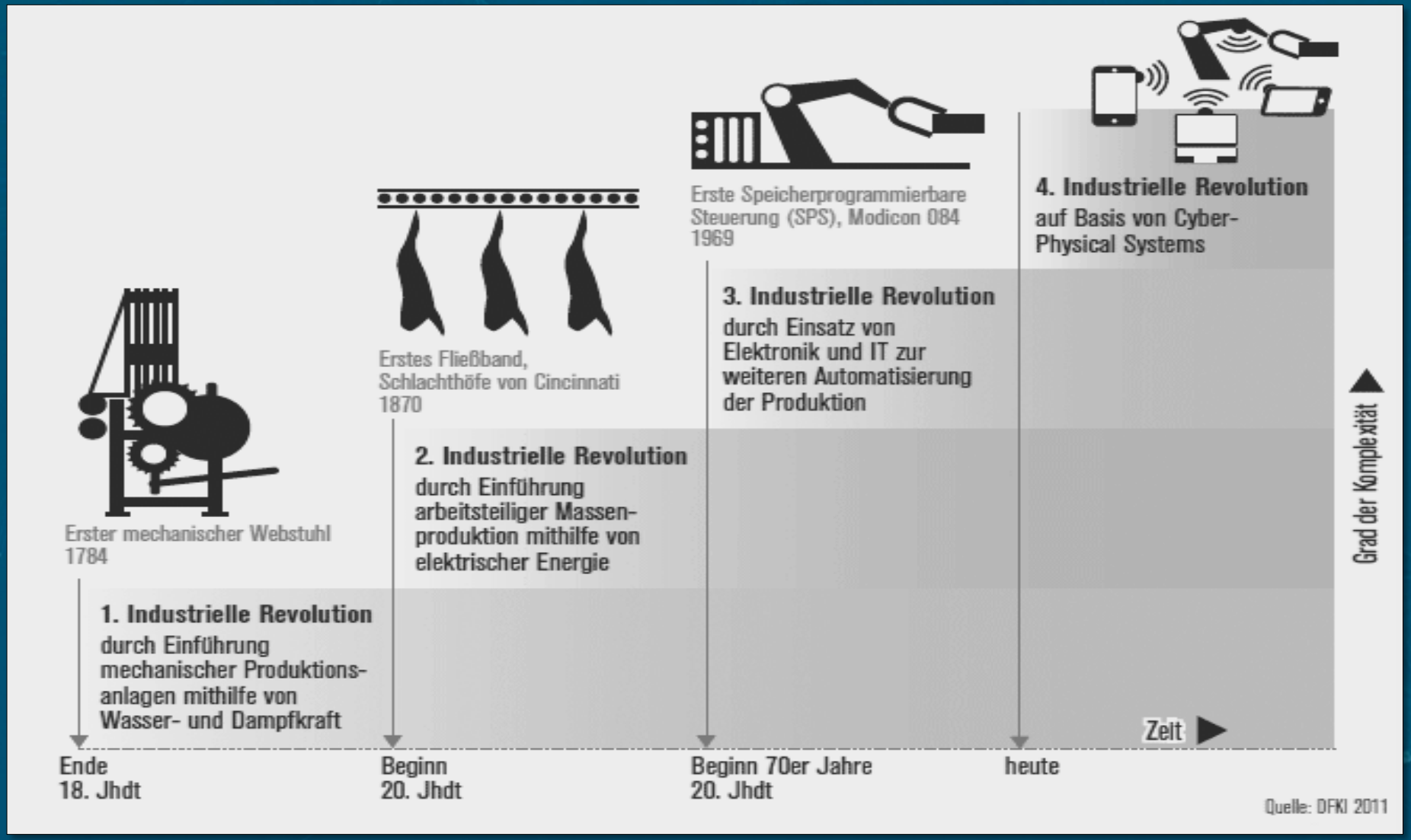
Cyber-Sicherheitsrat Deutschland e.V.

Spannungsfeld digitale Wirtschaft: Zwischen Innovation und Cyber-Sicherheit

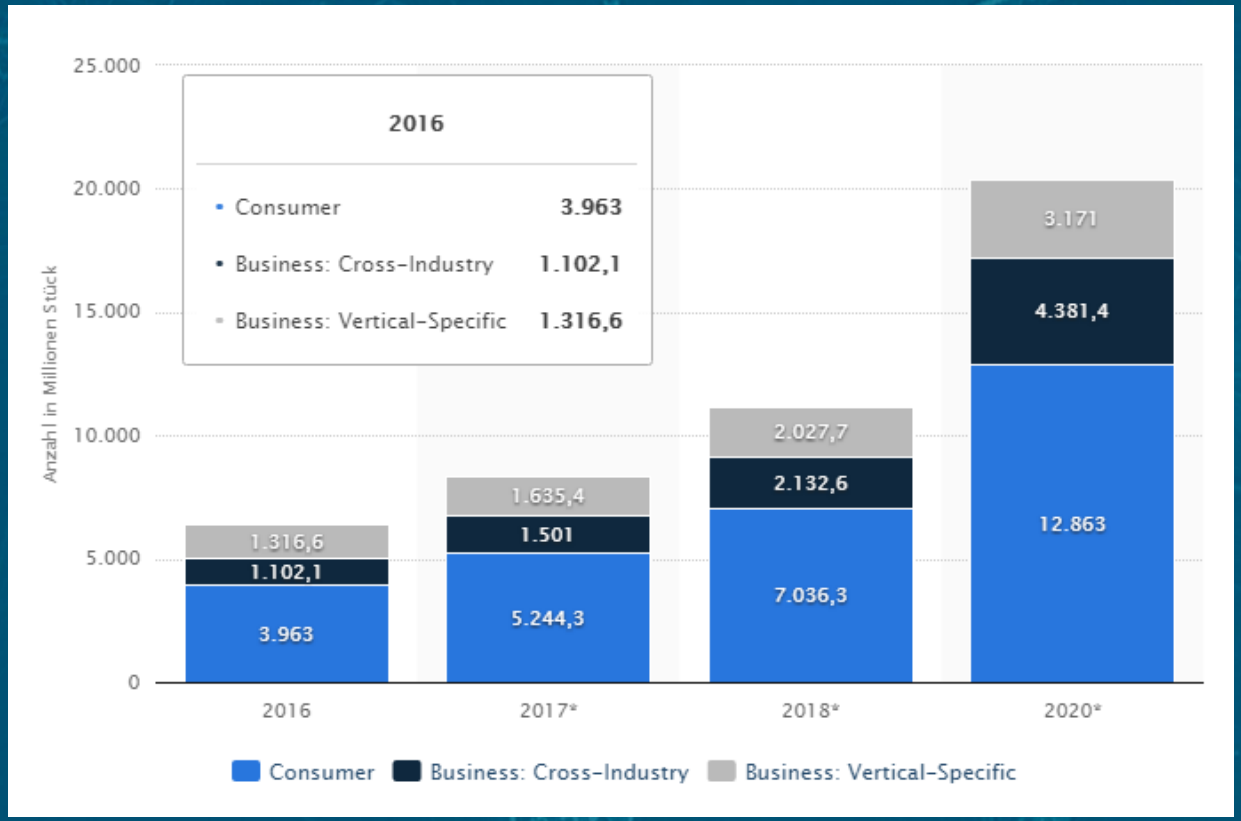
Hans-Wilhelm Dünn, Generalsekretär
Cyber-Sicherheitsrat Deutschland e.V.

Zunahme der Gefährdung am Beispiel Industrie 4.0



Cyber-Sicherheitsrat Deutschland e.V.

Digitale Vernetzung wächst unaufhaltsam



Prognose zur Anzahl der vernetzten Geräte im Internet der Dinge (IoT) weltweit in den Jahren 2016 bis 2020 (in Millionen Einheiten) (Quelle: Statista)

Jedes vernetzte Objekt als potenzielles Angriffsziel!

Cyber-Sicherheit ist die Grundlage funktionsfähiger IT-Infrastruktur!

Cyber-Sicherheit ist Prozess-Enabler der Digitalisierung!

Aktuelle Schlagzeilen…

ZEIT Politics

Politik Gesellschaf

Computer secu

of 'biggest rans

DER TAGESSPIEGEL

STARTSEITE | POLITIK | BERLIN | WIRTSCHAFT | SPORT | KULTUR

AGENDA | NSA-SKANDAL | RECHTSEXTREMISMUS | GESCHICHTE | UMWELT

Politik › Cyberkrieg: Es droht eine Cyber-Rüstungsspirale

Cyberkrieg

Es droht eine Cyber-Rüstur

Russische Hacker sollen Clintons Wahlkampf gestört u
Beweisen lässt sich das nicht. Konsequenzen werden

SCHUMANN

Gibt es eine neue Rüstungsspirale - in der Cyberwelt? Der Westen reagieren.... FOTO: REUTERS

A programmer shows an example of a ransomware cy
Pressphoto Agency)

n-tv

Suchen auf n-tv.de

Home | Politik | Wirtschaft | Börse | Sport | Panorama | Unterhaltung | Technik | Ratgeber | Wisser

WISSEN | REISE | BERUF & CH

4 % EUR/USD 1,1179

Startseite » Panorama » Viele Schäden noch unentdeckt : Europol zählt 200.000 Opfer bei Cyber-Angriff

PANORAMA

Europol-Chef Wainwright hegt keine große Hoffnung, dass die Urheber der Attacke jemals überführt werden können.

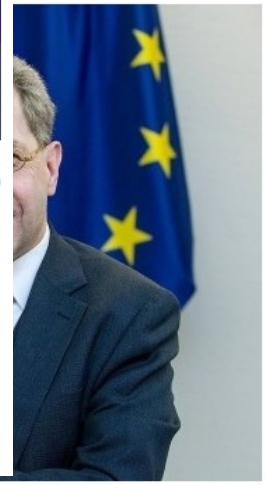
(Foto: picture alliance / dpa)

Sonntag, 14. Mai 2017

Viele Schäden noch unentdeckt

Europol zählt 200.000 Opfer bei Cyber-Angriff

Die Zahl der betroffenen Computer bei der weltweiten Cyber-Attacke am Freitag ist noch größer als bisher bekannt. Die Polizeibehörde Europol zählt bereits 200.000 Opfer. Viele Firmen und Behörden dürften den Angriff aber noch gar nicht bemerkt haben.



Breites Angriffsarsenal

Charakteristik Cyber-Bedrohungen

Attraktivität von Cyber-Kriminalität:

Anonymität, geringe Kosten, ortsunabhängig

Asymmetrisches Setting:	 Angreifer	 Verteidiger
Aktionsraum:	Transnational	National
Aktion/Reaktion:	Zentral	Dezentral
Relation Aufwand/ Erfolg:	Niedrig	Hoch
Rechtliche Einschränkungen:	Keine	Vorhanden

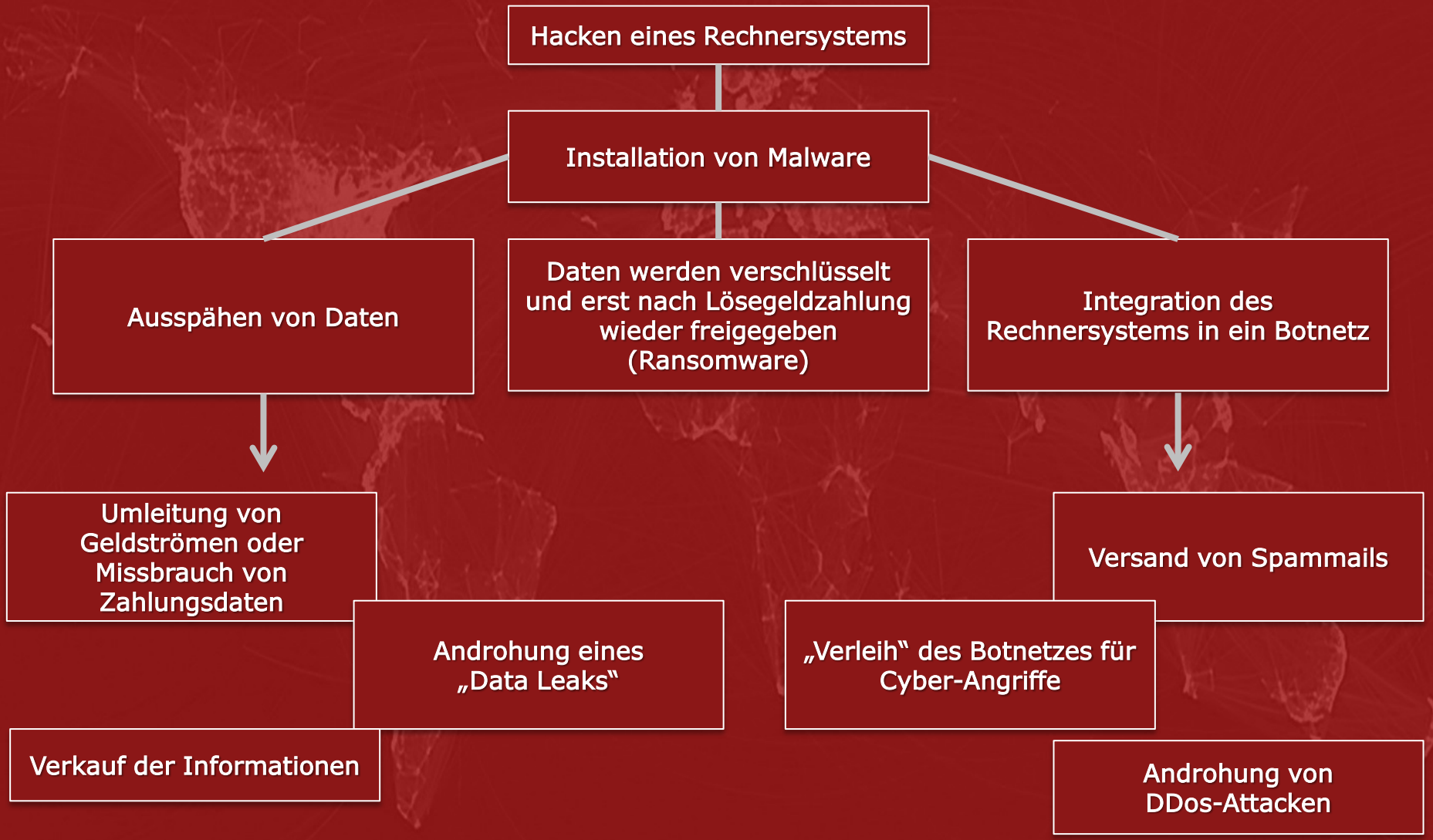
1920	1940	1970/80	Gegenwart
Alkohol, Glücksspiel	Schwarzmärkte in der Nachkriegszeit	Ausweitung des globalen Drogenmarktes	Organisierter Cybercrime

Traditionelle organisierte Kriminalität	Organisierte Cyber-Kriminalität
Sabotage	Blockieren von Logistikketten, Hijacken der Produktionssteuerung
Spionage	Diebstahl Geistigen Eigentums (Patente, Projekte, Formeln)
Geldwäsche	Geldwäsche durch digitale Währungen z.B. beim Autokauf
Drogenhandel	Handel illegaler Substanzen im Darknet

Seit 2009
verdient die organisierte Kriminalität mehr Geld mit Cyber-Crime als mit Drogenhandel!

Schadenspotential:
BRD: 50 Mrd. EUR
Weltweit: 1 Bio. $

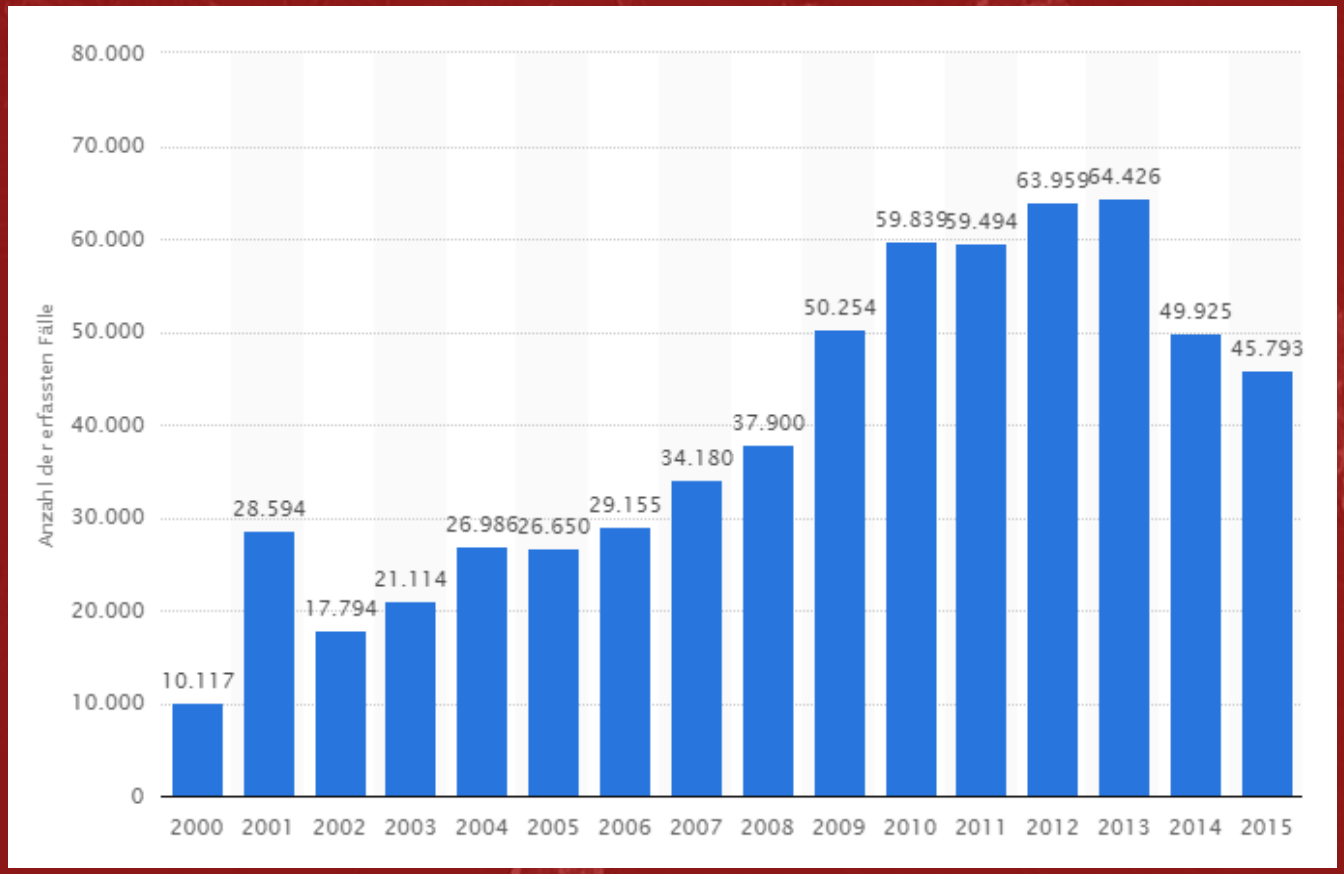
Wertschöpfungskette Cyber-Kriminalität



Motivation der Angreifer

Sabotage	• Blockieren von Logistikketten • Sabotage der Produktionssteuerung • Manipulation von Fahrzeugfunktionen
Spionage	• Gewinnung sensibler Kundendaten • Diebstahl von Produktionsplänen und geistigem Eigentum
Erpressung	• Zahlung von Lösegeld durch betroffene Unternehmen
Dienstleistung	• Hackerangriffe im Darknet als Dienstleistung verfügbar • z.B. DDos-Attacken auf wirtschaftliche Konkurrenten

Geringe Strafverfolgung und Problem der Attribution



Polizeilich erfasste Fälle von Cyber-Kriminalität im engeren Sinne in Deutschland
(Quelle: Statista)

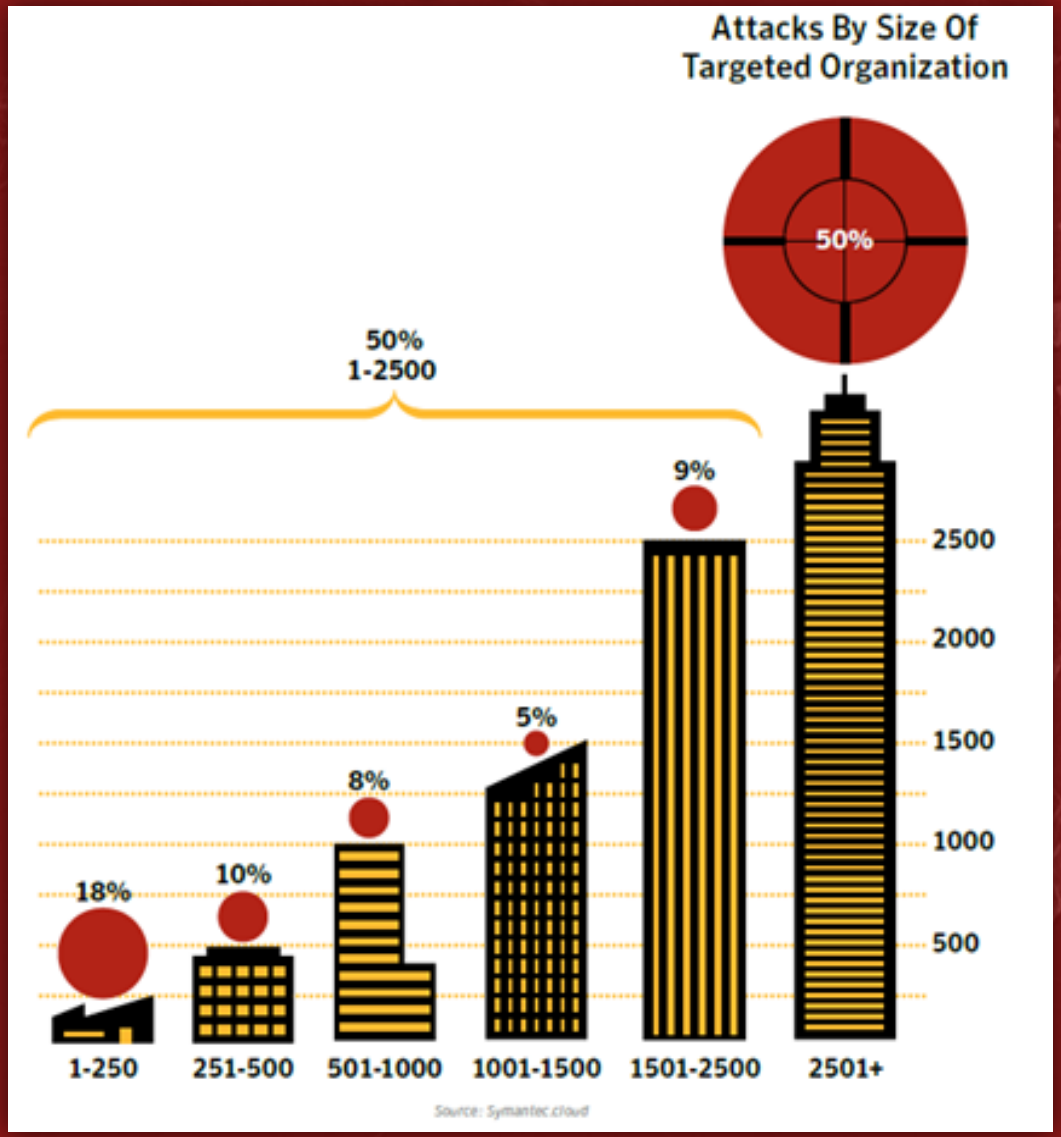
Nur 10% der Delikte werden angezeigt

Nichtaufklärung von 75%

Attribution als generelles und umfassendes Problem

Aufklärung nur durch Kombination von Technik und Intelligence möglich

Wer wird angegriffen?



(c) Symantec

Neben Großunternehmen sind auch KMUs betroffen

Großunternehmen und Zulieferer sind im Verhältnis 50% - 50% Opfer von Attacken

Durchschnittliche Kosten für Cybersicherheitsvorfall:
~861.000 $ für Großunternehmen
~86.500 $ für KMU

Großes Risiko für Liefer- und Produktionsketten, insbesondere bei der Industrie 4.0

Steigende Anforderungen an ein komplexes unternehmens-übergreifendes Qualitäts- und Sicherheitsmanagement

Folgen von Cyber-Angriffen auf Unternehmen

Produktionsausfälle oder Rückrufaktionen

Verlust von langfristigen Investitionen in Forschung und Entwicklung

Verlust von Geistigem Eigentum

Verlust von Wettbewerbsvorteilen für Unternehmen und für den gesamten Wirtschaftsstandort

Konsequenzen

- Reputationsschäden
- Umsatzverlust
- Verlust technologischen Vorsprungs

Interessenslage zu Cyber-Sicherheit im Unternehmen

Entscheidungsebene

Budgetplanung

Haftung

Reputation

Versicherung

Technisch-operative Ebene

Budgetfreigabe

Schutzbedarf

Report an Entscheidungsebene

Cyber-Sicherheit in Deutschland: Staatliche Institutionen

Bundesministerien:

- Bundesministerium des Innern — **BMI**
- Bundesministerium für Verkehr und digitale Infrastruktur — **BMVI**
- Bundesministerium der Finanzen — **BMF**

Bundesämter:

- Bundesnachrichtendienst — **BND**
- Bundesamt für Verfassungsschutz — **BfV**
- Bundeskriminalamt — **BKA**
- Bundesamt für Sicherheit in der Informationstechnik — **BSI**

Gremien:

- Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit — **Bundesbeauftragte für Datenschutz**
- Deutscher Bundestag — **Ausschuss „Digitale Agenda“ dt. Bundestag**
- Nationaler Cyber-Sicherheitsrat — **Nationale Cyber-Sicherheitsrat**
- Nationales Cyber-Abwehrzentrum — **Nationales Cyber-Abwehrzentrum**

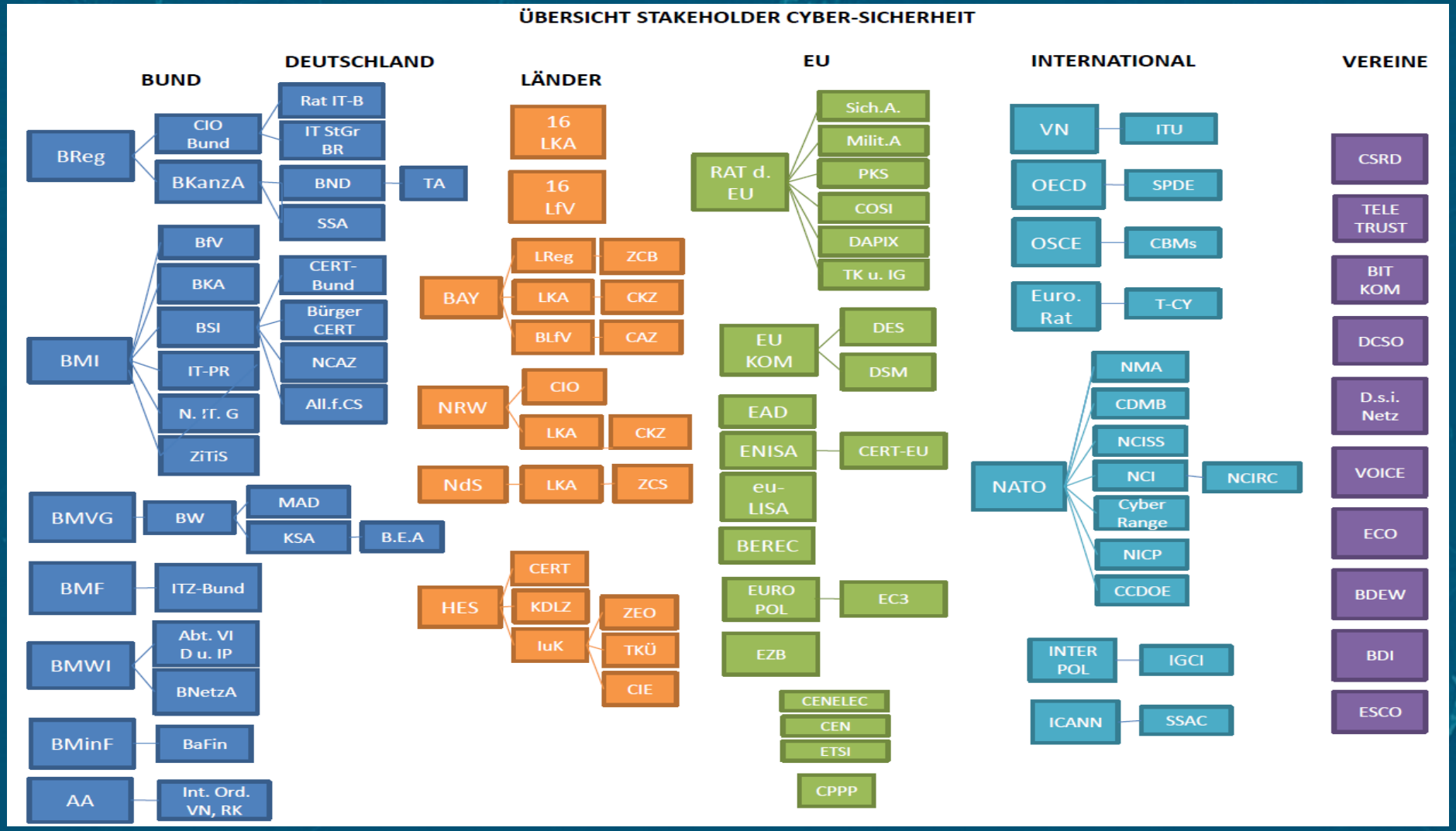
Ministerien und Landesämter der Länder:

z.B. Zentrale Ansprechstellen für Cyber-Crime der LKAs

Neu

- Bundesministerium der Verteidigung — **Abteilung Cyber / IT im BMVg *(CIT)***
- Bundeswehr — **Organisationsbereich Cyber und Informationsraum *(CIR)***
- ZITIS — **Zentrale Stelle für Informationstechnik im Sicherheitsbereich**
- Bundesministerium für Wirtschaft und Technologie — **Digitale Strategie 2025 (Forderung nach Digitalagentur)**

„Übersicht“ Cyber-Sicherheit in Deutschland: Akteure



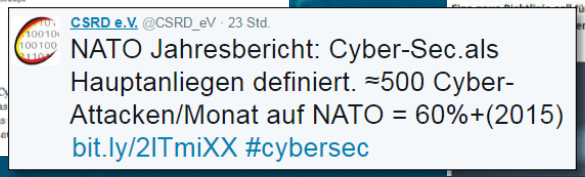
Gesetzliche Rahmenbedingungen

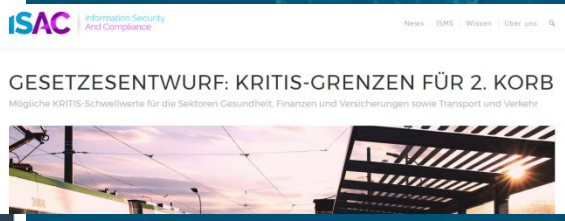
Cybersicherheitsstrategie 2016 der Bundesregierung

IT-Sicherheitsgesetz der Bundesregierung (2015)

NIS-Richtlinie der Europäischen Union (2016)

DSGVO der Europäischen Union (2016)





Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz, 2015)

Bundesamt für Sicherheit in der Informationstechnik

Diskussionspunkte:

- Definition ‚Stand der Technik'
- Umsetzung Korb I & Korb II – Ungleichbehandlung der Sektoren
- Systemrelevanz von KRITIS-Betreibern unterhalb der Schwellenwerte
- Studie CyberArk: bei 30% der betroffenen KRITIS-Betreiber noch keine Auseinandersetzung oder Einleitung entsprechende Vorkehrungen
- Verhältnis der Forderungen und Leistungen des BSI

Internationaler Vergleich: Staatsausgaben für Cyber-Sicherheit

Frankreich	UK	USA	Deutschland
Loi de programmation militaire	*Spending review 2014:*	*President´s Fiscal Year Budget 2017:*	*Cyber-Sicherheitsstrategie für Deutschland 2016:*
1 Mrd. € (2014 – 2019)	**3,2 Mrd. £** (2014-2019)	**19 Mrd. $** (2017)	**?**

Kooperation als Abwehrstrategie

Digitale Transformation

Cyber-Bedrohungen

Cyber-Sicherheit

Herausforderungen identifizieren

Awareness schaffen

Vernetzung von Entscheidungsträgern

Kooperation als Umsetzungsmomentum

Fortschritt ermöglichen

Synergieeffekte entfalten

Cyber-Sicherheitsrat Deutschland e.V.

Awareness schaffen für eine vertrauensvolle nationale sowie internationale branchen- und sektorübergreifende Zusammenarbeit mit allen Stakeholdern

Ausbau des globalen Netzwerks

HexaTrust – Cybersecurity & Digital Trust Alliance (FRA)

Cyber-Sicherheitsrat Deutschland e.V.
Gemeinsam in eine sichere Digitale Zukunft.
www.cybersicherheitsrat.de

Ben Gurion Universität des Negev (ISR)

Information Assurance Advisory Council (UK)

National Cyber-Forensics & Training Alliance (USA)

Internet Security Alliance (USA)

Cyber-Sicherheitsrat Deutschland e.V.

Vielen Dank für Ihre Aufmerksamkeit!

Cyber-Sicherheitsrat Deutschland e.V.

Hans-Wilhelm Dünn, Generalsekretär

Georgenstr. 22
10117 Berlin
Tel.: +49 - (0)30 6796365 - 28
Fax.: +49 - (0)30 6796365 - 29

www.cybersicherheitsrat.de
facebook.com/cybersicherheitsrat