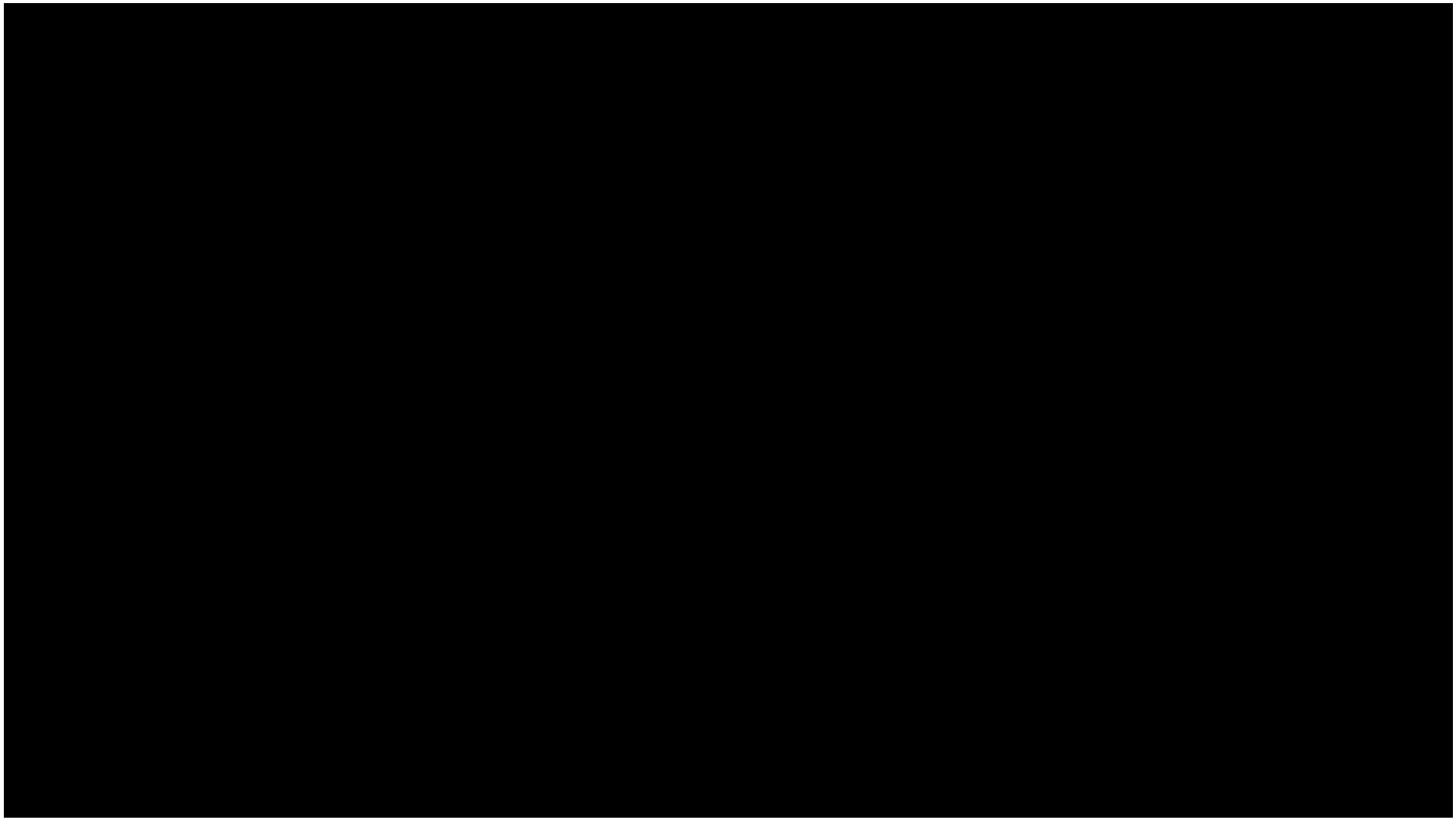
IT Security
The state of the onion...

Security-Herausforderungen in Industrie 4.0 und IoT

13.10.2016

Thomas Bleier • t@b-sec.net • +43 664 3400559

Das Problem



Die Herausforderung

Die Komplexität der IT-Systeme steigt ständig

- Mondlandung mit 7.500 Lines of Code
- Heute: Boeing 787: 6,5 Mio; Mercedes S: 20 Mio; Chevrolet Volt: 100 Mio.

Mehr Schwachstellen

Systeme werden immer mehr vernetzt

- Internet-of-Things, Industrie 4.0, M2M, V2X, etc.
- Virtuelle Infrastrukturen (Cloud, etc.)

Höheres Risiko

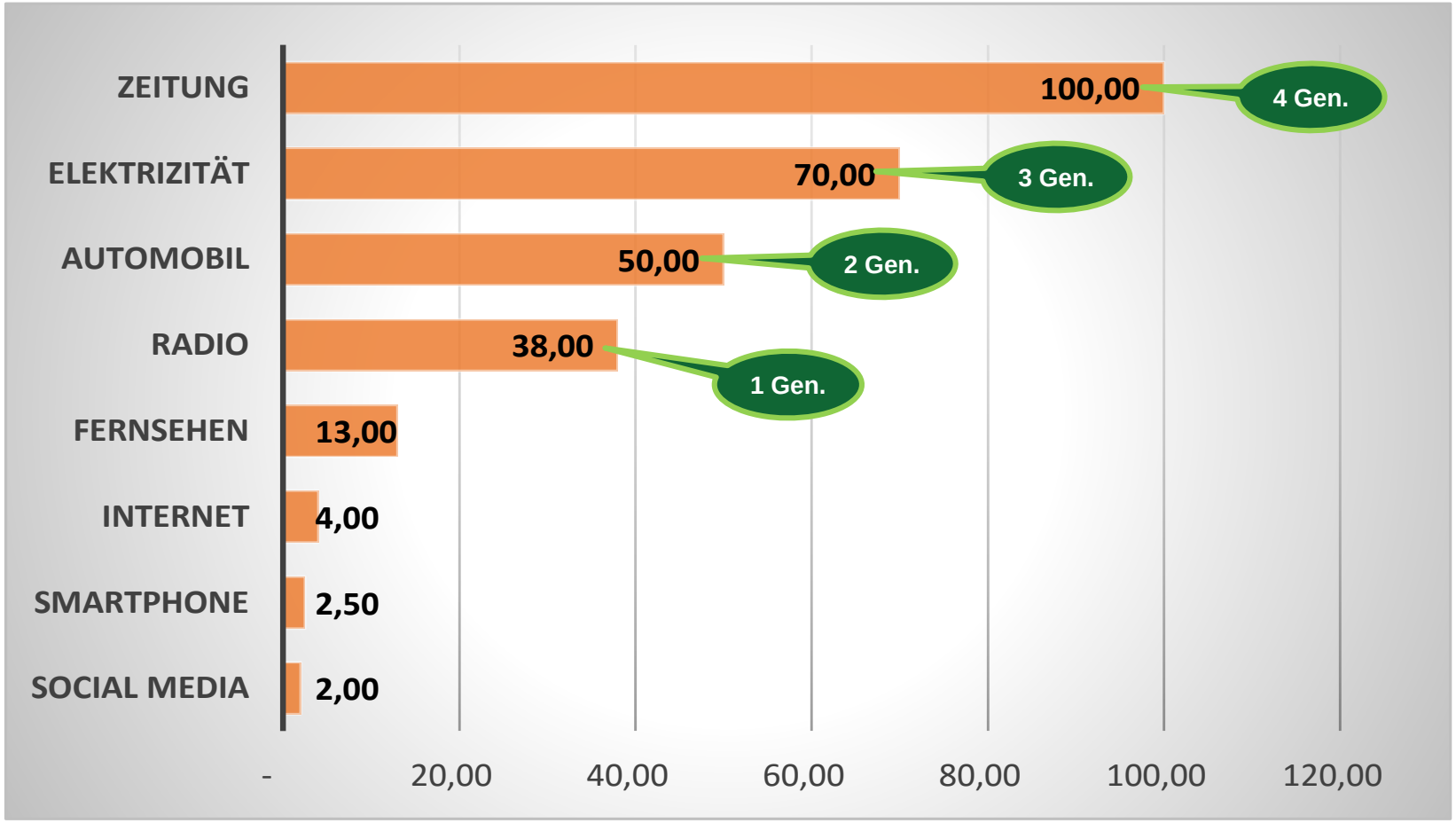
Abhängigkeit von den IT-Systemen steigt

- Smart Grid, Smart Home, Smart City, Smart Phone
- eGovernment, eCommerce, eHealth, eMobility

Größere Auswirkungen

50 Millionen Benutzer

Wie lange hat es gedauert, bis 50 Millionen Benutzer eine Technologie verwendeten?



Quellen: Joseph Webb: Disrupting the Future, 2010, http://thenextweb.com/google/2011/07/22/google-reached-10m-users-in-16-days-want-to-know-how-long-it-took-facebook-and-twitter/, Wikipedia (iPhone), http://spectrum.ieee.org/energy/policy/electrifying-society

Security und Technologie-Akzeptanz

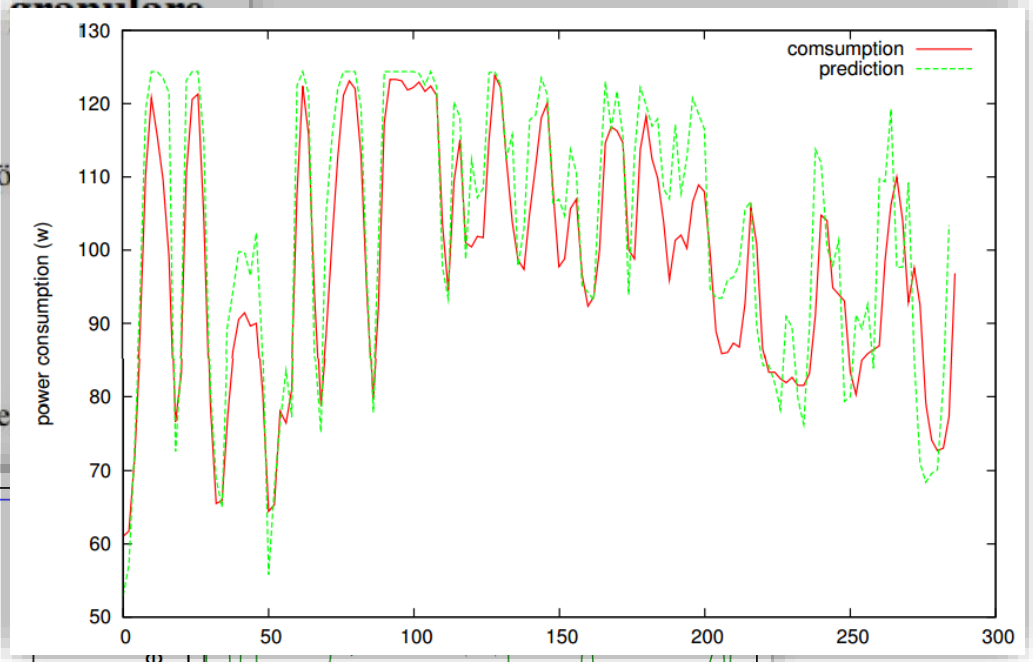
Beispiel: Datenschutz im Smart Metering

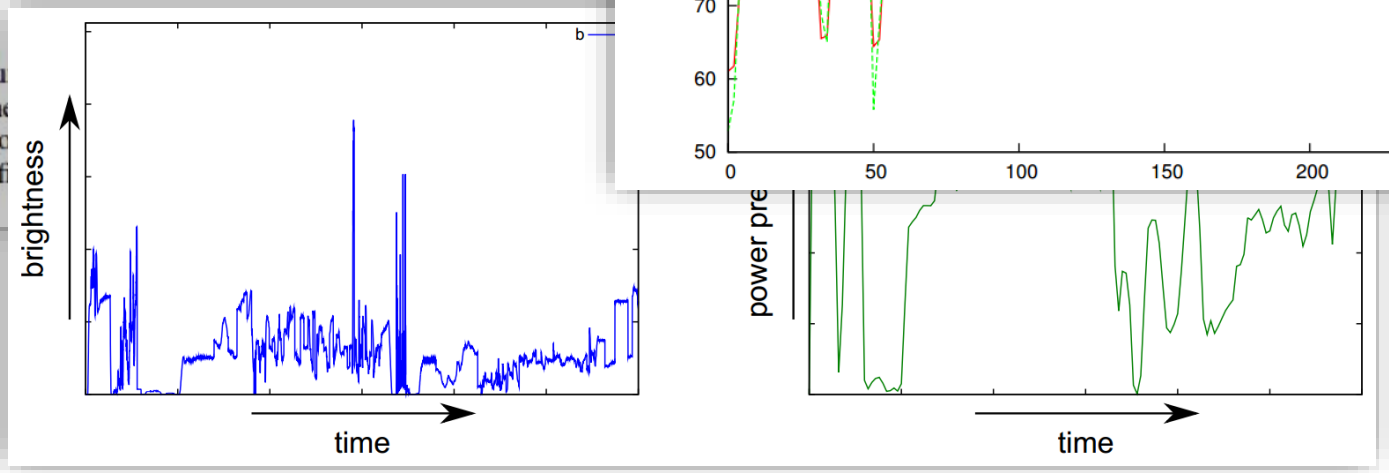
Identifikation von Videoinhalten über
Stromverbrauchsdaten*

Ulrich Greveler, Benjamin Justus, Dennis Lö

Labor für IT-Sicherheit
Fachhochschule Münster
Stegerwaldstraße 39
48565 Steinfurt
{greveler|benjamin.justus|loehr}@fh-muenste

Abstract: Seku
einen erhebliche
rechtliche Gebo
laren Messhäufi
entgegen.



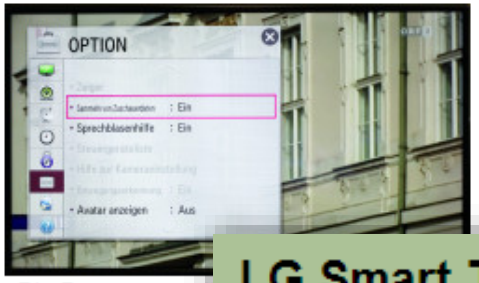


Was wirklich geschah…

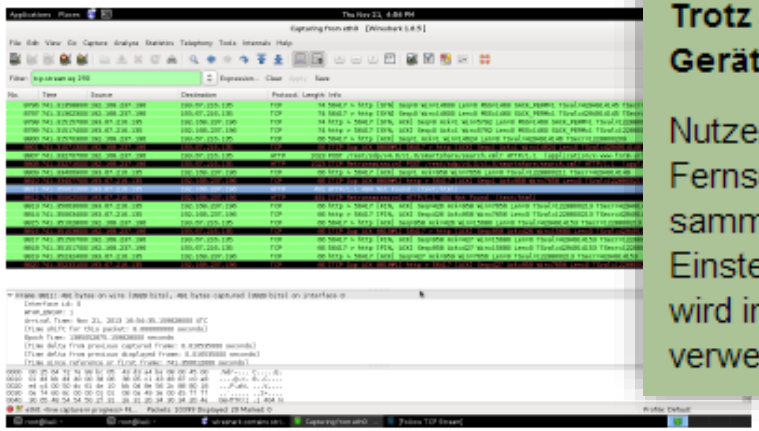
LG Smart-TVs spähen Nutzer aus

vorlesen / MP3-Download

Der Verdacht, dass bestimmte Smart-TVs von LG Daten über ihre Nutzer ausspähen und unverschlüsselt an das Unternehmen senden, hat sich bestätigt: LG hat auf Anfrage von heise online eingeräumt, dass einige ihrer Geräte sowohl Informationen über Dateien auf angeschlossenen USB-Speichern abgreifen als auch gegen den Willen der Nutzer das Sehverhalten erfassen und weitersenden. Das Unternehmen kündigte ein Firmware-Update an, das die Probleme korrigieren soll. Dabei ist noch offen, welche Modelle im einzelnen betroffen sind.



Die Datensammelf
aktiviert. Deaktivie
Fernseher trot



Smart-TVs von LG senden unverschlüsselt Nutzerdaten an einen Server des Herstellers.

LG Smart TVs zeichnen unerlaubt Fernsehverhalten auf

20. November 2013, 08:58

Trotz strikter Privatsphäre-Einstellung speichert das Gerät die Daten und schickt sie unverschlüsselt weiter

Nutzer von LGs Smart TVs berichten, dass die Geräte das Fernsehverhalten der Nutzer aufzeichnen und Daten sammeln, auch wenn die dazugehörige Privatsphäre-Einstellung deaktiviert wurde. Die Aufzeichnung der Daten wird im Normalfall laut LG für verbesserte Werbeanzeigen verwendet.

Die Motivation für Angriffe ändert sich

Cracker/Script Kiddies

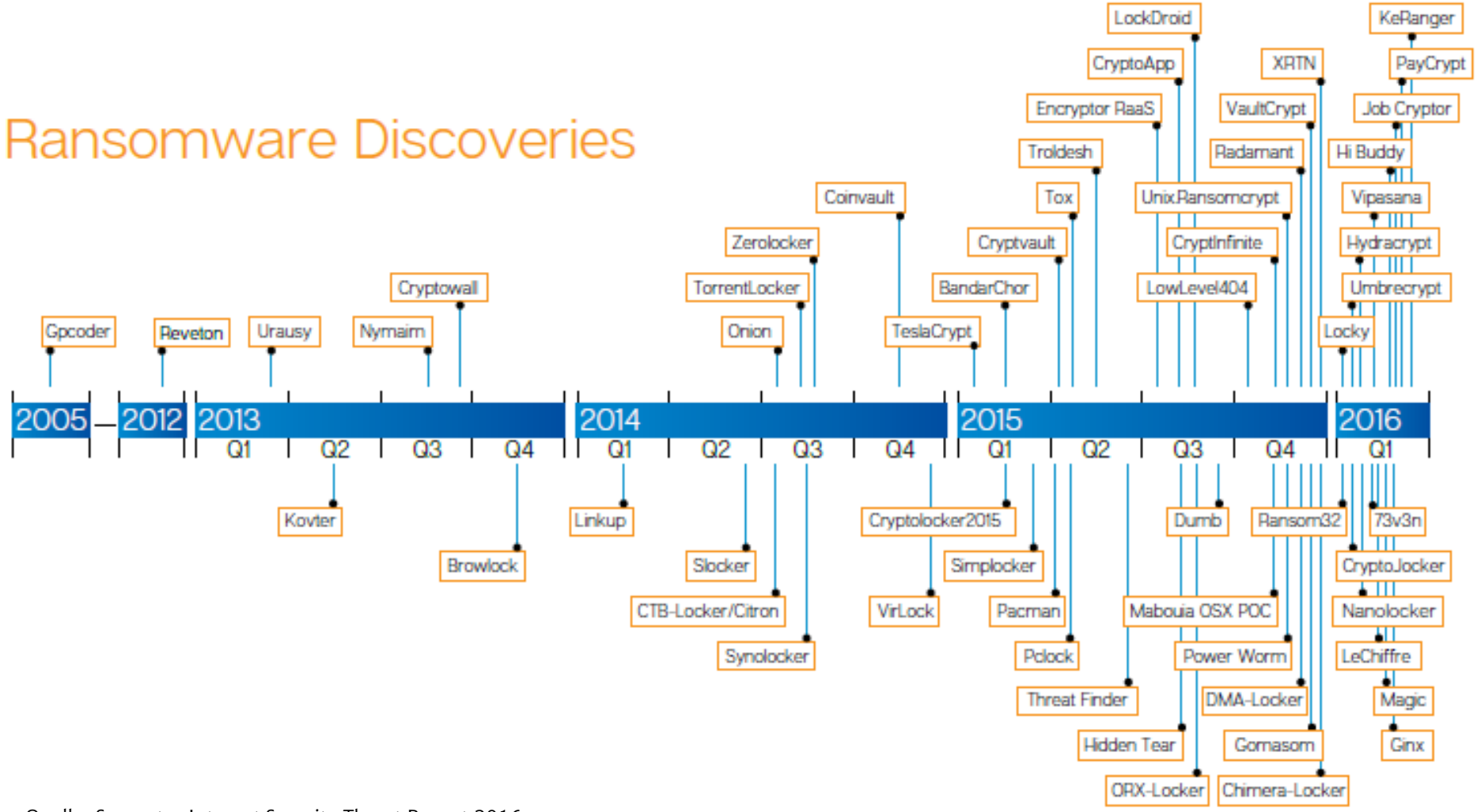
Cybercrime

„State-sponsored Attacks“

Ideen für Hacking finden sich immer wo ein Markt verfügbar ist

Technologisch gesehen sind die Werkzeuge im Prinzip die gleichen

Cybercrime - Ransomware



Quelle: Symantec Internet Security Threat Report 2016

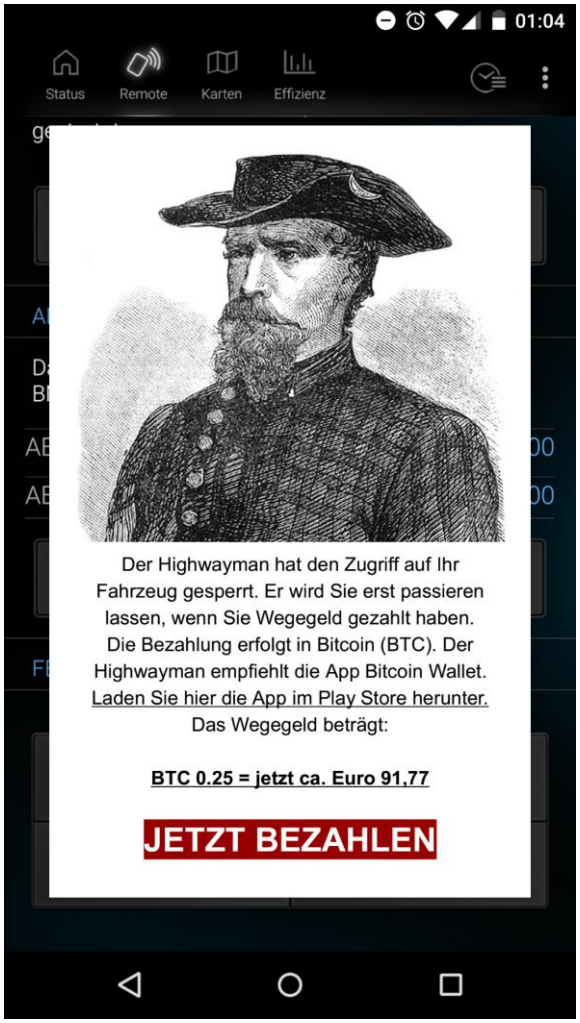
Die Zukunft der Ransomware?

Erpressungstrojaner "Highwayman" zielt auf Autofahrer

01.04.2016 04:01 Uhr – Jan Schüßler vorlesen

"Highwayman" lässt das Auto erst nach Lösegeldzahlung öffnen. Da lacht der grüne Mülleimer... nicht.

Wegelagerei 2.0: Die Keyless-Go-Apps einiger Autohersteller sind mit einem Erpressungstrojaner verseucht. Wer sein Auto gerne per App öffnet, erlebt eine böse Überraschung.



http://www.heise.de/security/meldung/Erpressungstrojaner-Highwayman-zielt-auf-Autofahrer-3158438.html

Cyberangriffe haben reale Auswirkungen

SPIEGEL ONLINE DER SPIEGEL SPIEGEL TV

NETZWELT Schlagzeilen | Wetter | DAX 10.490,86 | TV-P

Nachrichten > Netzwelt > Web > Computersicherheit > BSI-Bericht: Hacker legten deutschen Hochofen lahm

BSI-Sicherheitsbericht

Hacker legten deutschen Hochofen lahm

Der Sicherheitsbericht des IT-Bundesamts zeichnet ein düsteres Bild: Computerkriminelle werde professioneller, besonders betroffen sind alte Windows- und Android-Versionen. Sogar ein Stahlv zum Hacker-Ziel.

Arbeiter am Hochofen (Archivbild): "Massive Beschädigungen" durch Hacker

BBC Sign in News Sport Weather Shop Earth Travel M

NEWS

Home Video World UK Business Tech Science Magazine Entertainment & Arts

Technology

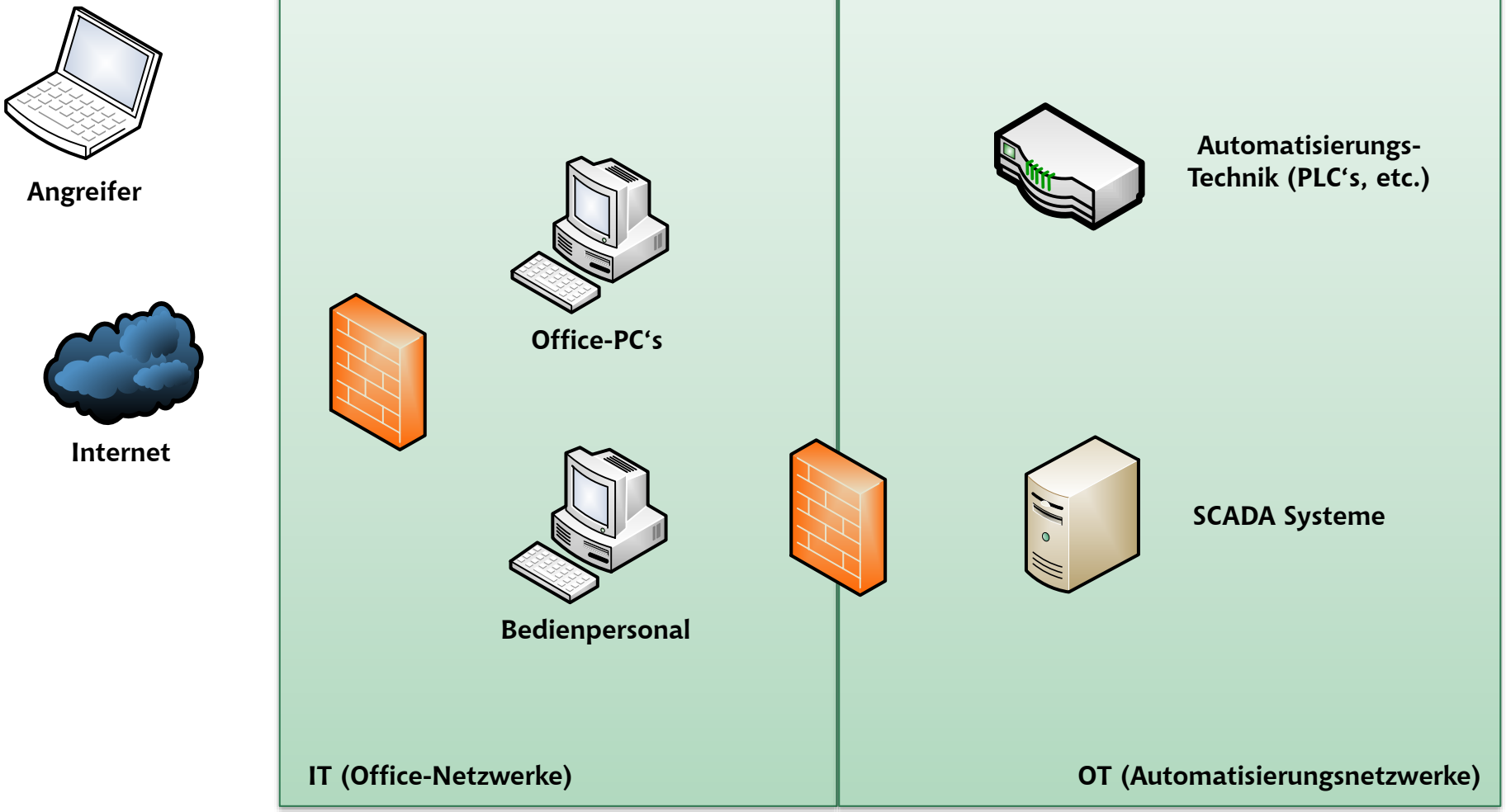
Hackers caused power cut in western Ukraine - US

12 January 2016 | Technology Share

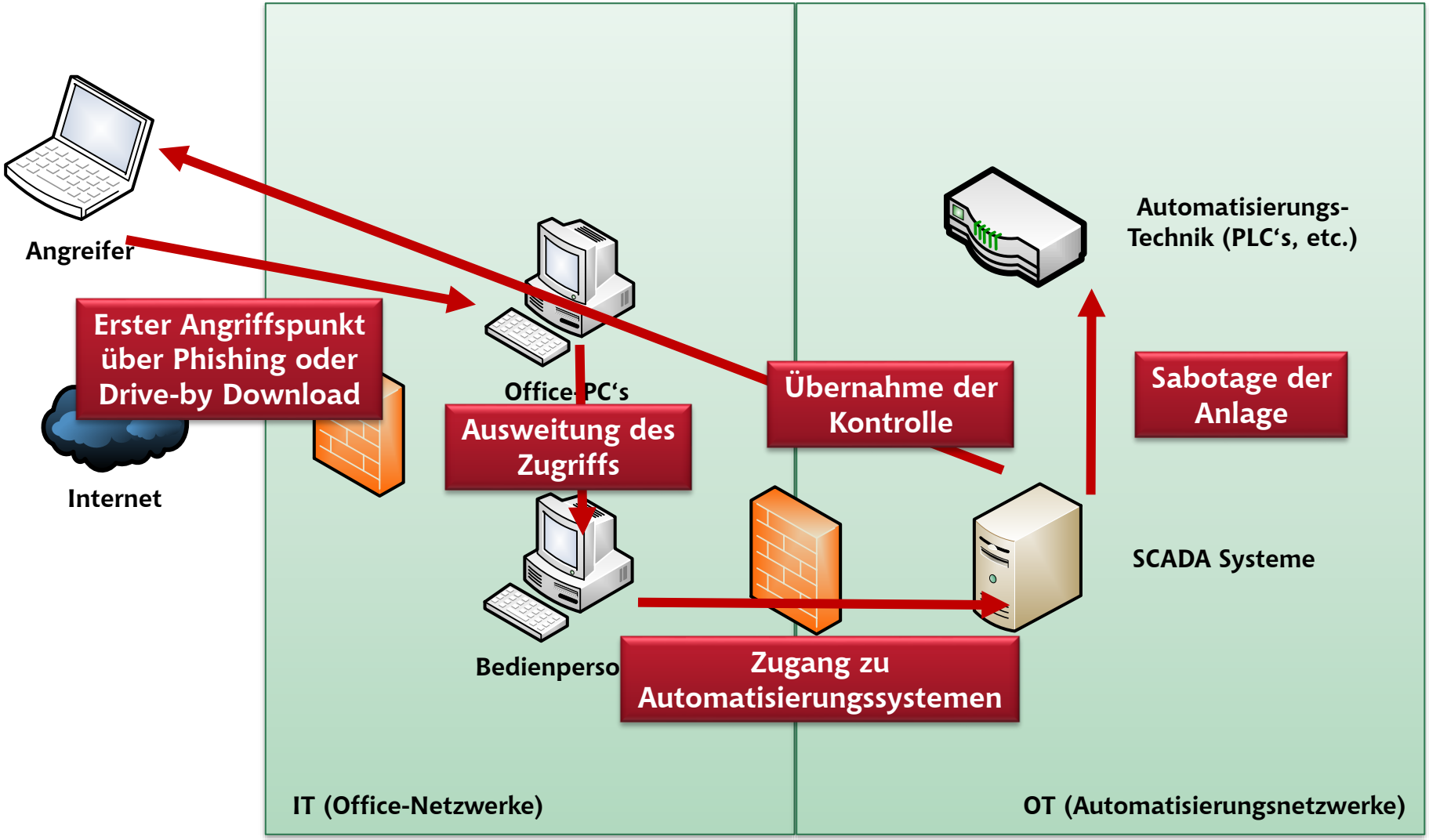
Ukraine has been forced to turn to back-up power sources in recent months following a spate of power cuts

A power cut in western Ukraine last month was caused by a type of hacking known as "spear-phishing", says the US Department of Homeland Security (DHS).

Wie funktionieren solche Angriffe?



Der Angriff


Angreifer
Erster Angriffspunkt über Phishing oder Drive-by Download
Internet
Office-PC's
Ausweitung des Zugriffs
Bedienperso
Übernahme der Kontrolle
Zugang zu Automatisierungssystemen
Automatisierungs-Technik (PLC's, etc.)
Sabotage der Anlage
SCADA Systeme
IT (Office-Netzwerke)
OT (Automatisierungsnetzwerke)

Demo

• • •

Also was tun?

- Bedrohungs- und Risikoanalyse
- Sicherheitsaspekte im gesamten Systemlebenszyklus
- Organisatorische Maßnahmen und Sicherheitsprozesse
- Technische Sicherheitsmaßnahmen bei Installation und Betrieb
- Erkennung und Behandlung von Sicherheitsvorfällen

„Good enough“ – Security Economics

- Ein „perfektes“ Sicherheitssystem ist meistens unnötig
  - Meist auch nicht machbar bzw. bezahlbar
  - Zu starke Fokussierung auf einen Bereich – vernachlässigen anderer Bereiche (→ weakest Link)
- „There are no secure systems, only degrees of insecurity“ (Adi Shamir)
- „It‘s all about risk“ – eine gute Risikoanalyse sollte am Beginn jedes Sicherheitskonzeptes stehen
- Ein absolut sicheres System das nicht benutzbar ist bringt genauso viel wie ein System ohne Sicherheitsmechanismen

Resilience

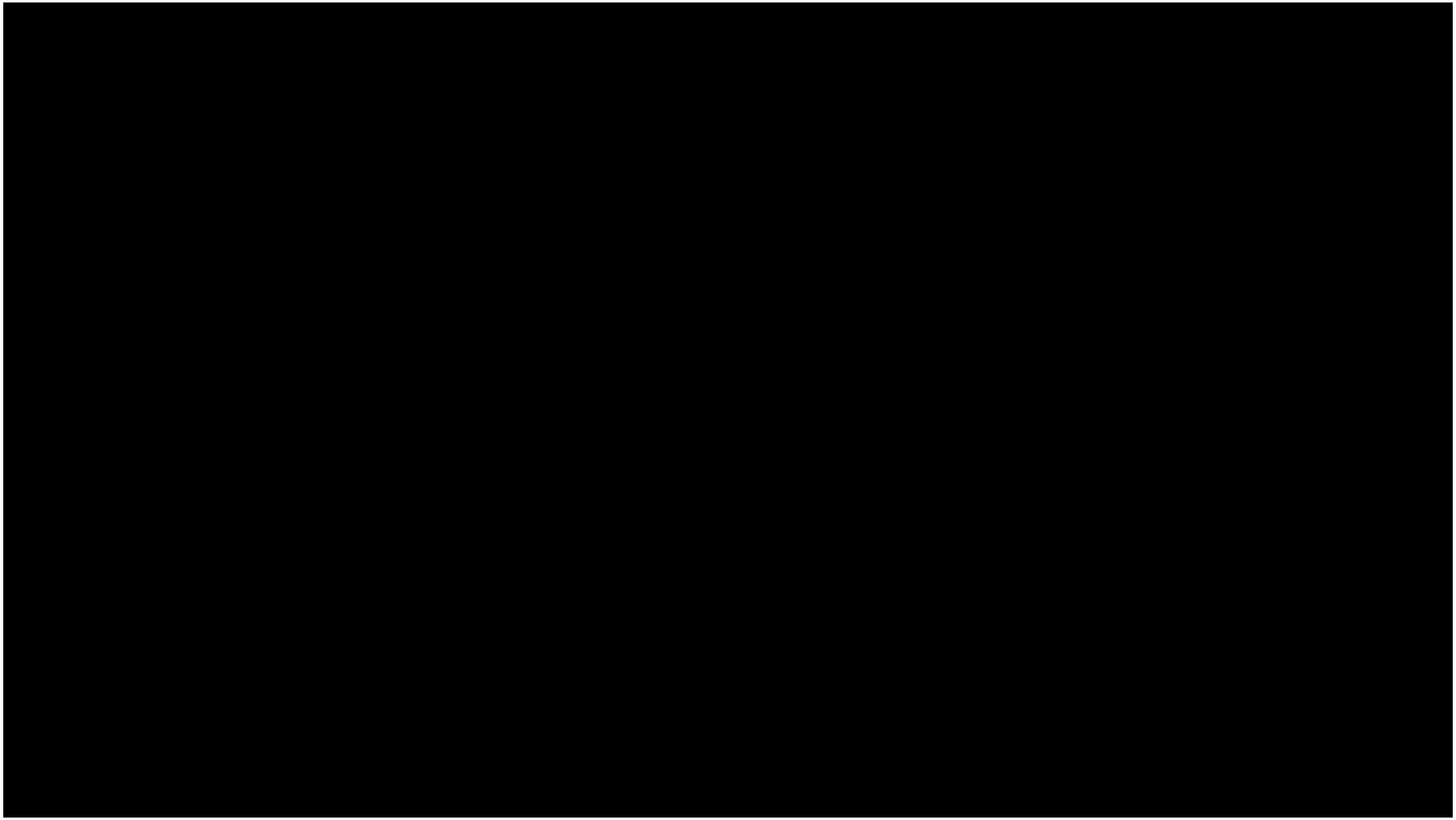
Was passiert nach einem Angriff?

Verhindern von Angriffen (Prevention) alleine reicht nicht

Erfolgreiche Angriffe müssen erkannt werden (Detection), um Abwehrmaßnahmen setzen zu können (Reaction)

Auch im Falle eines erfolgreichen Angriffes muss ein System danach weiter funktionieren können

Alles online in der Welt der Zukunft...



Sicherheit kostet etwas

Sicherheit  **Bequemlichkeit**
Funktionalität
Geschwindigkeit

Der richtige Mittelweg ist wichtig!

Thank You!

Questions?

Contact

Thomas Bleier
DI MSc CISSP CISA CISM CEH zPM
Chief Security Improvement Officer, Managing Director

E-Mail: **t@b-sec.net**
Phone: **+43 664 3400559**