FORUM VERANTWORTUNG

ZENTRUM FÜR ETHIK UND VERANTWORTUNG

Hochschule Bonn-Rhein-Sieg
University of Applied Sciences

gefördert vom

Bundesministerium für Bildung und Forschung

Gemeinsame Wissenschaftskonferenz GWK

Innovative Hochschule

Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

CYBERBEDROHUNGEN WACHSEN EXPONENTIELL

DIRK BACKOFEN,
SENIOR VICE PRESIDENT & LEITER TELEKOM SECURITY

AUSBLICK DIGITALISIERUNG 2020:

7.8 MRD. MENSCHEN
&
50 MRD. VERBUNDENE IOT-GERÄTE

„EVERYTHING CONNECTIVITY“

ERFORDERT

„EVERYTHING SECURITY“

Quelle IoT Geräte: Cisco
Quelle Bevölkerung: UN

CYBER ATTACKS SIND REAL UND NEHMEN ZU !

75 % ALLER FIRMEN IN DEUTSCHLAND WAREN 2019 OPFER VON CYBER ANGRIFFEN
(ZZGL. 13 % MIT VERMUTUNG EINES ANGRIFFS)

73% ALLER MITTELSTÄNDISCHEN UNTERNEHMEN WAREN BEREITS EINMAL BETROFFEN

100 MRD € SCHADEN FÜR DIE DEUTSCHE WIRTSCHAFT PRO JAHR

200 MRD € EUROPA

450 MRD € WELTWEIT

Source: Bitkom-Studie: „Wirtschaftsschutz in der Industrie“. Nov. 2019

ANGRIFFE PRO TAG AUF DIE INFRASTRUKTUR DER DEUTSCHEN TELEKOM

PEAK:

60 MIO.

Angriffe pro Tag im Mai 2019

620 physische, 3.400 logische Honeypot-Installationen

ZAHLEN EINES ARBEITSTAGES @ TELEKOM

42 MIO. Angriffe auf unsere 620 physischen Honeypot-Sensoren (3.400 logische Sensoren)

2,5 MRD. sicherheitsrelevante Events aus 3.300 Datenquellen

>6 MRD. Datensätze unserer DNS Server bzgl. Cyber Attacken ausgewertet

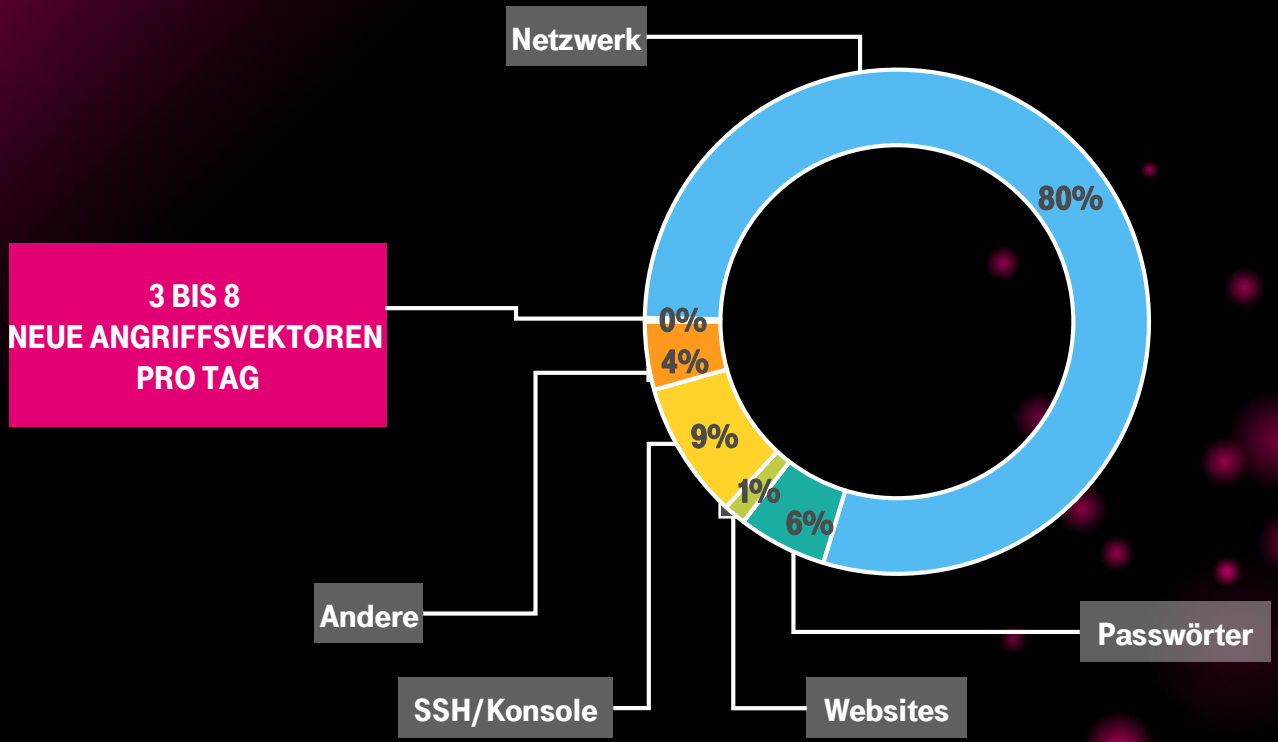
FAKTEN TELEKOM SEPTEMBER 2019

135 GBIT/S Umfang der grössten DDoS Attacke

5.400 MRD. Botnet-Pakete am Backbone vom Fest und Mobilfunknetz

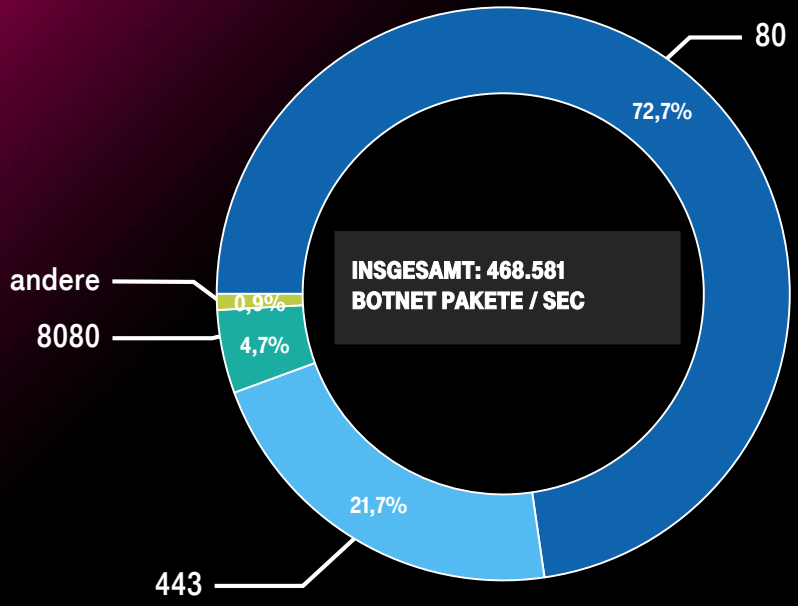
110.000 Informationen an Kunden auf Grund von Hinweisen über Datenmissbrauch durch Dritte

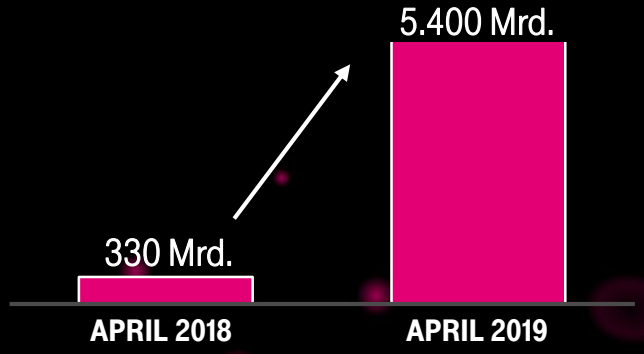
STRUKTUR DER ANGRIFFE GEGEN DAS HONEYPOT-NETZWERK



BOTNET-VERKEHR ANALYSE (FESTNETZ/ MOBIL)

BOTNET-VERKEHR AUF TCP PORTS





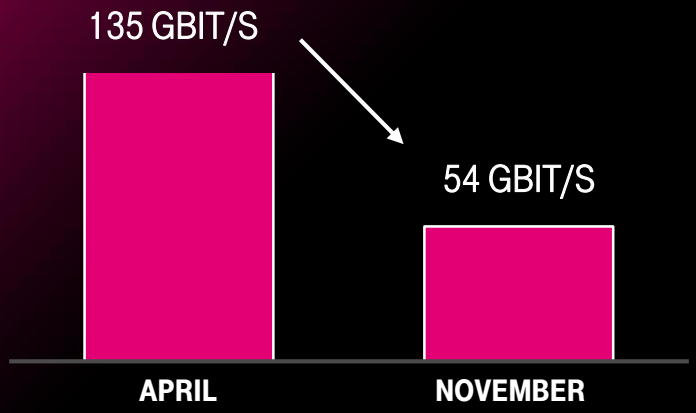
Legende:

80: HTTP Port (Browser Verkehr)
443: HTTPS Port (SSL Verkehr)

Kritisch, da nicht von Firewalls blockiert

8080: Alternativer HTTP Port

ERSTER ERFOLG GEGEN DDOS ANGRIFFE 2019



81 GBIT/S Reduktion von DDOS-Volumen basierend auf Blockaden / Eliminierung von Command and Control Servern / Sperrung deren IP Adressen

NEUE DIMENSION VON ANGRIFFSZIELEN

UNTERNEHMENSNETZWERKE

INDUSTRIENETZWERKE

STROMNETZ

SMART HOME

CONNECTED CAR

INFRASTRUKTUR FÜR AUTONOMES FAHREN

SMART CITIES

IDENTITÄT

ATTACK-SITUATION IN DEUTSCHLAND

42 Mio. Angriffe pro Tag auf die Infrastruktur der Deutschen Telekom (Peak: 60 Mio.)

3 – 8 neue Angriffsvektoren jeden Tag auf DAX-Infrastruktur

252 Meldungen von KRITIS-Betreibern (2019)

1.500 registrierte KRITIS-Anlage

(2018: 145 Meldungen)

114 Mio. neue Schad-Programm-Varianten

Windows: 65 Mio.; Android: 3,4 Mio.; MacOS: 0,09 Mio.; Weitere: > 39 Mio.

11,5 Mio. Berichte über Malwareinfektionen

Übermittelte das BSI an deutsche Netzwerkbetreiber

Häufigste Attacke: Malwareinfektionen (53%)

Der berichteten Angriffe 2018/2019

5.400 Mrd. Botnet-Pakete

Am Backbone des Fest- und Mobilfunknetzes der Deutsche Telekom innerhalb eines Monats

770.000 Mails mit Schadprogrammen

In deutschen Regierungs-netzen abgefangen

Bis zu 110.000 Botinfektionen pro Tag

Deutsche Systeme

Bis zu 300 Gbit/s Peak in DDoS-Angriffen (international)

National: 135 Gbit/s

40 Mio. EUR

Größter Schadensfall eines Unternehmens durch Ransomware -Angriff

Sources: BSI Lagebericht 2019; Telekom Security Lagebild 2019

DIE WICHTIGSTEN ANGRIFFVEKTOREN 2019

Ransomware

DDoS

Advanced Persistent Threats (APT)

Spectre / Meltdown (HW-attacks)

Emotet (Phishing)

Eternal Blue (RDP-Angriff)

Man in the Middle – Angriff

CEO-Fraud

Quellen: BSI Lagebericht 2019; Telekom Security Lagebild 2019

EIN TRANSPARENTER UND UMFASSENDER BLICK AUF ALLE ANGRIFFSVEKTOREN IST NOTWENDIG

- Unterschiedliche Angriffsvektoren aus allen Industriesektoren
- „Indicators of compromise“ aus Unternehmen aller Größenklassen
- Knowhow über kritische Infrastrukturen
- Optimierte Einstellungen für komplexe Cyber Security Architekturen
- Security und Datenschutz “made in Germany“

Photocredit: webandi, Didgeman, 127071, cegoh, code83, blickpixel, abruellmann | Pixabay

ZUSAMMENFASSUNG CYBER SECURITY ANGRIFFSVEKTOREN

EVERYTHING SECURITY IST NOTWENDIG

1. ANGRIFFE WERDEN IMMER KOMPLEXER (U.A. HACK AS A SERVICE)
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

DAS GRÖSSTE ASSET IN CYBER SECURITY IST NICHT TECHNOLOGIE...

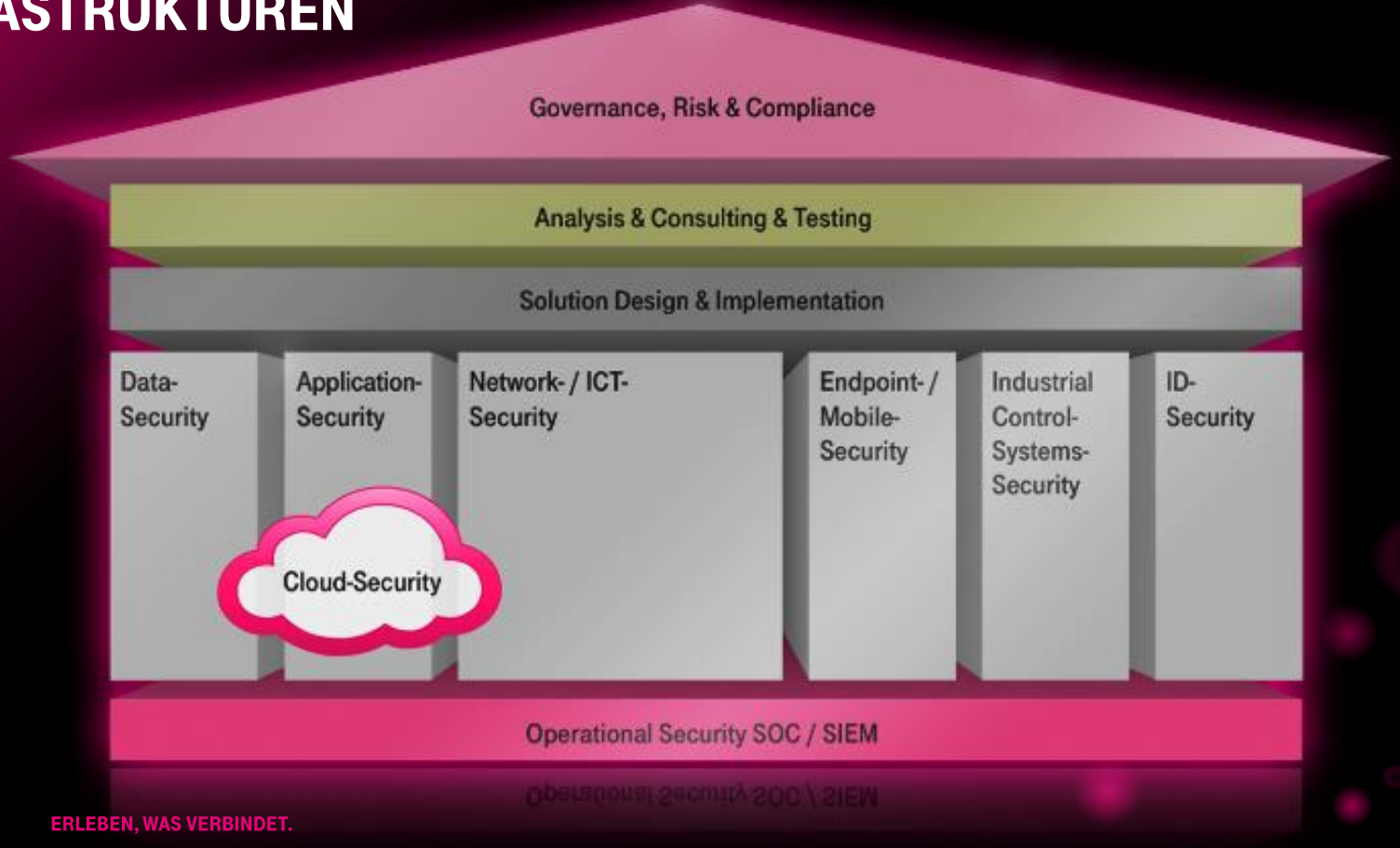
...DAS GRÖSSTE ASSET IST DAS WISSEN ÜBER ALLE ANGRIFFSVEKTOREN

... UND DAS WISSEN MUSS GETEILT WERDEN

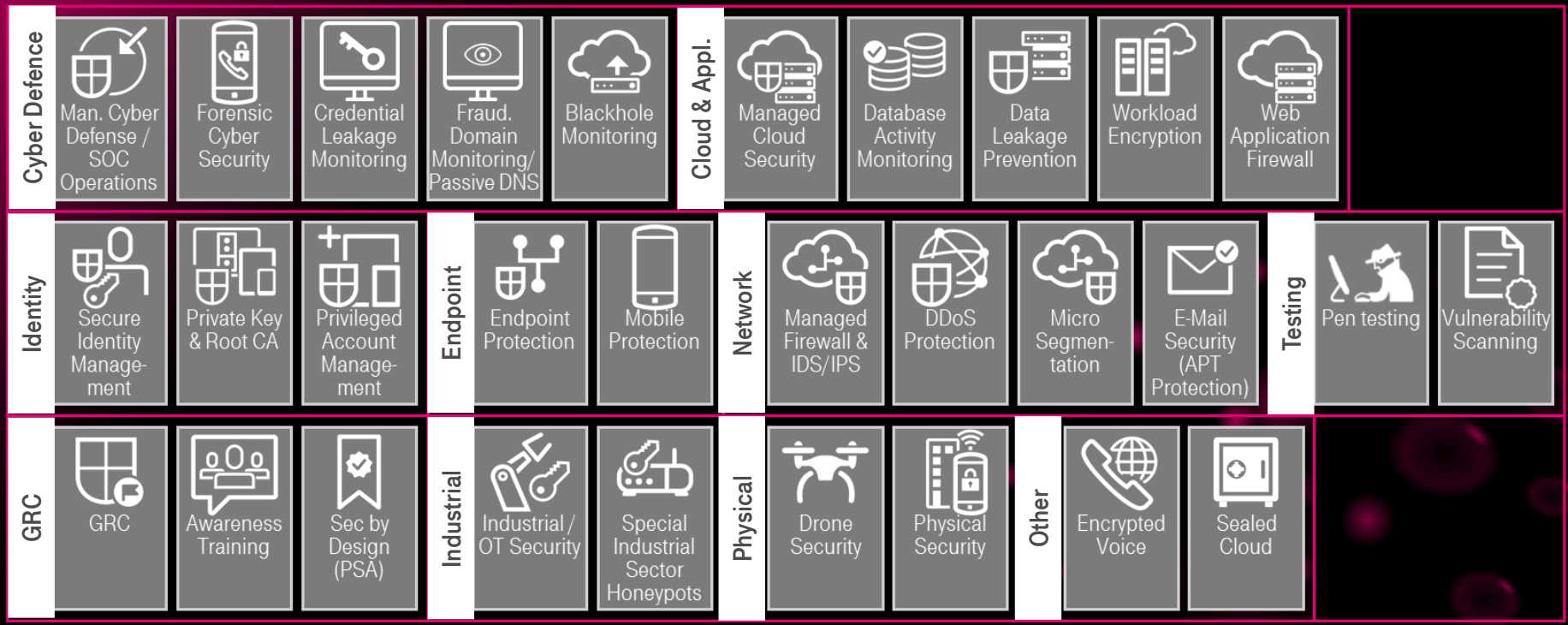
NIEMAND KANN ES ALLEIN…

…WIR BRAUCHEN EINE ARMEE DER GUTEN IN EUROPA !!

ELEMENTE DER CYBER SECURITY FÜR KRITISCHE INFRASTRUKTUREN



KRITISCHE INFRASTRUKTUREN MÜSSEN MÜSSEN IN ALL DIESEN BEREICHEN GESCHÜTZT WERDEN



PRÄVENTION ALLEIN REICHT HEUTE NICHT MEHR AUS...

SOC

PREVENT

DETECT

RESPOND

ZERO TRUST

SIE MÜSSEN ANTIZIPIEREN, DASS DER ANGREIFER BEREITS IHR NETZWERK INFILTRIERT HAT

WER KANN ERKENNEN, OB EIN ANGREIFER BEREITS IN IHRE INFRASTRUKTUR EINGEDRUNGEN IST ?

MANAGED CYBER DEFENCE MIT INNOVATIVER SOC OPERATION IST NOTWENDIG

VERSTÄNDLICHE USE CASE LIBRARY AUS ALLEN INDUSTRIEN

WIR BETREIBEN EUROPAS GRÖSSTES INTEGRIERTES CYBER DEFENCE UND SECURITY OPERATION CENTER IN BONN

1. **MASTER CDC + SOC**
2. **MAGENTA HERZSCHLAG FÜR CYBER SECURITY “MADE IN GERMANY”**
   Central incident coordination, Threat-Intelligence, Forensic
3. **ZUSAMMENARBEIT ALLER CDC / SOCS WELTWEIT**
4. **240 CYBER SECURITY PROFESSIONALS**
5. **USE CASES AUS JEDER INDUSTRIE**

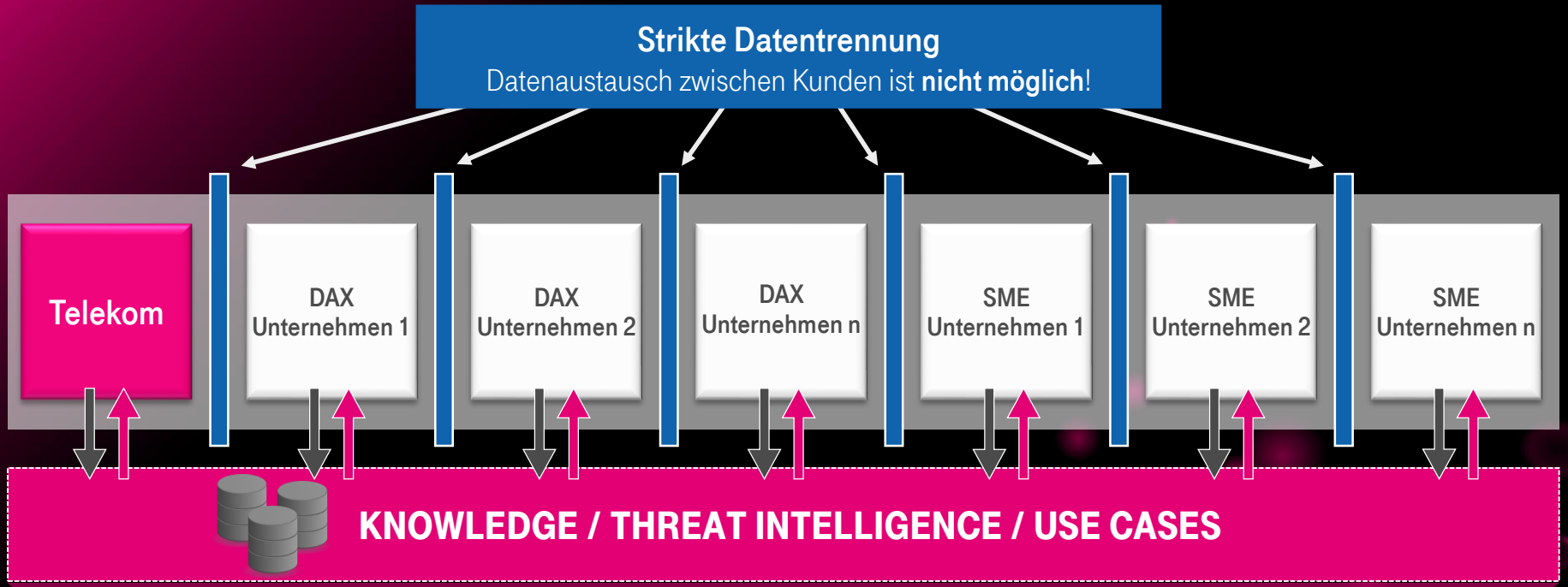
INTEGRIERTES CDC + SOC: EINE PLATTFORM FÜR ALLE KUNDEN

THREAT INTELLIGENCE / THREAT HUNTING / FORENSIK

SOC + SIEM TOOLS

ArcSight An HP Company
splunk>
Radar

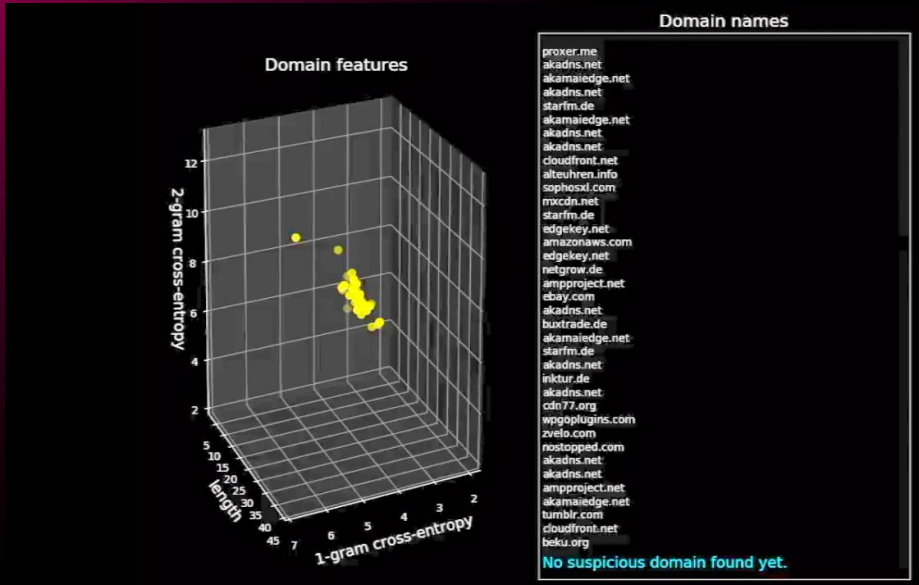
ARMEE DER GUTEN: SELBSTLERNENDE PLATTFORM



Wissens-Transfer: Alle Kunden profitieren automatisch und sofort von Einblicken in neue Angriffstypen!

GLOBALE SOC PRODUKTION – FOLLOWING THE SUN

PASSIVE DNS
DNS-CARRIER KNOW HOW



PASSIVE DNS	
1	GRÖSSTE DNS SERVER FARM IN EUROPA (6 MRD.ANFRAGEN PRO TAG)
2	200.000 NEUE DNS EINTRÄGE PRO TAG
3	KOMPLETT AUTOMATISIERTER CHECK VON ENTROPIE / INHALT
4	BLOCKIERUNG VON MALICIOUS DNS / IP ADRESSEN
5	AUTOMATISIERTE KONFIGURATION DES KUNDENNETZWERKES MÖGLICH (FIREWALL / IDS)

Results: Typo domains, homographically similar domains, international domain names (IDNs)
MISP = Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing

FRAUDULENT DOMAIN MONITORING
FRÜHERKENNUNG GEGEN PHISHING ATTACKS

REGISTRIERUNG VON ÄHNLICHEN DOMAINS ALS VORBEREITUNG VON PHISHING KAMPAGNEN

Tele-kom.de	85.16.135.147	Not seen in D
teIekom.de	80.93.65.144	2017-04-01 21:47
Telekö̈m.de	185.58.178.9	2017-03-16 17:43
telakom.de	54.187.129.255	2017-10-04 13:43
telikom.de	187.53.178.8	2017-03-21 21:59
telekom.my.de	49.32.213.174	2017-03-17 18:39
tellekom.hk	79.52.6.122	2017-03-25 10:52
Tellekom.com	87.203.60.254	2017-03-16 11:23
Teellekom.de	35.226.200.91	2017-09-16 02:02
.....		

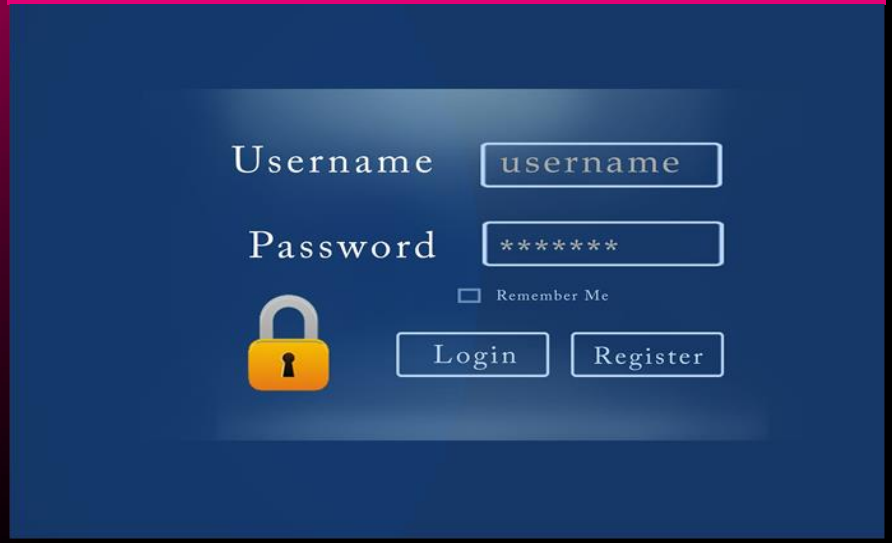
FRAUDULENT DOMAIN MONITORING

1. AUTOMATISIERTE ANALYSE VON NEUREGISTRIERTEN DOMAINS (CA. 100.000 - 200.000 DOMAINS/TAG)
2. VERIFIZIERTE VARIANTEN: TYPO SQUATTING UND HOMOGRAPHIC ATTACK
3. AUTOMATISIERTE BEREICHERUNG MIT SCREENSHOTS UND DOMAIN REGISTRATION INFORMATION
4. INTERFACE ZUM KUNDEN VIA MISP ORDER-MAIL, PDF-REPORT, INCIDENT TICKET
5. SERVICE OPTION: REMOVAL OF FALSE POSITIVES (E.G. LEGITIMIERUNG DER DOMAINS MIT ÄHNLICHEM NAMEN)

Results: Typo domains, homographically similar domains, international domain names (IDNs)
MISP = Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing

CREDENTIAL LEAKAGE MONITORING
EINZIGARTIGE CREDENTIALS

LEAKAGE IST EIN RISIKO FÜR JEDES UNTERNEHMEN



CREDENTIAL LEAKAGE MONITORING

1. TÄGLICHES MONITORING VON INTERNETQUELLEN FÜR LEAKED CREDENTIALS
2. AUSLÖSER SIND KUNDENBEZOGENE DOMAINS
3. DATA CLEANUP, REMOVAL OF DUPLICATES
4. 24X7 MONITORING VON 57 VERSCHIEDENEN QUELLEN, AD-HOC-ALARMIERUNG (TICKET) O. TAGESREPORTS
5. STATISTISCHE ANALYSE VERGLICHEN MIT ANDEREN FIRMEN (ANONYMISIERT)

BLACKHOLE MONITORING
IDENTIFIZIERUNG VON BOTNET-ATTACKEN

BLACKHOLE MONITORING

1. DEFINITION VON UNGESCHALTETEN IP ADDRESS RANGES (BLACKHOLES)
2. MONITORING VON VERKEHR IN DEN BLACKHOLES (VERURSACHT DURCH BOTNETS)
3. SICHTBARKEIT VON CLEAN BOTNET TRAFFIC
4. DETEKTION VON BOTNET-KAMPAGNEN WELTWEIT MÖGLICH
5. SOFORTIGE REAKTION

VORAUSSETZUNGEN FÜR EINE SICHERE DIGITALE ZUKUNFT

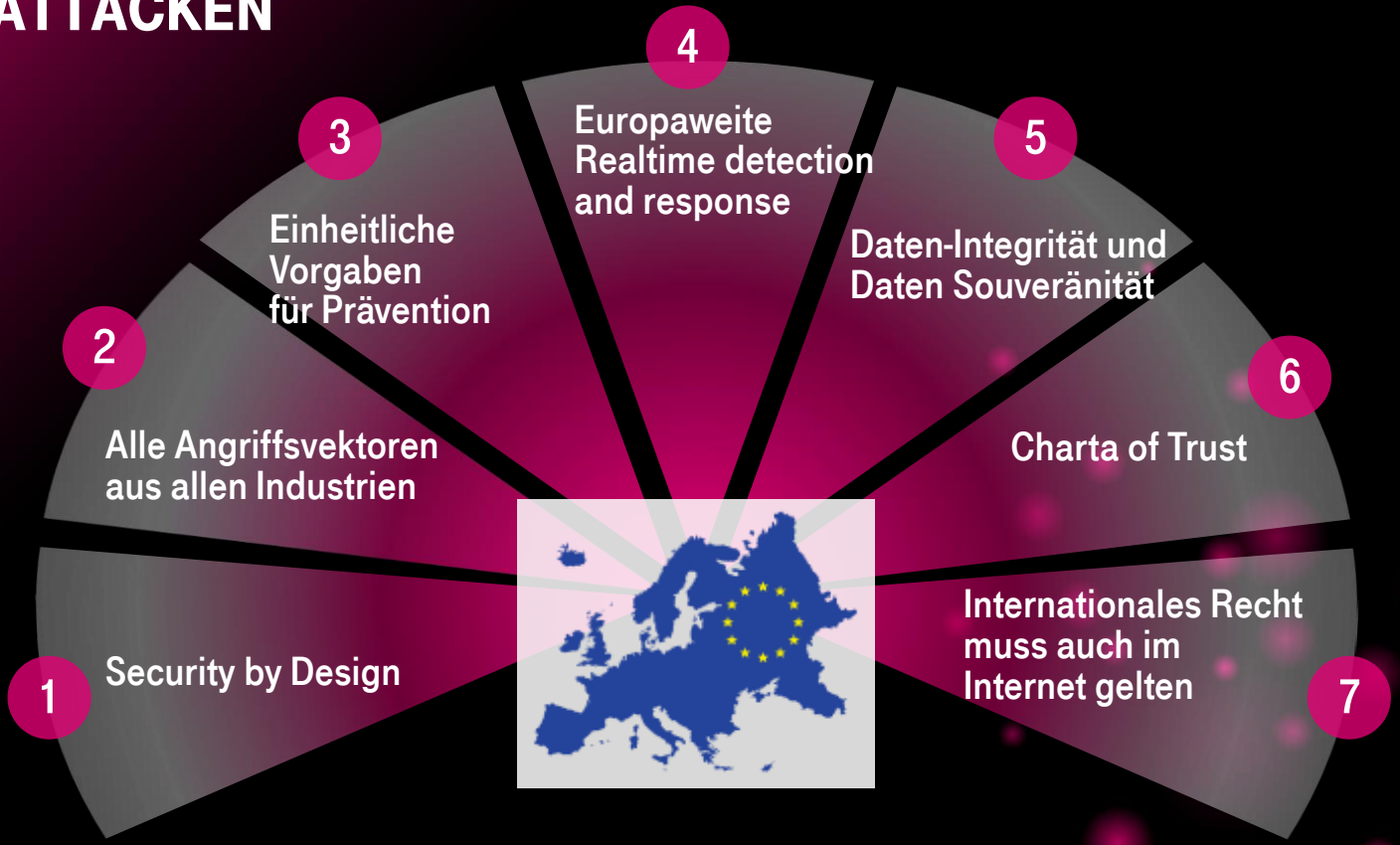
1. SECURITY BY DESIGN - IMMER & ÜBERALL
2. VERPFLICHTENDE PENTESTS / VULNERABILITY SCANNING
3. BUSINESS: E-MAIL / WEB NUR MIT APT-SCHUTZ
4. DDOS SCHUTZ IN DER TERABIT RANGE NOTWENDIG
5. MOBILE SECURITY IST VERPFLICHTEND
6. UNTERNEHMENSNETZWERKE NUR MIT MANAGED CYBER DEFENCE
7. INDUSTRIENETZWERKE SIND “KRITISCHE" INFRASTRUKTUREN
8. SCHNELLIGKEIT DER DEFENCE MASSNAHMEN NOTWENDIG

WIE ERREICHEN WIR EINE HOCH ENTWICKELTE VERTEIDIGUNG GEGEN CYBER-ANGRIFFE?

1. KEINER KANN ES ALLEINE!
   WIR BRAUCHEN DIE ARMEE DER GUTEN
2. KOORDINIERTE “REALTIME RESPONSE“
3. STÄNDIGES LERNEN UND VERBESSERN VON TECHNOLOGIEN, FÄHIGKEITEN & FERTIGKEITEN
4. ZUSAMMENARBEIT IST EIN MUSS – INSBESONDERE ZWISCHEN PRIVATEM UND ÖFFENTLICHEM SEKTOR
5. ENGAGEMENT IM CYBER SECURITY CLUSTER BONN

CYBER SECURITY CLUSTER BONN
The heart of cyber security in Europe

WIR BRAUCHEN EINE IMMUNISIERUNG DER GESELLSCHAFT GEGEN CYBER ATTACKEN



MACHEN SIE MIT…

CYBER SECURITY CLUSTER BONN

Cyber Bedrohungen wachsen exponentiell

Dirk Backofen,
Vorstandsvorsitzender Cyber Security Cluster Bonn e.V.

Der Herzschlag von Cyber Security in Europa

CYBER SECURITY CLUSTER BONN

VEREINSSTRUKTUR

Verein
Cyber Security Cluster Bonn e.V.

gegründet am 04.Oktober 2018

Clustermanager

Management Board

- Stadt Bonn
- IHK Bonn / Rhein-Sieg
- Fraunhofer-Gesellschaft e.V.
- Anykey GmbH
- Telekom Security
- axxessio GmbH
- Hochschule Bonn Rhein-Sieg
- Conet Solutions GmbH

Beirat*

- Bundesamt für Sicherheit in der Informationstechnik
- Cyber- und Informationsraum Wir. Dienen. Deutschland.
- Police Präsidium Bonn

* Der Beirat hat ausschließlich beratende Funktion

Mitgliederversammlung

MITGLIEDER DES VORSTANDS

Vorstands-Vorsitzender

Dirk Backofen,
Leiter Telekom Security

Stellvertretender Vorsitzender

Prof. Dr. Peter Martini,
Institutsleiter
Fraunhofer FKIE

Stellvertretende Vorsitzender

Victoria Appelbe,
Leiterin Wirtschafts-
förderung Stadt Bonn

Stellvertretender Vorsitzender

Goodarz Mahbobi,
CEO axxessio GmbH

Finanzvorstand

Dr. Hubertus Hille,
Hauptgeschäftsführer
IHK Bonn/Rhein-Sieg

Vorstandsmitglied

Prof. Dr.
Thorsten Bonne,
Hochschule Bonn-
Rhein-Sieg

Vorstandsmitglied

Dirk Lieder,
Geschäftsführer
CONET Solutions
GmbH

Vorstandsmitglied

Stephan Wirtz,
CEO anykey GmbH

MITGLIEDER DES BEIRATS

Jürgen Setzer

Generalmajor Bundeswehr

Cyber- und Informationsraum

Ursula Brohl-Sowa

Polizeipräsidentin

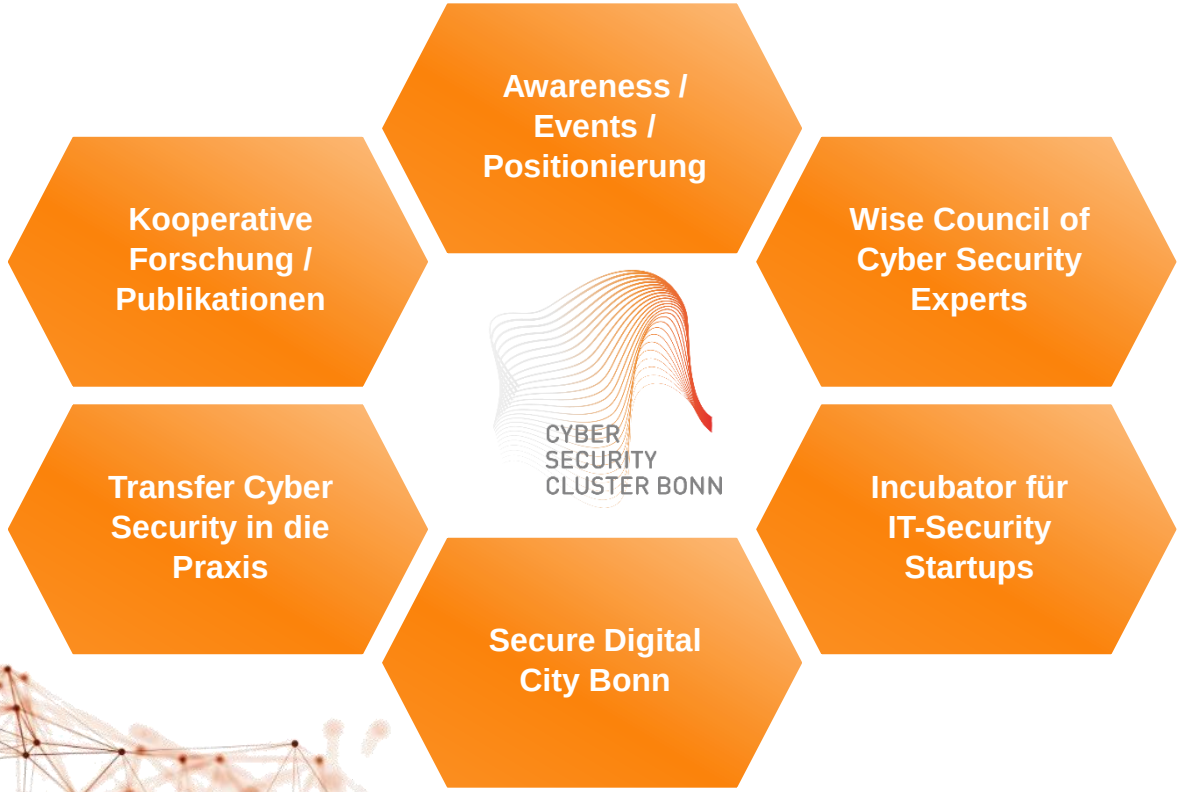
Bonn

Dr. Gerhard Schabhüser

Vizepräsident

Bundesamt für Sicherheit in der Informationstechnik

INHALTLICHE SCHWERPUNKTE



WISE COUNCIL VON CYBER SECURITY EXPERTEN

Prof. Dr. Matthew Smith

Professor für Usable Security and Privacy, Universität Bonn und Fraunhofer FKIE

Prof. Dr. Claudia Eckert

Leiterin des Fraunhofer-Instituts für Angewandte und Integrierte Sicherheit (AISEC), München

Prof. Dr. Norbert Pohlmann

Professor für Informatik, verteilte Systeme und Informations-sicherheit, Westfälische Hochschule Gelsenkirchen

Prof. Dr.-Ing. Delphine Reinhardt

Leitung Forschungsgruppe „Computer-sicherheit und Privatheit“

Uni Göttingen

Prof. Dr. Angela Sasse

Professorin für Human-Centred Security, Ruhr Universität Bochum

Prof. Dr. Mathias Hollick

Leiter Secure Mobile Networking Lab

TU Darmstadt

WIR WOLLEN BONN ZUM “DAVOS” FÜR CYBER SECURITY MACHEN