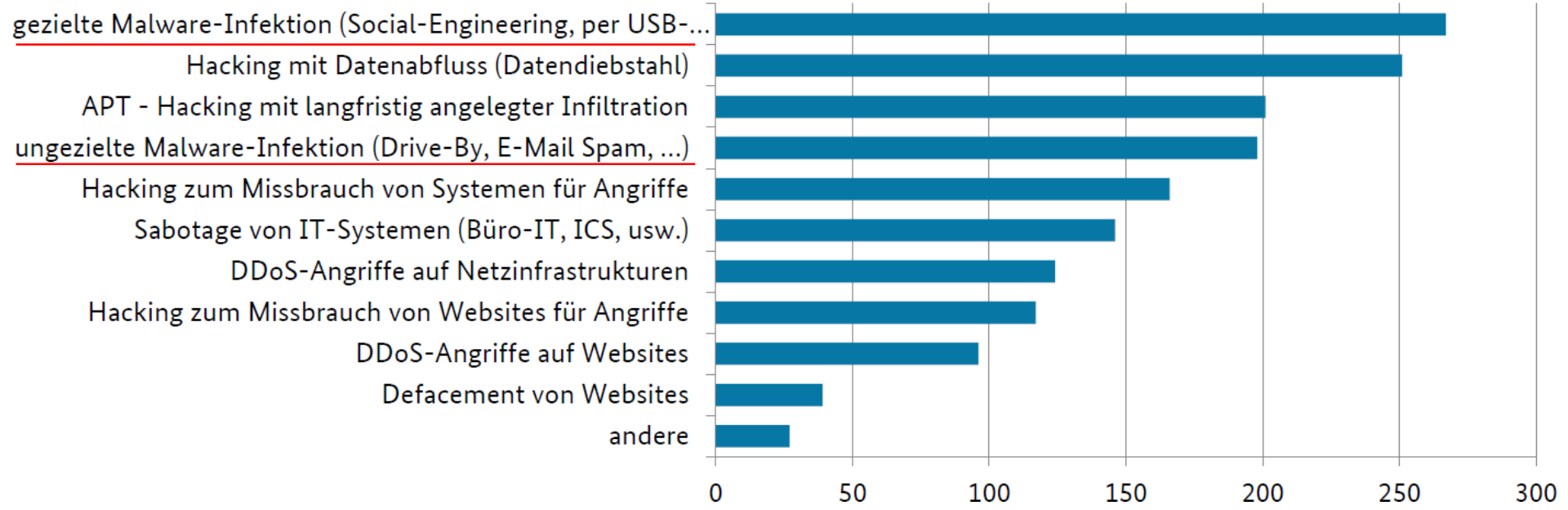
Von 248 Befragten gaben ... folgende Arten von Angriffen an



Quelle: BSI (Cyber-Sicherheits-Umfrage 2015)

WELCHEN ARTEN VON CYBER-ANGRIFFEN MESSEN DIE BEFRAGTEN FÜR DIE KOMMENDEN 2 JAHRE DAS GRÖßTE BEDROHUNGSPOTENTIAL BEI?

Von 424 Befragten gaben jeweils ... an



Quelle: BSI (Cyber-Sicherheits-Umfrage 2015)

GEGENMAßNAHMEN

1. Zielgruppenspezifisches Security-Awarenesstraining.
2. Organisatorische Maßnahmen: Erstellung und Durchsetzung von Sicherheitsrichtlinien.
   a) Informationen, die für das Unternehmen einen Wert aufweisen, identifizieren und klassifizieren.
   b) Etablieren eines Datensicherungskonzeptes.
   c) Einführen von Verschwiegenheits- und/oder Datenschutzerklärungen für Mitarbeiter/Partner/Dienstleister.
   d) Richtlinien für das Vernichten von auf Papier gedruckten Informationen (z. B. Schreddern).
   e) Sichere Entsorgung von digitalen Datenträgern.
   f) Regelungen für den Umgang mit mobilen Geräten (Sichtschutzfolie, Aufbewahrung in einem Safe, usw.).
3. Etablieren von Alarmierungswegen bei Vorfällen und auch bereits bei Verdacht.
4. Nutzung von technischen Sicherheitsmechanismen zur Durchsetzung der geltenden Regelungen und zur automatischen Erkennung von Fehlverhalten oder Angriffen (z. B. Device Control oder Zutrittskontrolle).
5. Regelmäßige Datensicherungen zur Wiederherstellung von Daten und Anwendungen

Vielen Dank für Ihre Aufmerksamkeit!

Ihr Ansprechpartner

Dennis Schröder, M.Sc.

Product Manager Cyber Security Services
IT Security
Business Security & Privacy

+49 201 8999-606
+49 160 8885-606
d.schroeder@tuvit.de

TÜV NORD GROUP