



# Cybersicherheit

## Bedrohungslage und Herausforderungen

Managementsitzung Cybersicherheit, 10.07.2019





# Cybercrime ist real



Quelle: BSI vom 13.06.2018,  
[https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Cyber\\_Angriffe\\_auf\\_deutsche\\_Energieversorger\\_13062018.html](https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Cyber_Angriffe_auf_deutsche_Energieversorger_13062018.html)



# Hacking the solar grid



Quelle: <https://horusscenario.com>



# Cybercrime ist real

## FLUGSICHERHEIT

# Wenn der Hacker fliegen lernt

**Der Hackerangriff auf die polnische Fluggesellschaft Lot zeigt: Luftfahrtunternehmen kümmern sich zu wenig um IT-Sicherheit. Dabei wäre es technisch sogar möglich, Flugzeuge in der Luft zu kapern – per Smartphone.**

Quelle: Handelsblatt online vom 23.06.2015,  
<https://www.handelsblatt.com/unternehmen/handel-konsumgueter/flugsicherheit-per-smartphone-ins-navigationssystem/11954222-2.html>

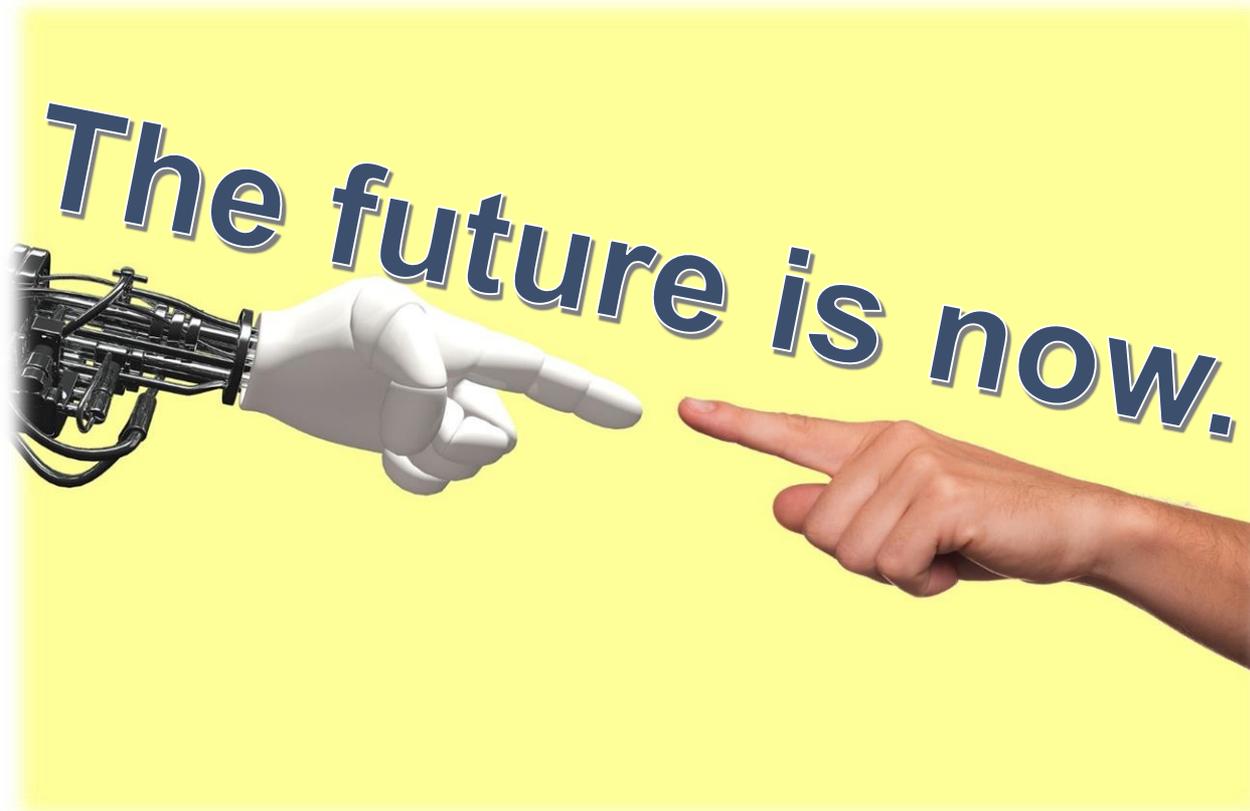


# IoT-Disclaimer





# Praxischeck





# Beispiel

 Alert! 07.03.2014 11:53 Uhr | Security

## Hack gegen AVM-Router: Fritzbox-Lücke offengelegt, Millionen Router in Gefahr

Die Schonfrist ist abgelaufen: Im Netz kursieren Details, wie man die kritische Schwachstelle in den Fritzboxen ausnutzt. Das bedeutet akute Gefahr, da nach Erkenntnissen von heise Security noch immer sehr viele AVM-Router verwundbar sind.

Quelle: Heise vom 07.03.2014

<https://www.heise.de/security/meldung/Hack-gegen-AVM-Router-Fritzbox-Luecke-offengelegt-Millionen-Router-in-Gefahr-2136784.html>



## MIRAI-IOT-BOTNET

# IP-Kamera nach 98 Sekunden mit Malware infiziert

Droht die Netzwerkapokalypse, sobald ein unsicheres IoT-Gerät im Heimnetzwerk angeschlossen wurde? Der Sicherheitsforscher Rob Graham hat es ausprobiert - und sich innerhalb von 98 Sekunden die erste Infektion abgeholt.

21. November 2016, 12:30 Uhr, Hauke Gierow

Quelle: Golem.de vom 21.11.2016

<https://www.golem.de/news/mirai-iot-botnet-ip-kamera-nach-98-sekunden-mit-malware-infiziert-1611-124602.html>





# Cybercrime ist allgegenwärtig

**Møller-Mærsk**

## **Hackerangriff kostet Reederei Hunderte Millionen**

Mit Erpressersoftware haben Angreifer die größte Container-Reederei der Welt zeitweise lahmgelegt. Die Unternehmensgruppe A.P. Møller-Mærsk schätzt den Schaden auf bis zu 300 Millionen Dollar.



Quelle: Spiegel online vom 16.08.2017

<http://www.spiegel.de/netzwelt/netzpolitik/moller-m-rsk-cyberangriff-kostet-reederei-hunderte-millionen-a-1163111.html>



# Cybercrime ist innovativ

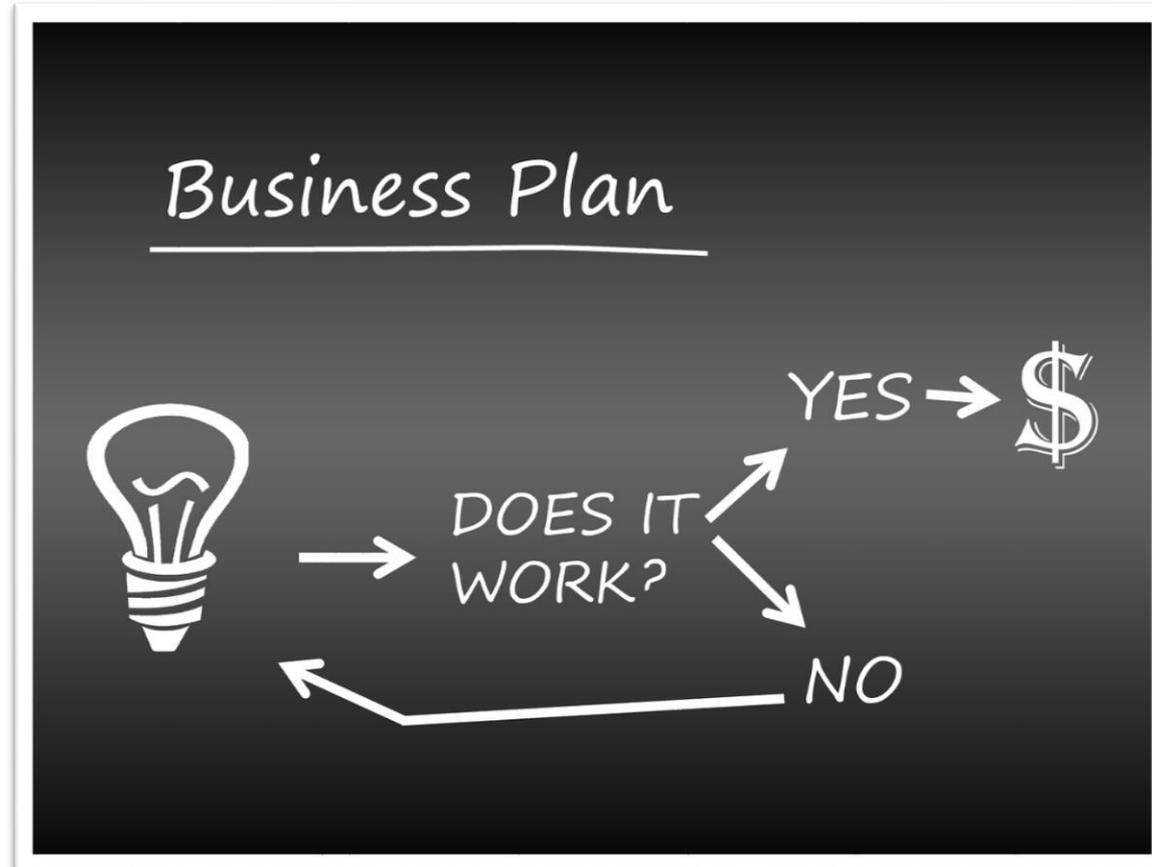
ANDY GREENBERG SECURITY 08.22.18 05:00 AM

## THE UNTOLD STORY OF NOTPETYA, THE MOST DEVASTATING CYBERATTACK IN HISTORY

Quelle: Wired, 22.08.2018,  
<https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>



# Cybercrime ist ein Geschäft





## Cybercrime ist ein Geschäft - Schadenssummen

- ➔ **\$870,000,000**  
Pharmakonzern Merck
- ➔ **\$400,000,000**  
FedEx (->TNT Express)
- ➔ **\$384,000,000**  
Saint-Gobain
- ➔ **\$300,000,000**  
Reederei Maersk
- ➔ **\$188,000,000**  
Mondelēz
- ➔ **\$129,000,000**  
Reckitt Benckiser
- ➔ **\$10 Milliarden**  
**Gesamtschaden durch**  
**NotPetya**, Schätzung der  
US-Regierung

Quelle: <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>



# Cybercrime ist professionell





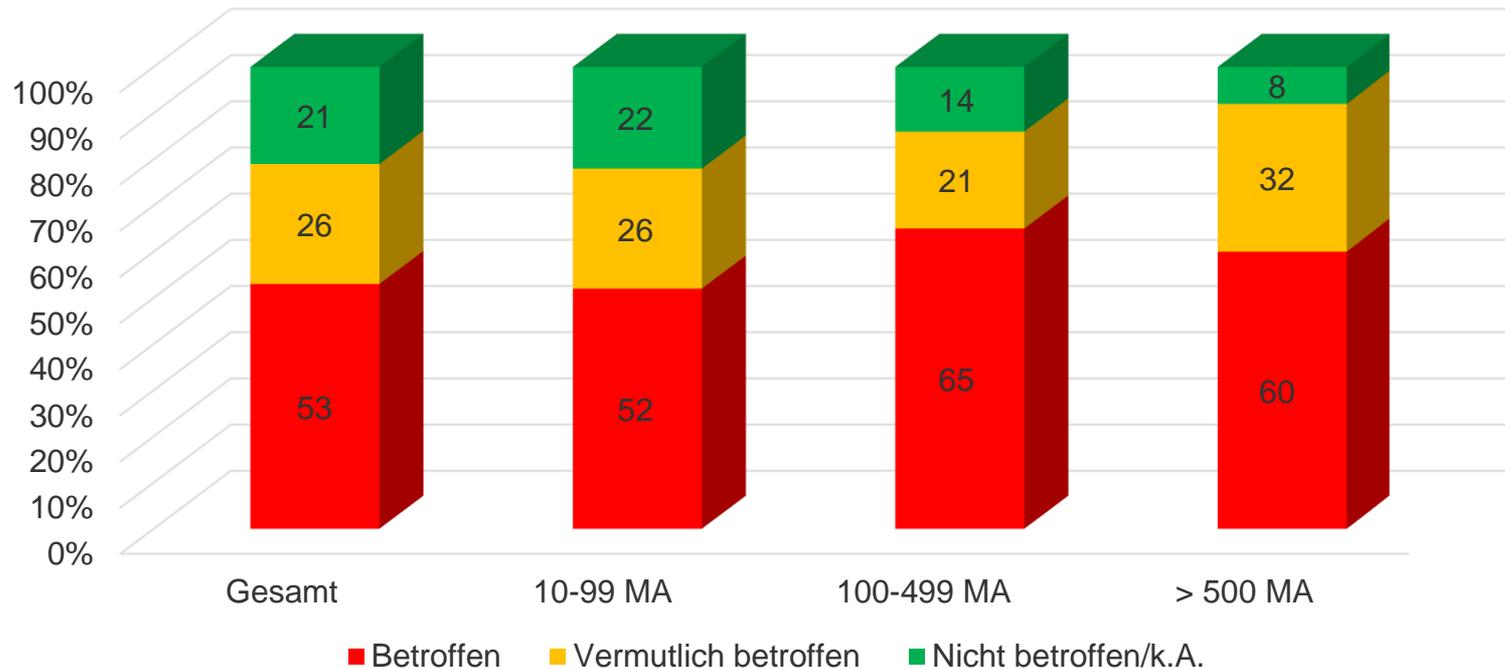
# Cybercrime as a Service





## Studie Bitkom – Wirtschaftsschutz in der digitalen Welt, 21.07.2017

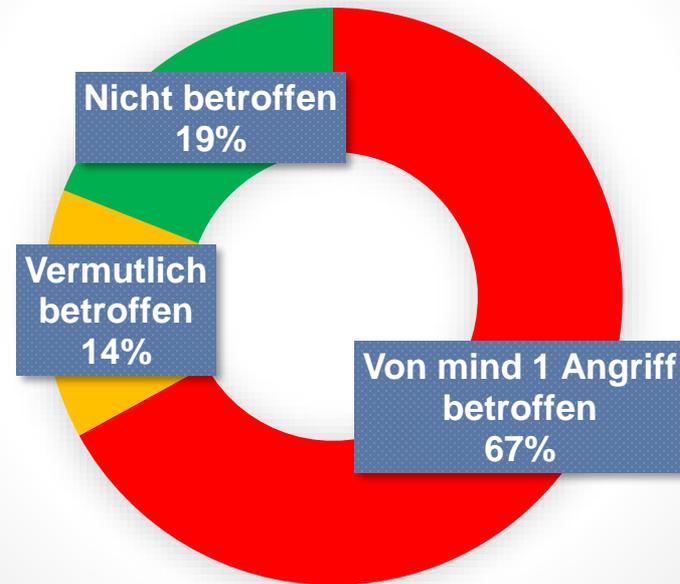
War Ihr Unternehmen in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen?





## Studie Bitkom Research: Status Quo IT-Sicherheit in Deutschen Unternehmen, Oktober 2017

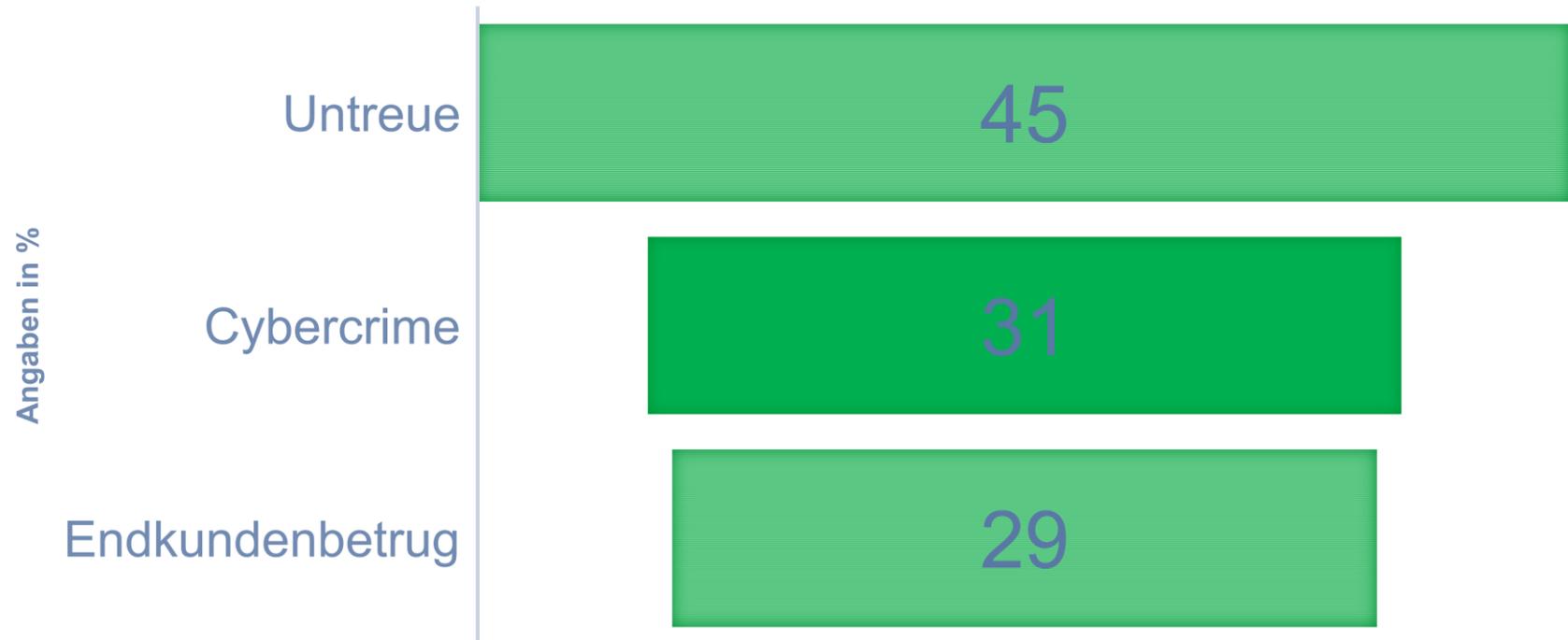
War Ihr Unternehmen innerhalb der letzten 12 Monate von IT-Sicherheitsvorfällen betroffen bzw. vermutlich betroffen?





# PWC Global Economic Crime and Fraud Survey 2018

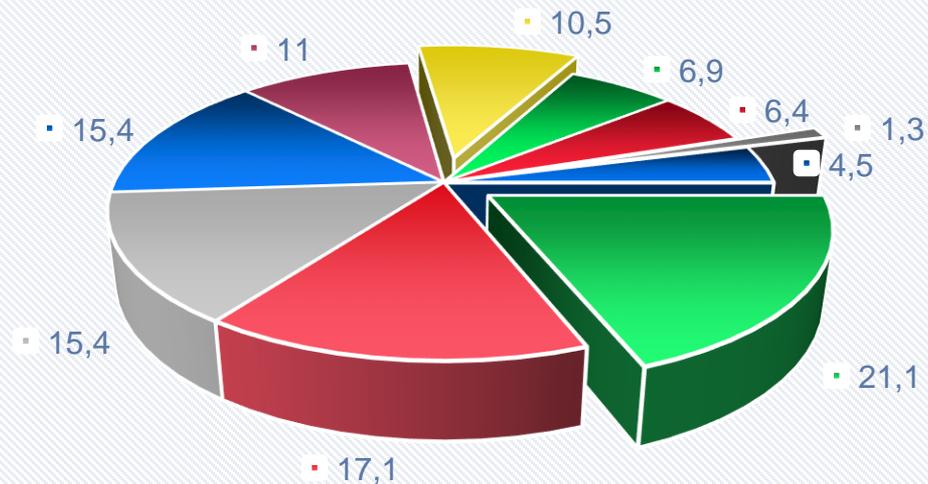
WELCHES SIND DIE HÄUFIGSTEN DELIKTSFORMEN IM BEREICH WIRTSCHAFTSKRIMINALITÄT UND BETRUG?





## Studie Bitkom – Wirtschaftsschutz in der digitalen Welt, 21.07.2017

### 109,6 Milliarden Euro Schaden in den letzten zwei Jahren



- Kosten für Ermittlungen und Ersatzmaßnahmen
- Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen
- Patentrechtsverletzungen
- Imageschaden/negative Medienberichterstattung
- Kosten für Rechtsstreitigkeiten
- Ausfall, Diebstahl, Schädigung von Systemen oder Betriebsabläufen
- Umsatzeinbußen durch Plagiate



# Schaden: Social Engineering meets Tech Attack



CHIEF EXECUTIVE OFFICER  
**FRAUD**



# Ausmaß (Quelle: <https://www.ic3.gov/media/2018/180712.aspx>)



**Jul 12, 2018**  
Alert Number  
**I-071218-PSA**

**BUSINESS E-MAIL COMPROMISE THE 12 BILLION DOLLAR SCAM**

This Public Service Announcement (PSA) is an update and companion to

The following BEC/EAC statistics were reported to the IC3 and are derived from multiple sources, including IC3 and international law enforcement complaint data and filings from financial institutions between **October 2013 and May 2018**:

Domestic and international incidents:	78,617
Domestic and international exposed dollar loss:	\$12,536,948,299



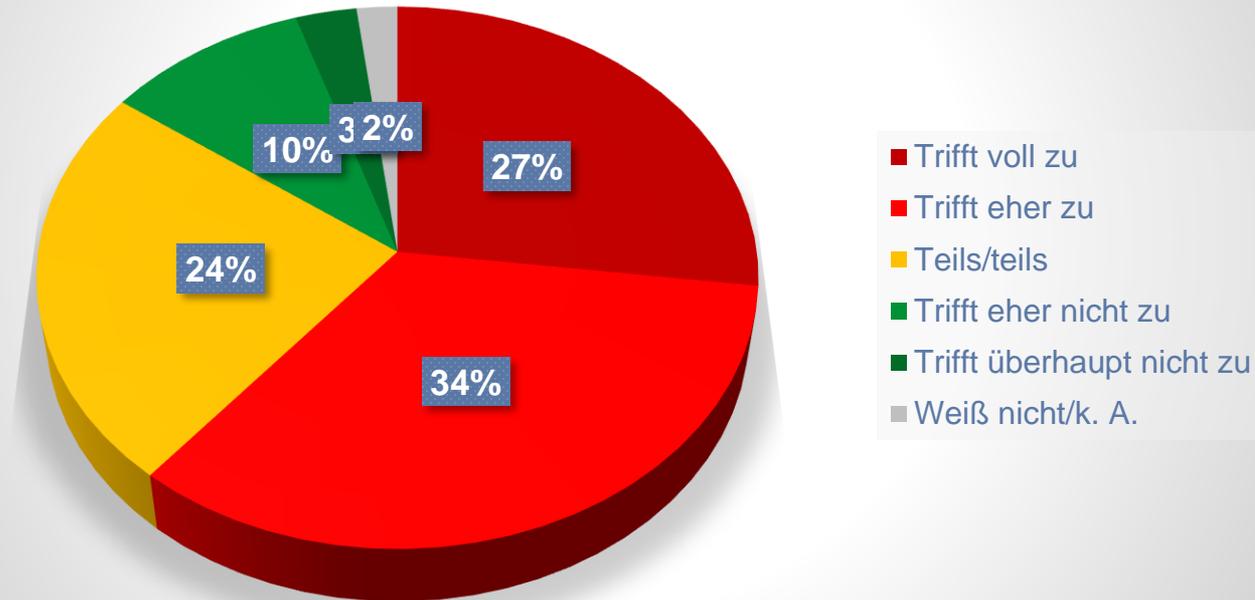
# Neue Erscheinungsformen





## Studie Bitkom Research: Status Quo IT-Sicherheit in Deutschen Unternehmen, Oktober 2017

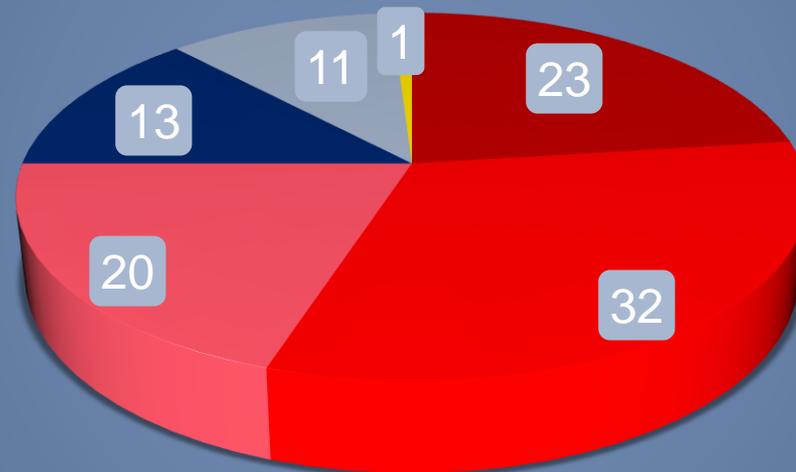
“Das Risiko, von IT-Angriffen geschädigt zu werden, ist für unser Unternehmen sehr groß.”





## Studie Bitkom Research: Status Quo IT-Sicherheit in Deutschen Unternehmen, Oktober 2017

"Wir sind der Auffassung, dass man IT-Angriffe vollständig verhindern kann."

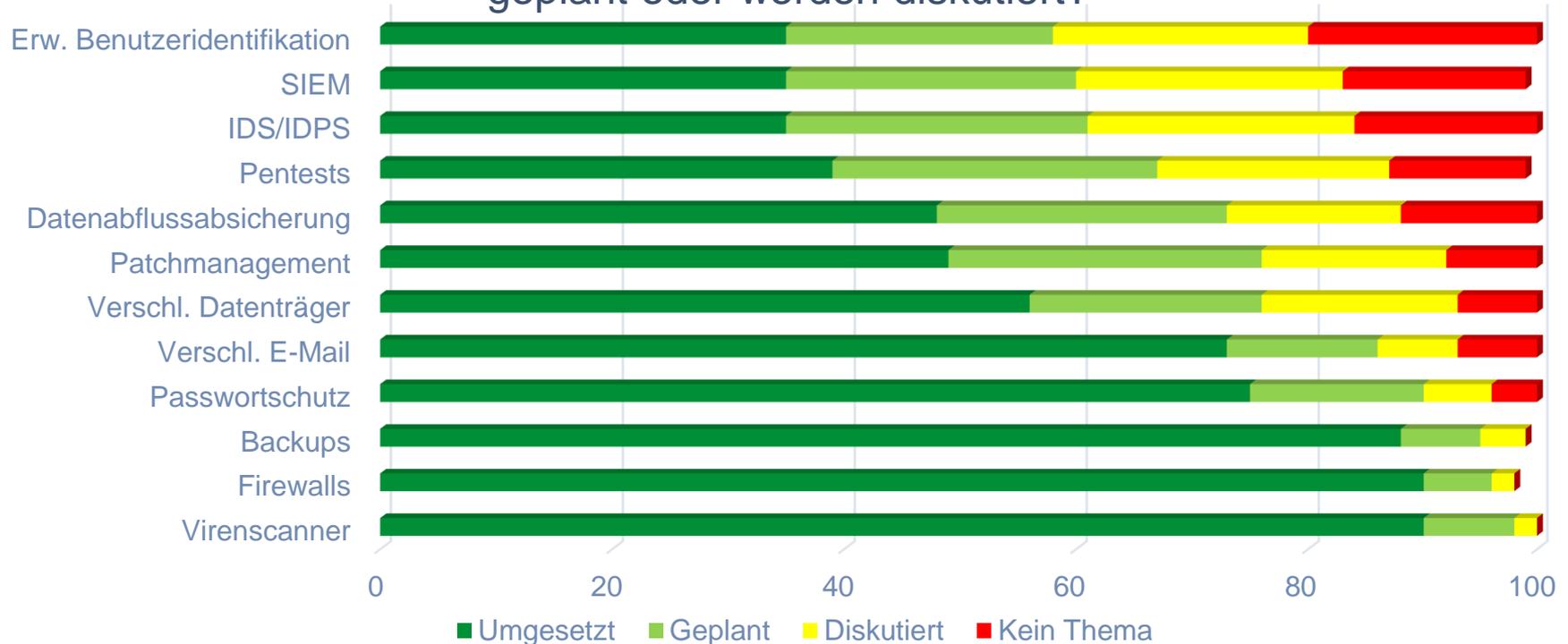


■ Triift voll zu ■ Triift eher zu ■ Teils/teils ■ Triift eher nicht zu ■ Triift überhaupt nicht zu ■ Weiß nicht/k.A.



# Studie Bitkom Research: Status Quo IT-Sicherheit in Deutschen Unternehmen, Oktober 2017

Welche IT-Sicherheitsmaßnahmen sind umgesetzt, geplant oder werden diskutiert?







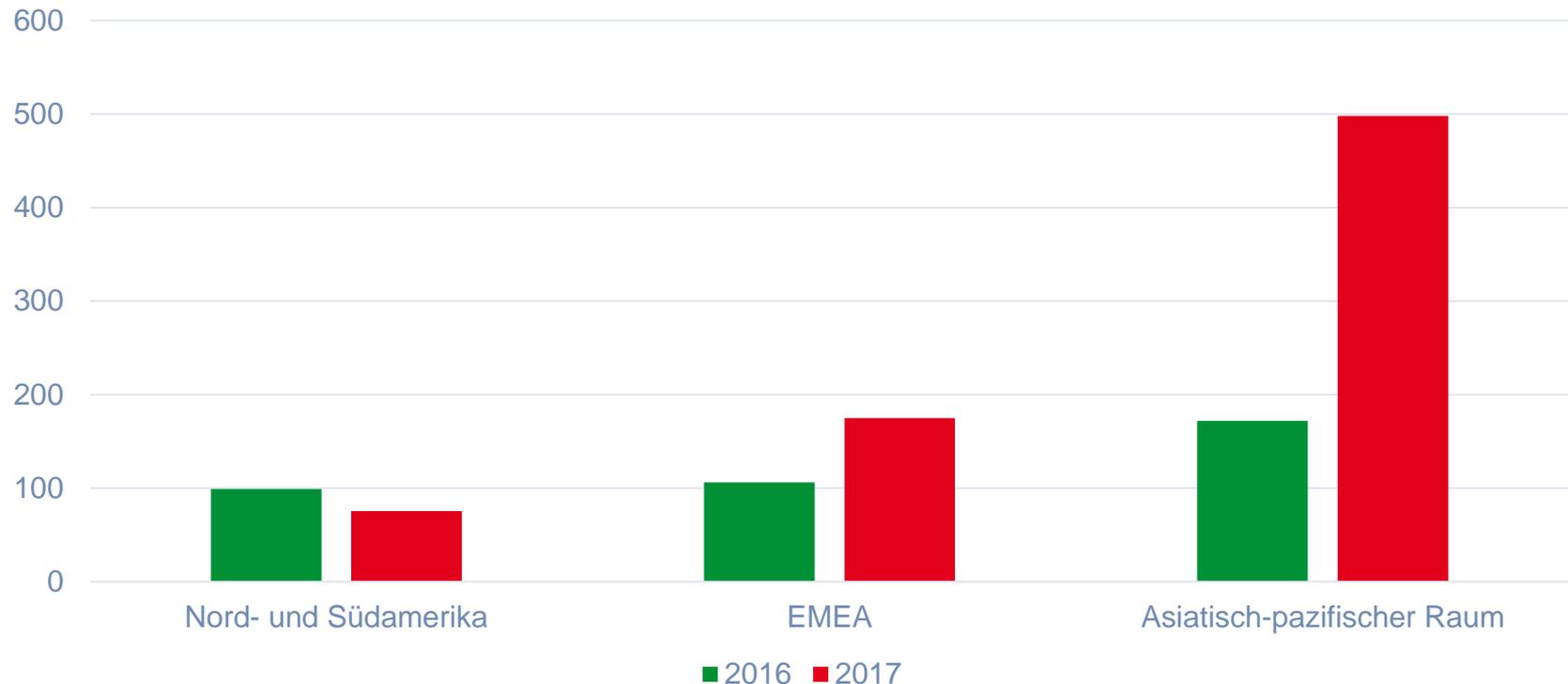
# Die Folgen: APT - Die unterschätzte Gefahr





# Mandiant M-Trends 2018 Report

## Medianwert der Verweildauer im Netzwerk in Tagen





# Das Milka-Problem

**WIRTSCHAFT** MALWARE „NOTPETYA“

## Dieser Fall entscheidet, ob Hacken eine Kriegswaffe ist

Veröffentlicht am 14.12.2018 | Lesedauer: 5 Minuten

Von **Benedikt Fuest**

Quelle:

<https://www.welt.de/wirtschaft/article185510234/Notpetya-Dieser-Fall-entscheidet-ob-Hacken-eine-Kriegswaffe-ist.html>



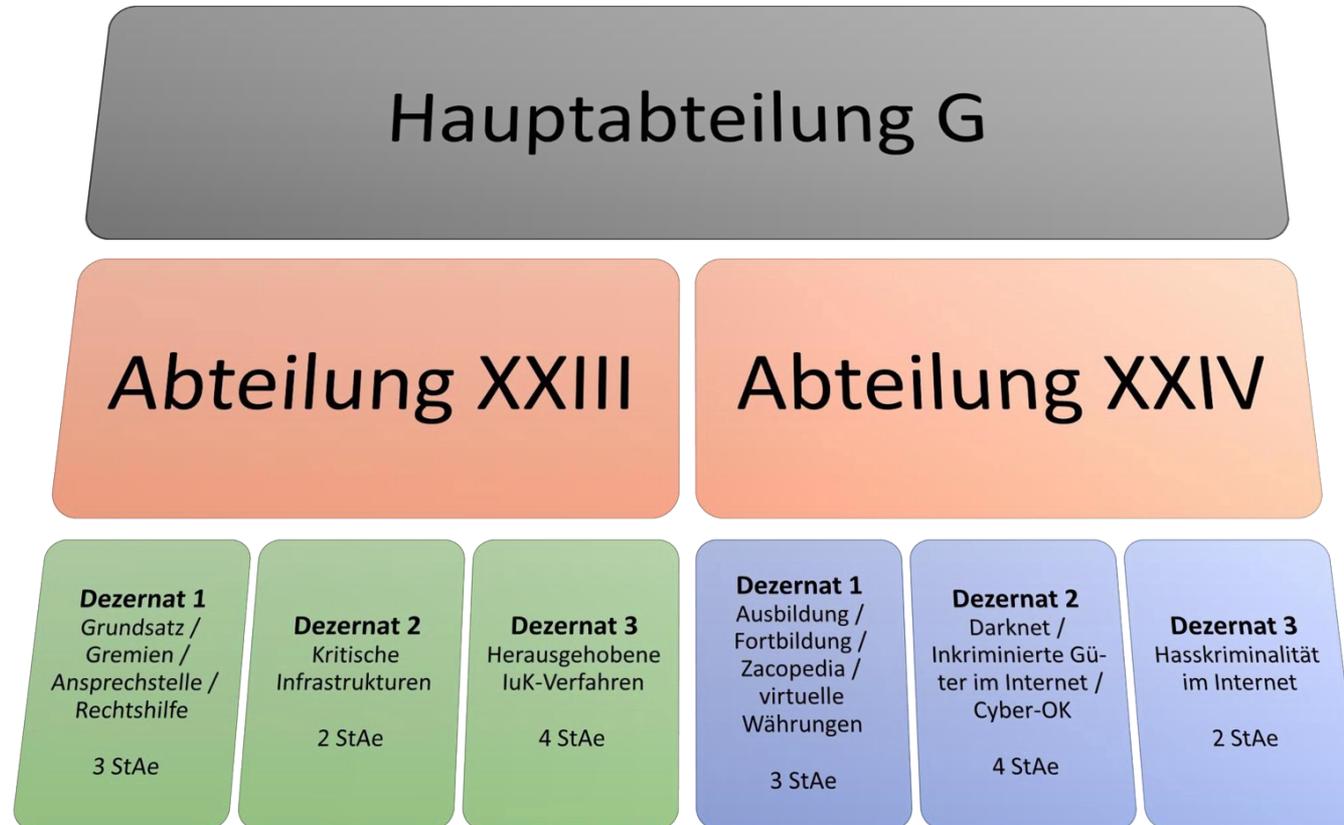


# Die Antwort der Justiz





# ZAC NRW – Aufbau und Struktur





## § 143 Abs. 4 GVG





## Blick auf die Republik

# Zentralstellen der Länder





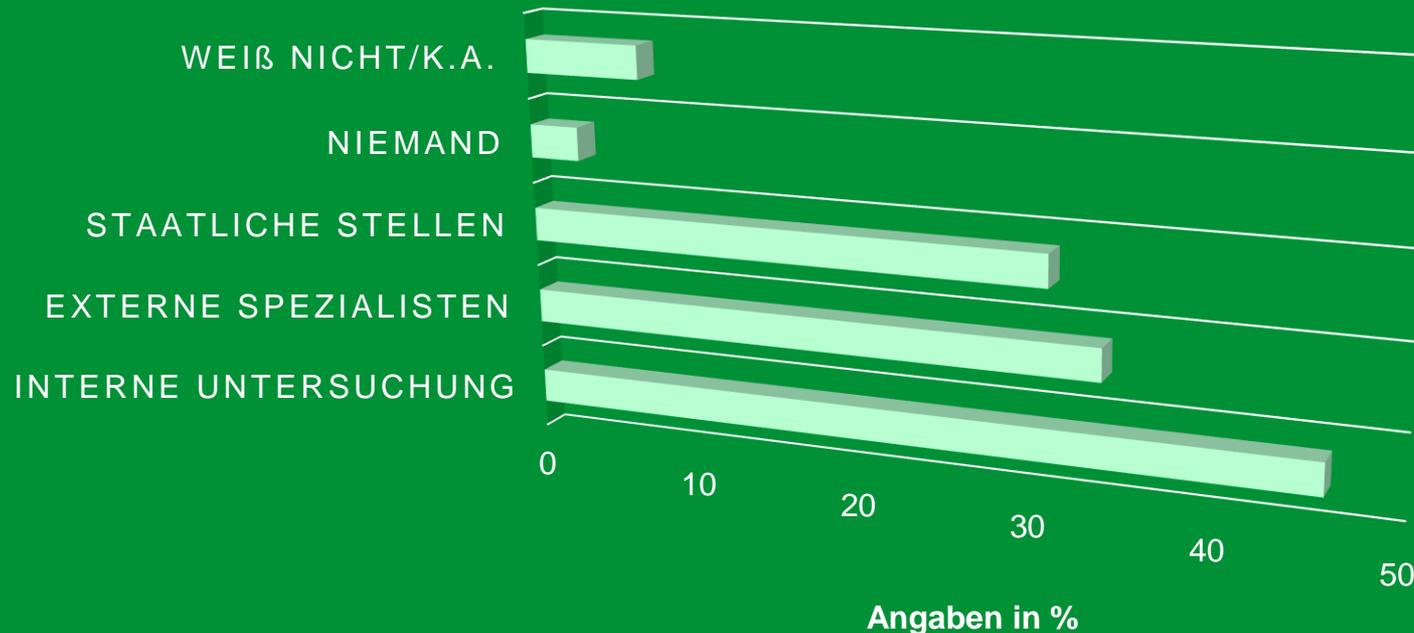
# Thesen aus und für die Praxis





Quelle: Bitkom, Wirtschaftsschutz in der digitalen Welt, 21.07.2017

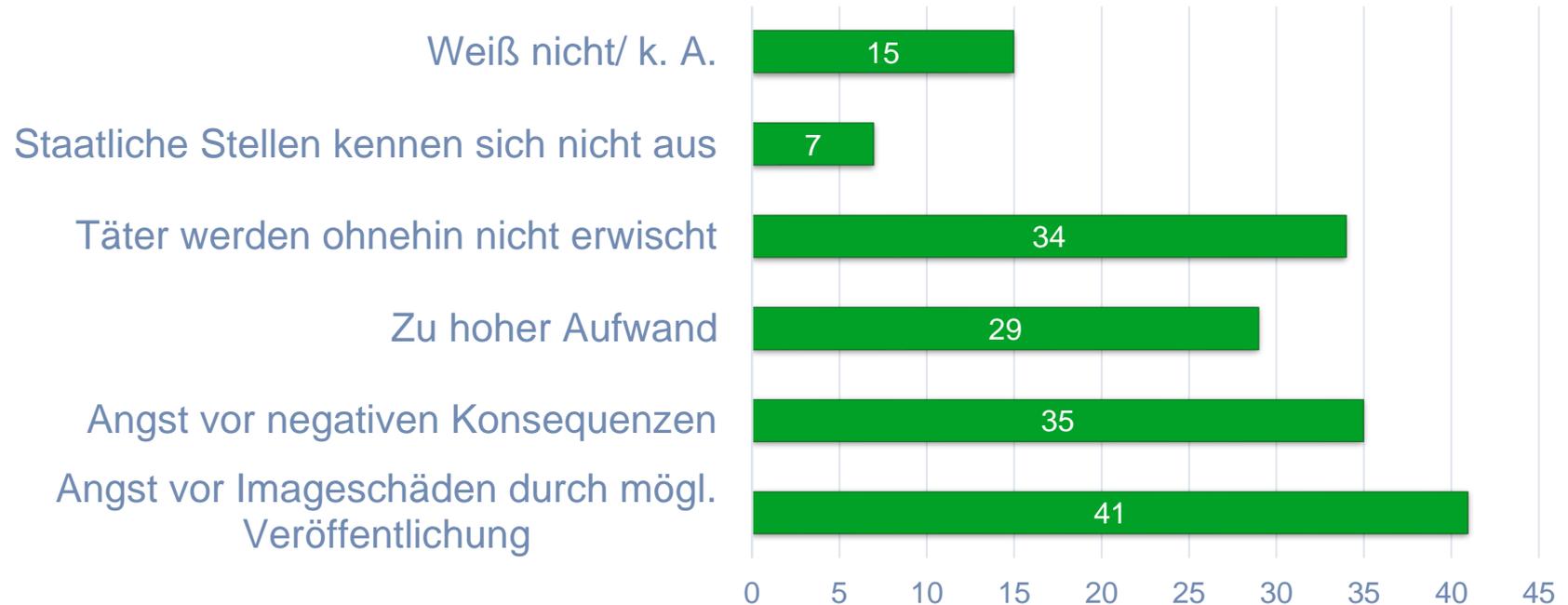
## VERTRAUENSFRAGE: WER HAT DIE IT-SICHERHEITSVORFÄLLE UNTERSUCHT?





Quelle: Bitkom, Wirtschaftsschutz in der digitalen Welt, 21.07.2017

## Aus welchen Gründen hat Ihr Unternehmen keine staatlichen Stellen eingeschaltet?





# Angst vor Imageschäden durch Veröffentlichung





# Angst vor negativen Konsequenzen





# Zu hoher Aufwand



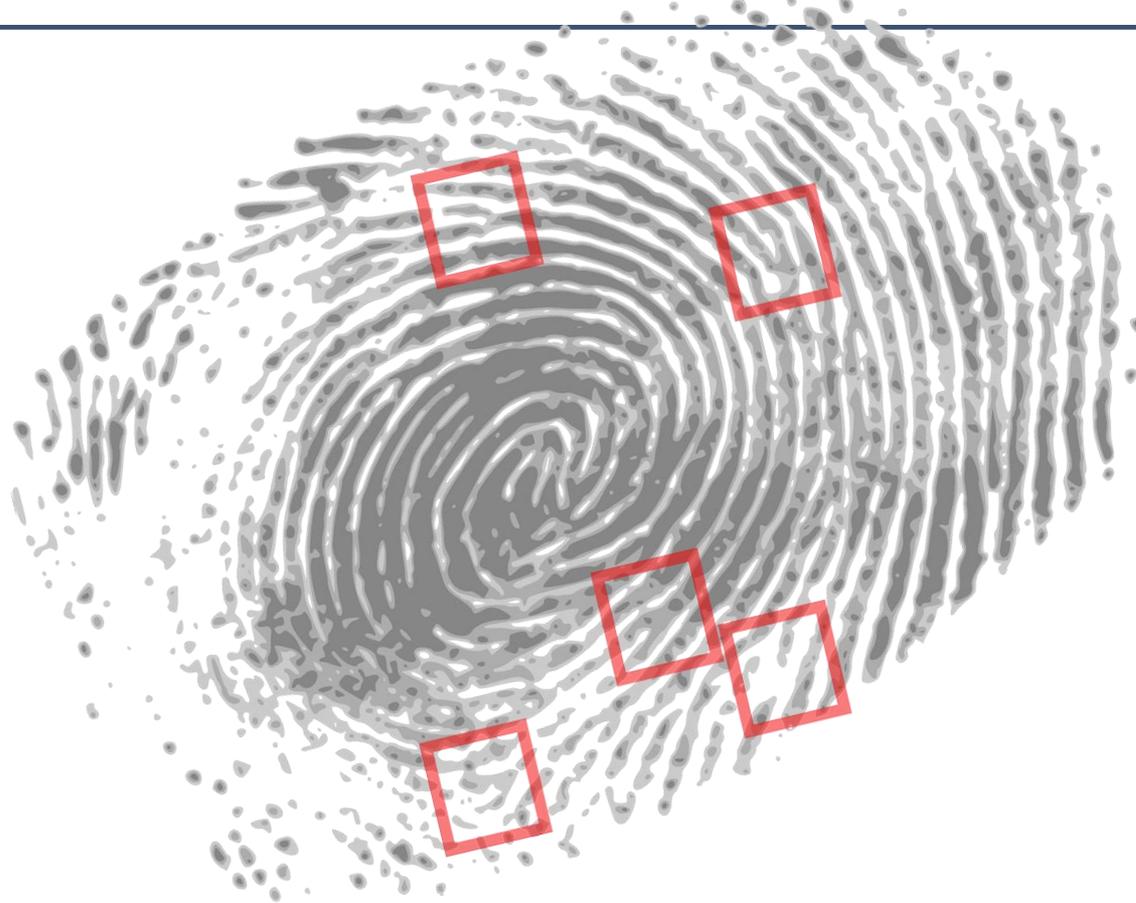


# Ein positiver Blick





# Beweissicherung



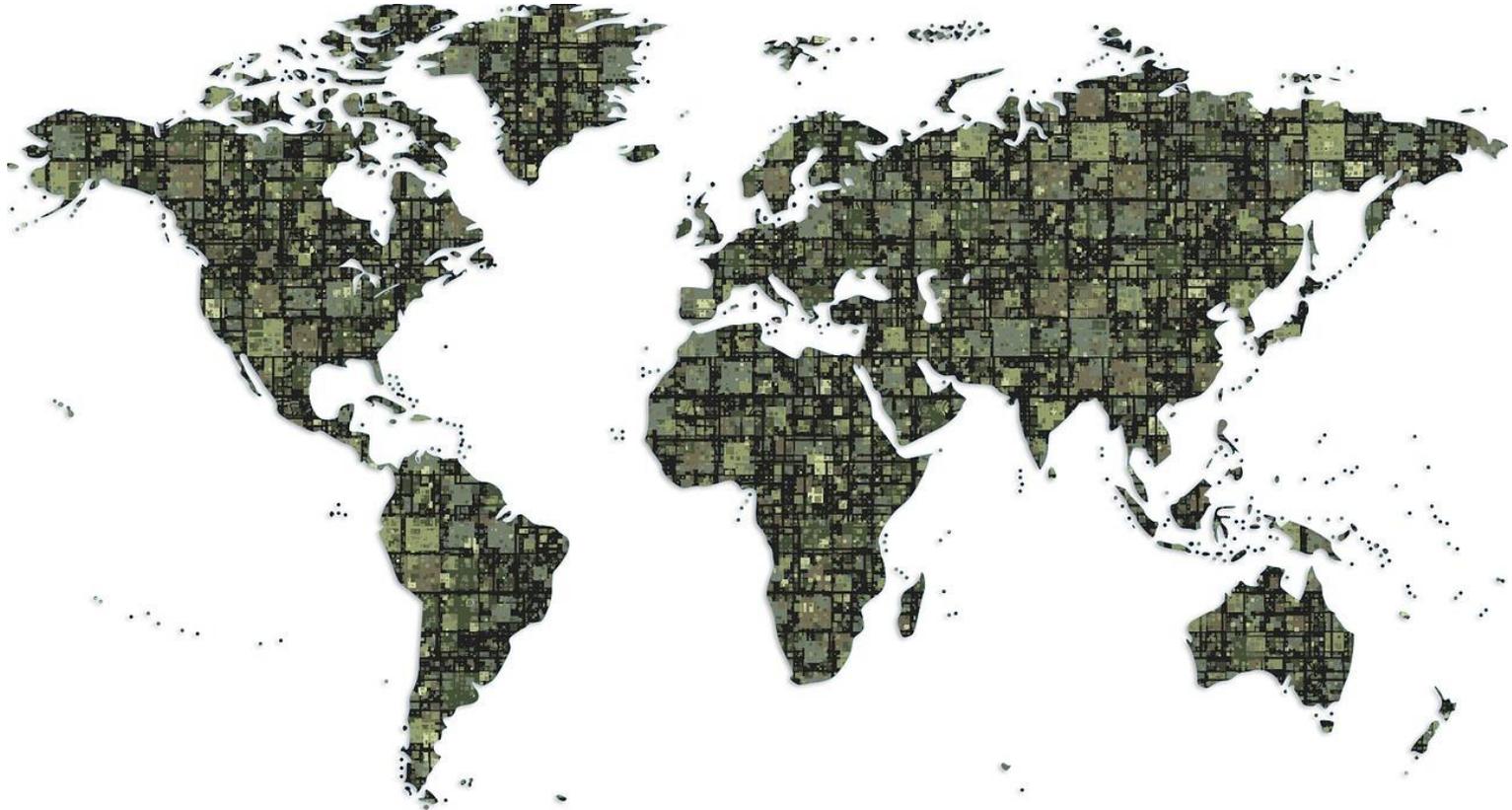


# Dunkelfeld erhellen





# Internationale Maßnahmen





# Täter werden ohnehin nicht erwischt (!?)





## Täter werden nicht erwischt?

**DREI MONATE NACH DEM MEGA-ANGRIFF AUF MILLIONEN ROUTER**

# Telekom-Hacker in London festgenommen!

Quelle: bild.de vom 23.02.2017

<https://www.bild.de/news/ausland/hacker-angriff/telekom-hacker-in-london-festgenommen-50564682.bild.html>





# Was tun im Krisenfall?





## Ein wesentlicher Beitrag





# Strategie

Crime as a  
Service

VS

Prosecution  
as a Service



## Pres. Trump, Debattenbeitrag vom 26.09.2016

“It is - it is a huge problem.  
I have a son. He's 10 years old.  
He has computers. He is so good  
with these computers, it's unbelievable.  
The security aspect of cyber is very,  
very tough. And maybe it's hardly doable.”

Quelle: <https://www.washingtonpost.com/news/the-fix/wp/2016/09/27/the-answer-that-best-exemplifies-how-badly-donald-trump-was-out-of-his-depth-in-the-debate>



## Pres. Obama, Stanford Summit 2015

**“This has to be a shared mission. Government cannot do it alone, and the private sector cannot do this alone either. There’s only one way to defend America [...] government and private sector working together as true partners.”**

Quelle: forbes.com vom 13.02.2015

<https://www.forbes.com/sites/katevinton/2015/02/13/obama-signs-executive-action-calls-for-collaboration-to-fight-cyber-attacks-at-stanford-summit/>





# Vielen Dank für Ihre Aufmerksamkeit!



## Markus Hartmann

Oberstaatsanwalt als Hauptabteilungsleiter

Leiter der ZAC NRW

[markus.hartmann@sta-koeln.nrw.de](mailto:markus.hartmann@sta-koeln.nrw.de)

(0221) 477-4426

## 24/7-Hotline (0221) 477-4922

Bildquellen (soweit nicht anders angegeben): [pixabay.com](https://pixabay.com) / CC0

