

DROHT UNS DER TOTALE BLACK- UND SERVICE - OUT?

DIRK BACKOFEN,
SVP & LEITER TELEKOM SECURITY

AUSBLICK DIGITALISIERUNG 2020:

**7,8 MRD. MENSCHEN
&
50 MRD. VERBUNDENE
IOT-GERÄTE**



„EVERYTHING CONNECTIVITY“

ERFORDERT

„EVERYTHING SECURITY“



CYBER ATTACKEN SIND LEIDER REAL UND NEHMEN EXPONENTIELL ZU

31 MIO.

April 2019

12 MIO.

in 2018

4 MIO.

in 2017



ANGRIFFE PRO TAG AUF DIE INFRASTRUKTUR DER DEUTSCHEN TELEKOM

PEAK:

46 MIO.

Angriffe pro Tag im
April 2019



AKTUELLE CYBER SECURITY ANGRIFFSVEKTOREN

1,35 TBIT/S

GRÖSSTE DDOS-ATTACKE WELTWEIT 2018

135 GBIT/S

GRÖSSTE DDOS ATTACKE AUF TELEKOM 2019

5.300 MRD.

BOTNET-PAKETE AM BACKBONE TELEKOM
IM APRIL 2019



EVERYTHING SECURITY IST NOTWENDIG

1

ANGRIFFE WERDEN IMMER KOMPLEXER

2

**STEIGENDE ANZAHL VON ANGRIFFEN
DURCH ROBOTER UND KÜNSTLICHE
INTELLIGENZ (AI)**

3

**SPEED DER INFILTRIERUNG BENÖTIGT
AUTOMATISIERTE ECHTZEIT REAKTION**

4

MASSGESCHNEIDERTE CYBER ATTACKEN

5

**KÜNSTLICHE INTELLIGENZ GEGEN
KÜNSTLICHE INTELLIGENZ**

ANGRIFFE AUF KRITISCHE INFRASTRUKTUREN SIND REALITÄT !

SEP 2010



Zugriff auf iranisches Atomkraftwerk

**STUXNET
BEFÄLLT
INDUSTRIE-
ANLAGEN**

MAI 2015



Kompletter Austausch der IT

**ANGRIFF AUF IT
DES BUNDES-
TAGES**

DEZ 2015



80.000 Menschen ohne Strom

**UKRAINE:
ANGRIFF AUF
STROMNETZ**

FEB 2016



IT-Systeme lahmgelegt

**RANSOMWARE
ANGRIFF AUF
KRANKENHAUS**

NOV 2016



900.000 Menschen ohne Internet

**MIRAI-BOTNET-
ANGRIFF AUF
ROUTER**



ERLEBEN, WAS VERBINDET.

Quelle: <http://app.wiwo.de/technologie/digitale-welt/cyberangriffe-it-sicherheit-verkommt-zur-randnotiz/19568942.html?mwl=ok>

ANGRIFFE AUF KRITISCHE INFRASTRUKTUREN SIND REALITÄT !

MAI 2017



Bislang größter Ransomware Angriff

**‚WANNACRY‘
BEFÄLLT
230.000 RECHNER
IN 150 LÄNDERN**

JAN 2018



Prozessor-Schwachstelle

**SPECTRE
MELTDOWN**

JAN 2019



Schüler hackt das politische System

**SORGLOSER
UMGANG MIT
PASSWÖRTERN
UND DATEN**

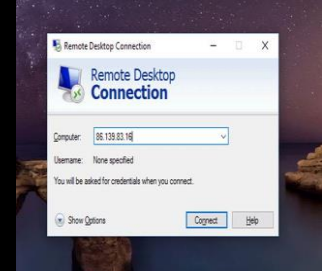
Q2 / 2019



Spionageangriffe durch Winnti

**VERSUCHTER
DATENKLAU BEI
DAX
KONZERNEN**

MAI 2019



Remote Desktop Protocol (RDP)

**WURMARTIGE
RDP-SCHWACH-
STELLEN IN
WINDOWS**



ERLEBEN, WAS VERBINDET.

Quelle: <http://app.wiwo.de/technologie/digitale-welt/cyberangriffe-it-sicherheit-verkommt-zur-randnotiz/19568942.html?mwl=ok>

STROMNETZE

ANGRIFFE AUF STROMNETZE



1

ANGRIFFE AUF KRAFTWERKE

2

ANGRIFFE AUF TRANSPORTNETZE

3

GEZIELTES AUSSPIONIEREN / MÖGLICHE
VORBEREITUNGEN ZUM AUSSCHALTEN
KRITISCHER INFRASTRUKTUREN

HALTEN WIR IN UNSERER GESELLSCHAFT

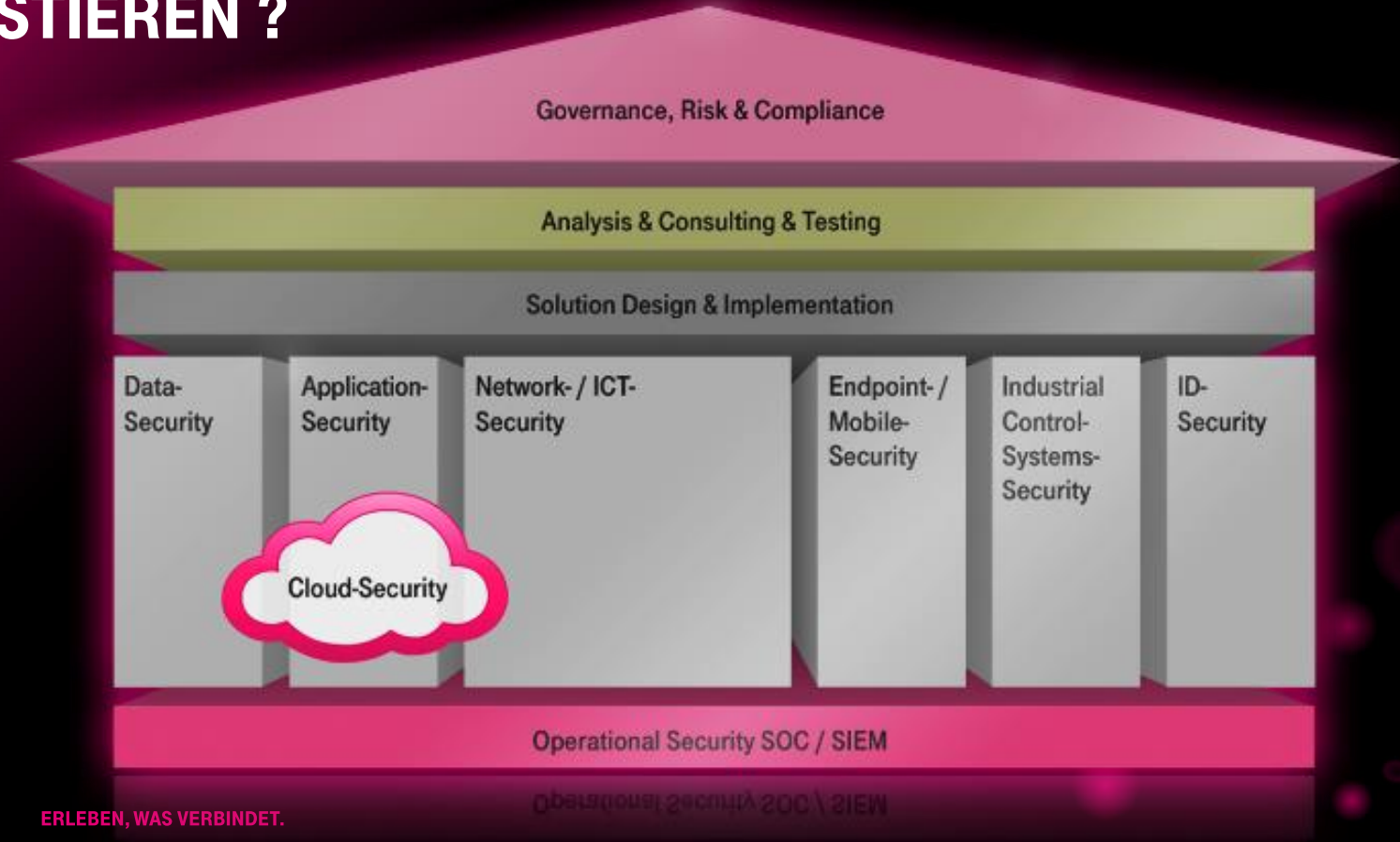
LÄNGER ALS 3 TAGE

OHNE STROM, GAS, WASSER,
ELEKTRIZITÄT UND INTERNET DURCH ?































WIR BRAUCHEN EINE ARMEE DER GUTEN



IN WELCHE SECURITY BEREICHE SOLLTEN SIE INVESTIEREN ?



KOMPLEXITÄT VS. HIGH SOPHISTICATION

Cyber Defense	 Man. Cyber Defense / SOC Operations	 Forensic Cyber Security	 Credential Leakage Monitoring	 Fraud. Domain Monitoring/Passive DNS	 Blackhole Monitoring	Cloud & Appl.	 Managed Cloud Security	 Database Activity Monitoring	 Data Leakage Prevention	 Workload Encryption	 Web Application Firewall			
Identity	 Secure Identity Management	 Private Key & Root CA	 Privileged Account Management	Endpoint	 Endpoint Protection	 Mobile Protection	Network	 Managed Firewall & IDS/IPS	 DDoS Protection	 Micro Segmentation	 E-Mail Security (APT Protection)	Testing	 Pen testing	 Vulnerability Scanning
GRC	 GRC	 Awareness Training	 Sec by Design (PSA)	Industrial	 Industrial / OT Security	 Special Industrial Sector Honeypots	Physical	 Drone Security	 Physical Security	Other	 Encrypted Voice	 Sealed Cloud		

DAS GRÖSSTE ASSET IM BEREICH CYBER SECURITY IST DAS WISSEN – UND DAS MÜSSEN WIR TEILEN !



TELEKOM
SECURITY

1.600 Cyber Security
Experten



Europas größtes
integriertes CDC & SOC



Zero Impact Ansatz

SECURITY BY DESIGN BASED



Security tief in Netzwerk-
konnektivität integriert



Die gleichen hochprofessionel-
len Tools im internen Einsatz



Eine der größten Threat
Intelligence Datenbanken



Security und Datenschutz
„made in Germany“

A futuristic control room with a large curved wall display. The display shows various data visualizations, including bar charts and line graphs, with a central banner that reads "WIR BILDEN DIE ARMEE DER GUTEN". The room is dimly lit with blue and purple ambient lighting. Several people are seated at desks with multiple computer monitors, some of which display a globe with a padlock icon. The overall atmosphere is high-tech and data-driven.

WIR BILDEN DIE ARMEE DER GUTEN

MACHEN SIE MIT...