Aktuelle
Internet-Sicherheitshinweise

Gefährliche Anhänge in Bewerbungsmails!

Donnerstag 28. September 2017

tagesschau

LKA Niedersachsen

Landeskriminalamt Niedersachsen
Dezernat 38 - Zentralsstelle Cybercrime
Christian Pursche

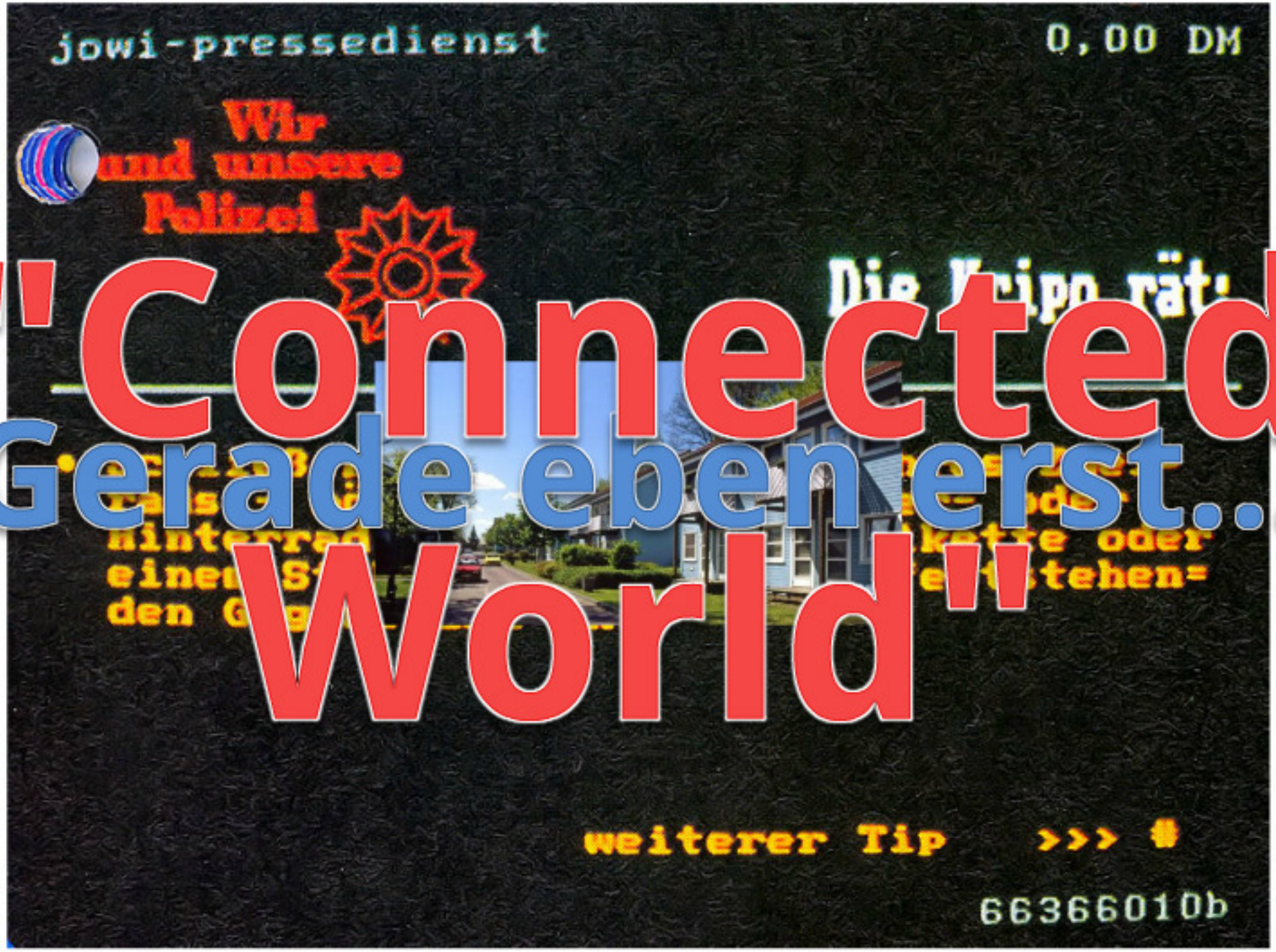

Single Point of Contact
Unabhängige Informationsquelle zu aktuellen Cybercrime-Phänomenen
Technische Beratung im Schadensfall
Unterstützung bei der Sensibilisierung der Mitarbeiter

Zentrale Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft			
	Land/Bund	Telefonnummer	E-Mailadresse
	Bundeskriminalamt	+49 611 55-16684	SO41-NKC@bka.bund.de
	Baden-Württemberg	+49 711 5401-2444	cybercrime@polizei.bwl.de
	Bayern	+49 89 1212-3300	zac@polizei.bayern.de
	Berlin	+49 30 4664-924924	zac@polizei.berlin.de
	Brandenburg	+49 3334 388-8600	cybercrime.fiktiv@polizei.brandenburg.de
	Bremen	+49 421 362-3853	cybercrime@polizei.bremen.de
	Hamburg	+49 40 4286-75455	zac@polizei.hamburg.de
	Hessen	+49 6 .3-3377	zac.hlka@ ei.hessen.de
	M lenburg Vorpom n	.3 3866 64-4545	cybercrim a@polizei.mv.de
	Niedersachsen	+49 511 26262-3804	zac@lka.polizei.niedersachsen.de
	Nordrhein-Westfalen	+49 211 939-4040	cybercrime.lka@polizei.nrw.de
	Rheinland-Pfalz	+49 6131 65-2565	lka.cybercrime@polizei.rlp.de
	Saarland	+49 681 962-2448	cybercrime@polizei.slpol.de
	Sachsen	+49 351 855-3481	zac.lka@polizei.sachsen.de
	Sachsen-Anhalt	+49 391 250-2244	ermittlungen.4c@polizei.sachsen-anhalt.de
	Schleswig Holstein	+49 431 160-4545	cybercrime@polizei.landsh.de
	Thüringen	+49 361 314-1425	cybercrime.lka@polizei.thueringen.de


Gefahren
im
Internet

LKA Niedersachsen

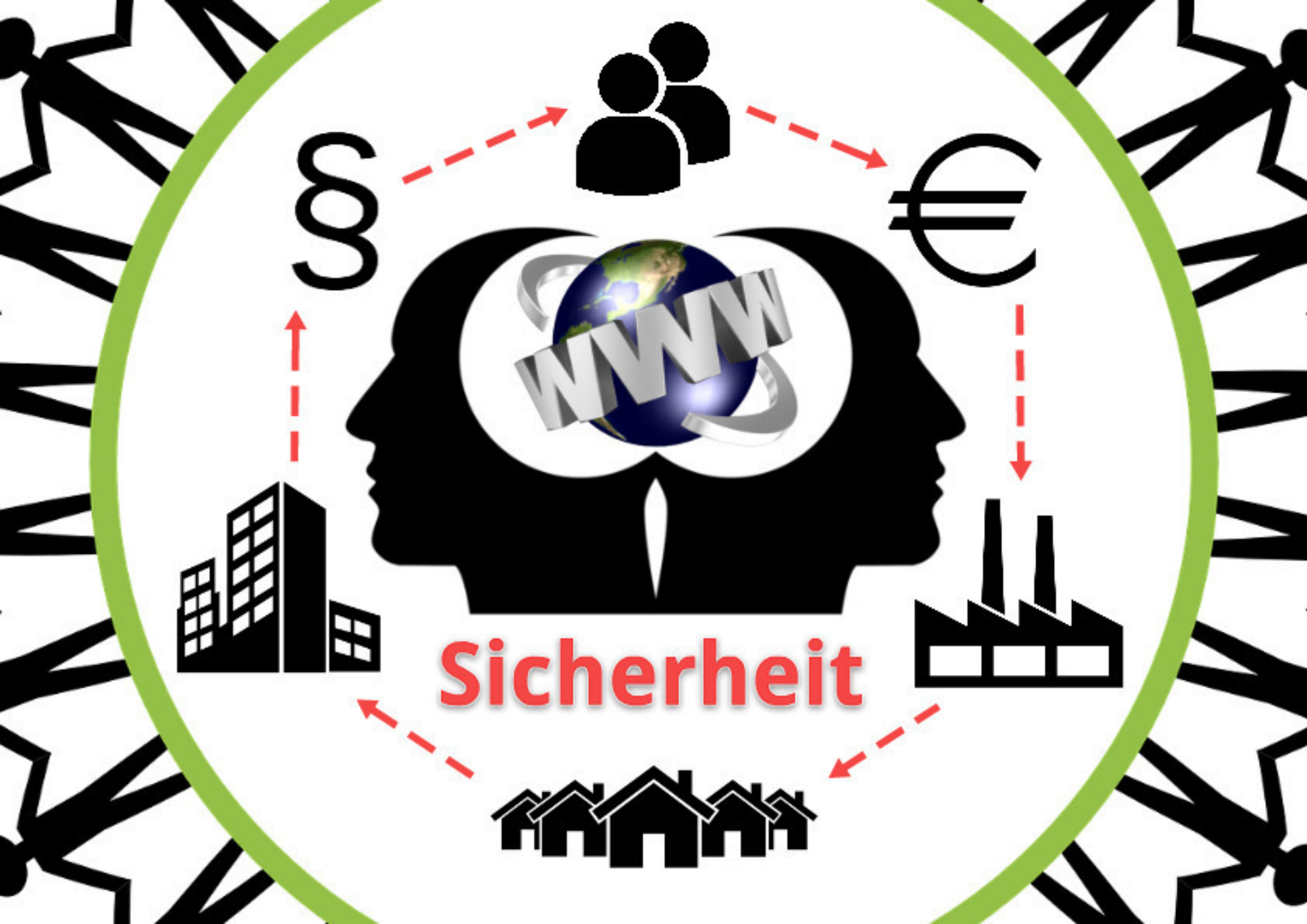
Landeskriminalamt Niedersachsen
Dezernat 38 - Zentralsstelle Cybercrime
Christian Pursche



"Connected World"

Gerade eben erst...


WWW


§
€
WWW
Sicherheit

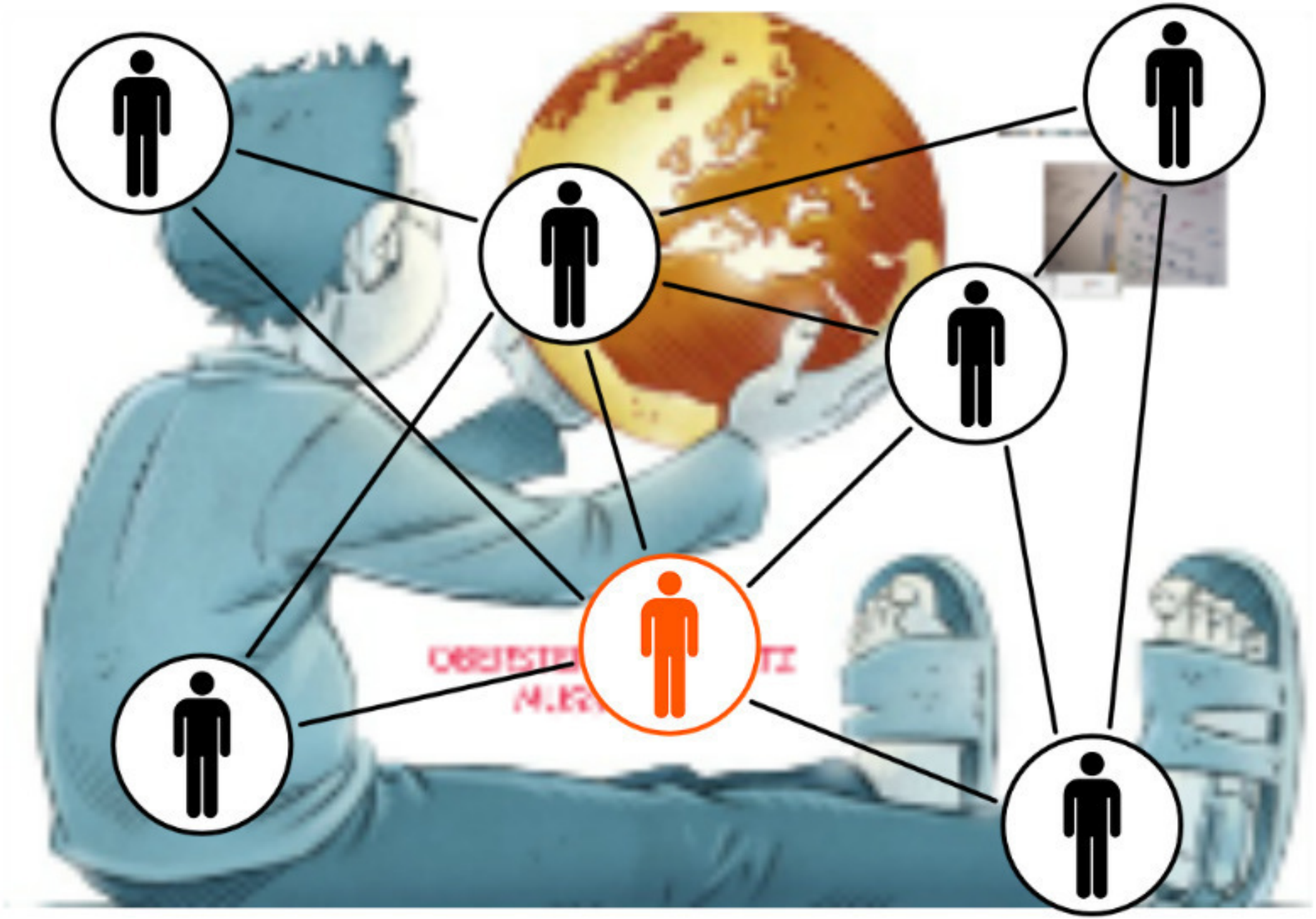

§
€
WWW
Sicherheit

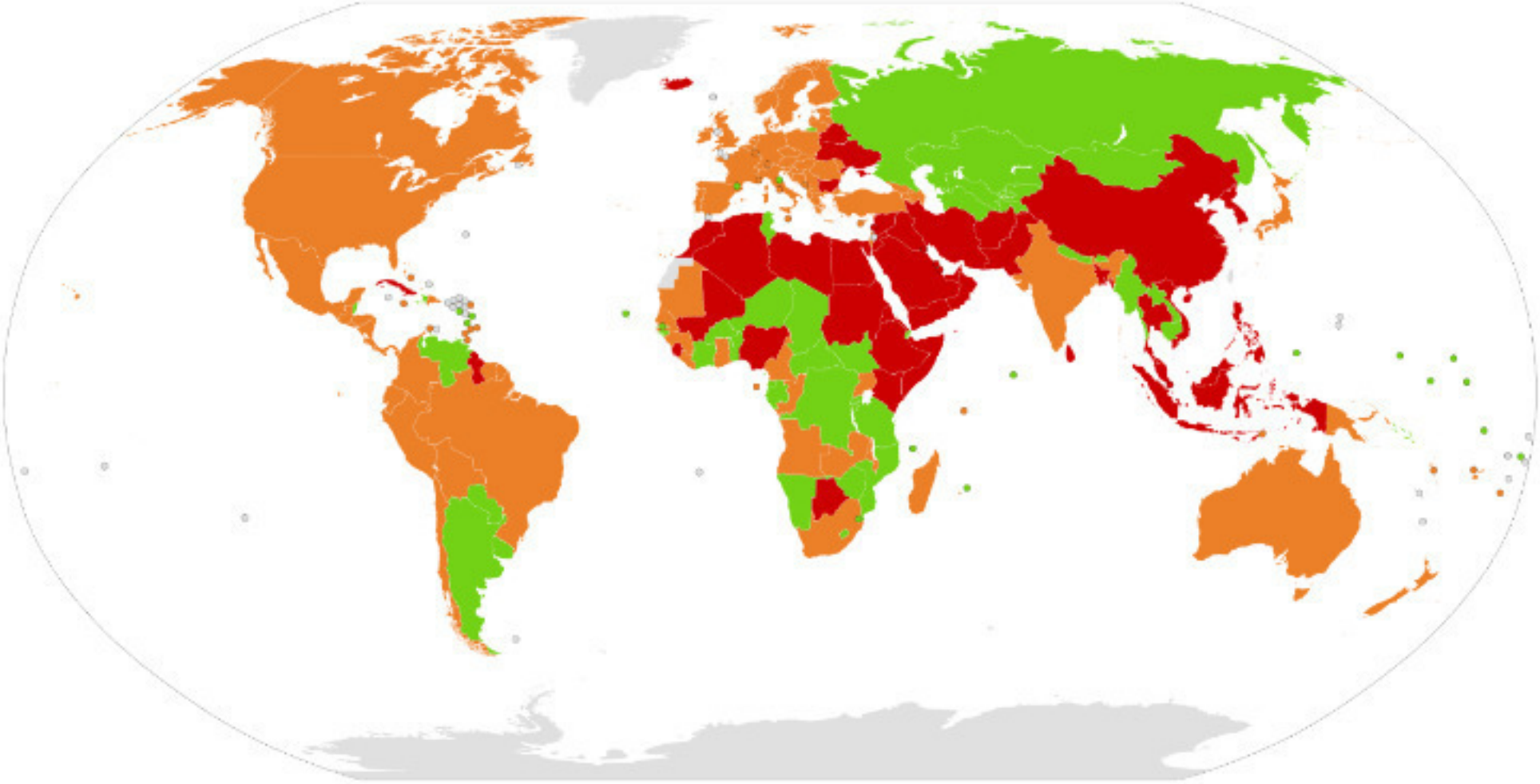

"Faktor
Mensch"
>50%

Prävention - Sensibilisierung - IT-Security Awareness


Bluetooth®
Wi Fi™


Die
Ausnutzbarkeit
der digitalen
Identität
verstehen!
INTERNET
REAL LIFE






DANCE
TO THE


"Faktor
> 50%
Mensch"


3.409.901 123456
1.228.363 123456789
688.456 abc123
648.393 password
585.653 password1
532.441 12345678
235.341 dragon
233.915 1234
213.099 123
193.040 123456a
< Sekunde
> 2.000.000.000
Passwörter/Sekunde


"Bestimmte Dinge muß man einfach einmal gehört haben!"
Microsoft Office-Sicherheitsoptionen
Sicherheitswarnung - Makro
Makro
Makros wurden deaktiviert. Makros können Viren oder sonstige Sicherheitsrisiken enthalten. Aktivieren Sie diesen Inhalt nur, wenn Sie der Quelle dieser Date vertrauen.
Warnung: Es kann nicht festgestellt werden, ob dieser Inhalt aus einer vertrauenswürdigen Quelle stammt. Sie sollten diesen Inhalt deaktiviert lassen, außer wenn von diesem Inhalt wichtige Funktionalität bereitgestellt wird und Sie dessen Quelle vertrauen.
Weitere Informationen
Dateipfad: E:\Patentbearbeitung.dot
Vor unbekanntem Inhalt schützen (empfohlen)
Diesen Inhalt aktivieren
Vertrauensstellungscenter öffnen
OK
Abbrechen
E W E R B U N G
Lebenslauf
Max Muster
Birkenallee 199
Geburtsdatum:
Geburtsort:

Infizierte Joomla-Server verteilen Erpressungs-Trojaner TeslaCrypt

22.02.2016 15:44 Uhr – Jürgen Schmidt

vorlesen

Auch wer seine Mails sorgfältig filtert, läuft Gefahr, sich den Erpressungs-Trojaner TeslaCrypt einzufangen. Auf scheinbar harmlosen Web-Seiten lauern Exploits, die deren Besucher infizieren.

Bislang sah es so aus, als würde TeslaCrypt vor allem via E-Mail verteilt. Versehentlich geöffnete Word-Dateien mit bösartigen Makros waren ein übliches Infektionsszenario. So konzentrierten sich viele zu ihrem Schutz auf den Mail-Eingang. Das könnte fatale Folgen haben; denn mittlerweile kann man sich den Erpressungs-Trojaner auch beim Surfen einfangen.

Der Schädling lauert dabei auf scheinbar harmlosen Seiten und nutzt Sicherheitslücken in Windows beziehungsweise der installierten Software aus, um aktiv zu werden. Kurze Zeit später erscheint dann die Nachricht, dass die Dateien verschlüsselt wurden und nur gegen Zahlung von Bitcoins wieder zu entschlüsseln sind. Die Opfer können auf Dokumente, PDFs, Bilder und anderen Daten nicht mehr zugreifen, denn TeslaCrypt hat daraus verschlüsselte Dateien etwa mit der Endung .mp3 gemacht.

Bitcoin auf Höhenflug

Wechselkurs in US-Dollar je Bitcoin

HANDELSBLATT

Quelle: Bloomberg


"Advanced
Cyber
Crime"

Fast 55 Milliarden Euro Schaden pro Jahr

Schäden in Deutschland in Milliarden Euro (Basis: Selbsteinschätzung)

	Schadenssummen in Mrd. Euro
Kosten für Ermittlungen und Ersatzmaßnahmen	21,1
Umsatzein[illegible]ßen durch V[illegible]st von Wettbew[illegible]bsvorteilen	17,1
Pate[illegible]tzu[illegible]hon[illegible]nmel[illegible]	15,4
Imageschad[illegible]Ki[illegible]n ode[illegible]feranten[illegible]gativ[illegible]dienb[illegible]terstattung	15,4
Kosten f[illegible]ntsstr[illegible]eiten	11,0
Aus[illegible]de[illegible]g von Info[illegible]ions- u[illegible]tionssystemen oder Betriebsabläufen	10,5
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	6,9
Datenschutzrechtliche Maßnahmen (z.B. Information von Kunden)	6,4
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	1,3
Sonstige Schäden	4,5
[illegible]esam[illegible]halb[illegible]hre	[illegible]6

2019

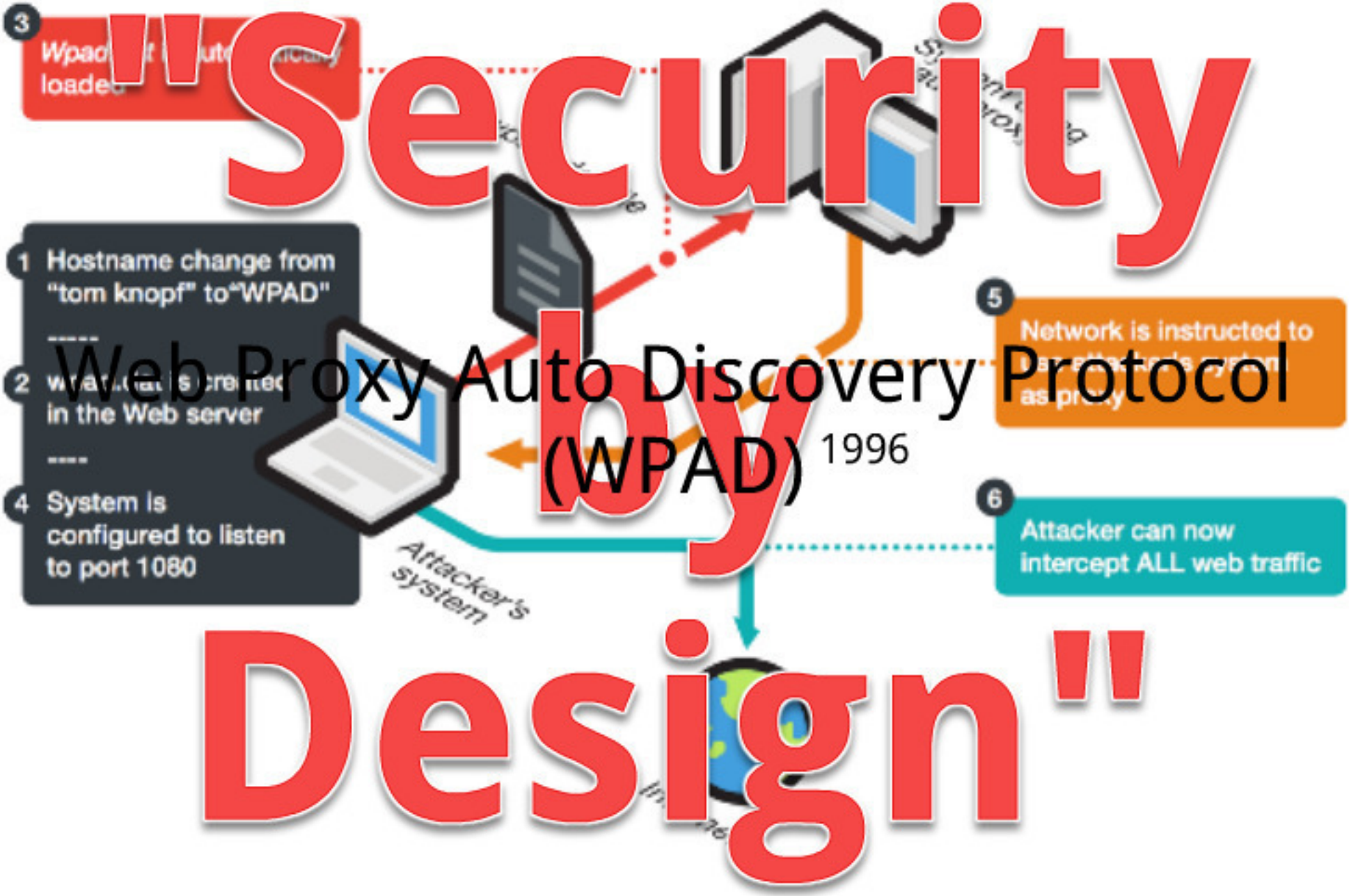
(Juniper Research, 2016)

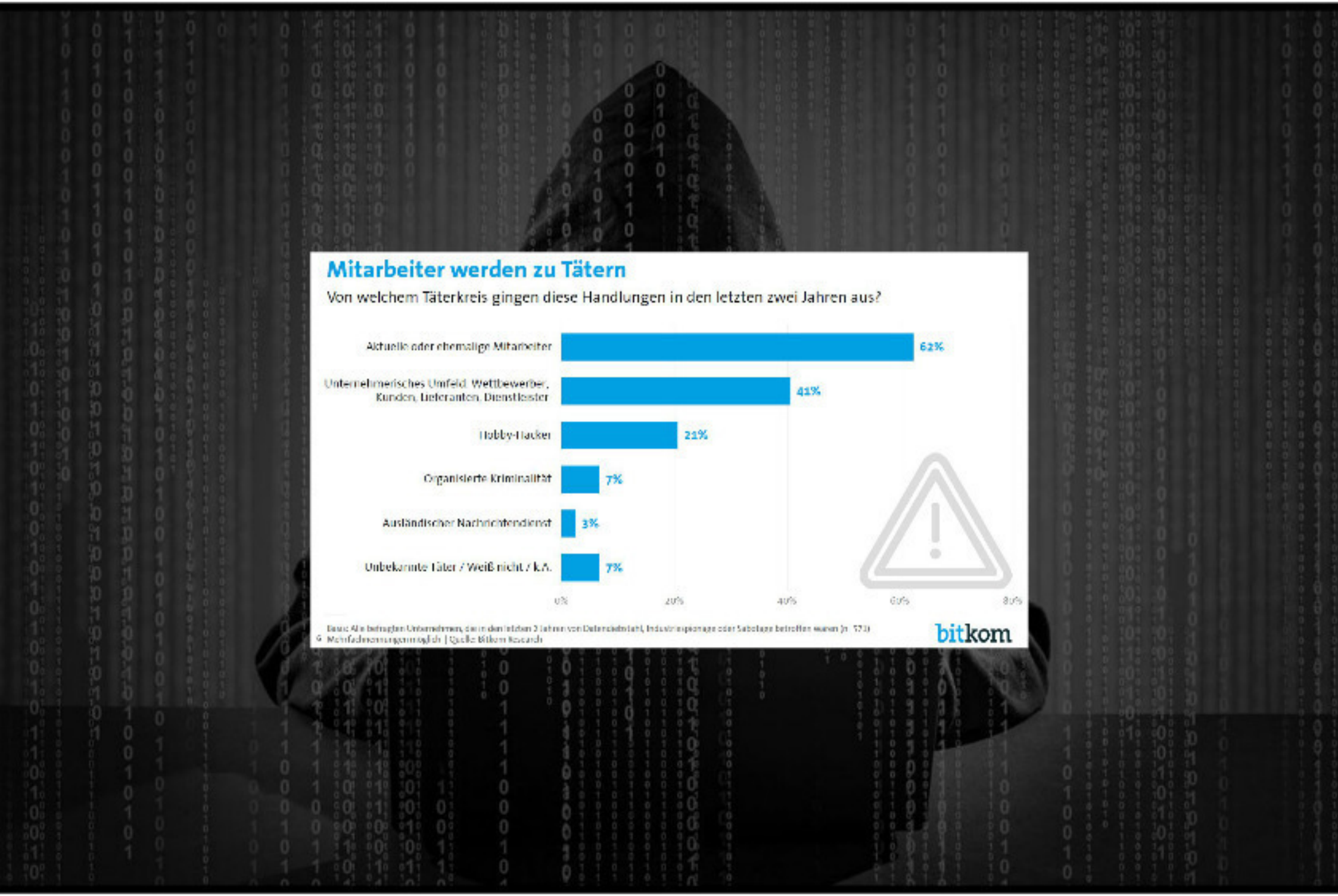
2.000.000.000.000 US-Dollar

Basis: Alle befragten Unternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=571) | Quelle: Bitkom Research

bitkom


INDUSTRIE 4.0
MOBILITÄT
LOGISTIK
INTELLIGENTE FABRIK
STROMNETZE
GEBÄUDE
PRODUKTE


"Security by Design"
Web Proxy Auto Discovery Protocol (WPAD) 1996
1 Hostname change from "tom knopf" to"WPAD"
2 in the Web server
4 System is configured to listen to port 1080
5 Network is instructed to
6 Attacker can now intercept ALL web traffic
Attacker's system


Mitarbeiter werden zu Tätern
Von welchem Täterkreis gingen diese Handlungen in den letzten zwei Jahren aus?
Aktuelle oder ehemalige Mitarbeiter
62%
Unternehmerisches Umfeld: Wettbewerber, Kunden, Lieferanten, Dienstleister
41%
Hobby-Hacker
21%
Organisierte Kriminalität
7%
Ausländischer Nachrichtendienst
3%
Unbekannte Täter / Weiß nicht / k.A.
7%
0%
20%
40%
60%
80%
bitkom


Plan B
Plan A

Anzeige?

Ja!

Nutzen wird als gering erachtet!

Befürchtungen bezüglich Sicherstellung & möglicher Zufallsfunde!

Angst vor Reputationsschaden!

Vorteile!

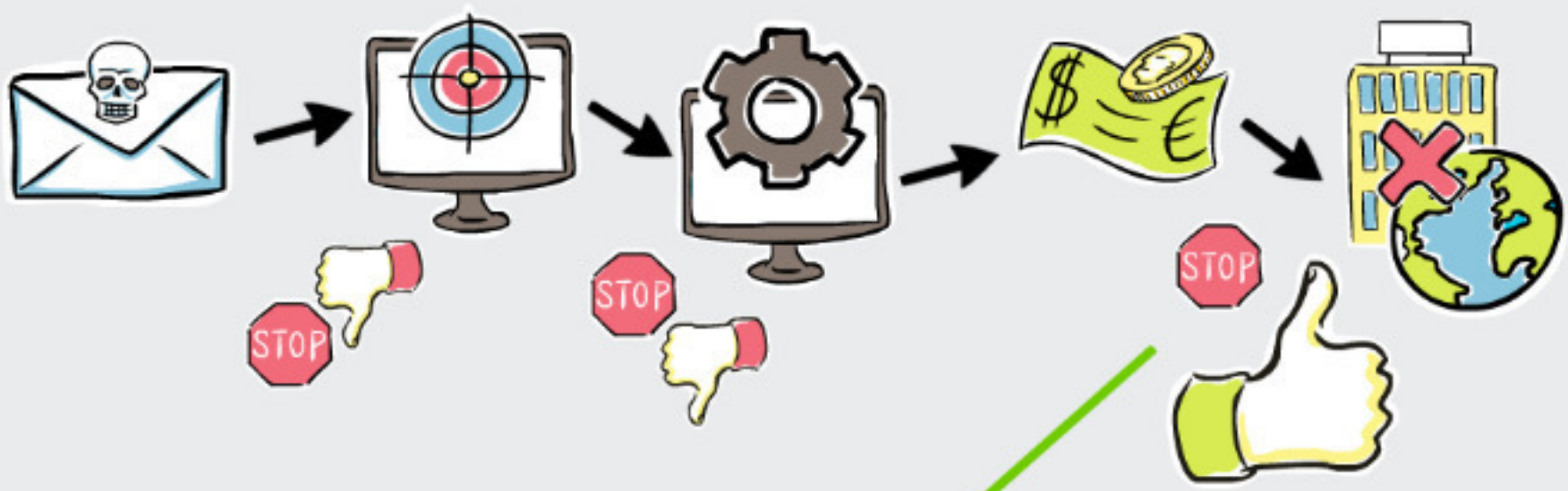
Zugriff auf Erfahrungswissen aus polizeilicher Lage & Praxis!

Unterstützung und Handlungsempfehlungen!

Kriminalpolizeiliche Bewertung!

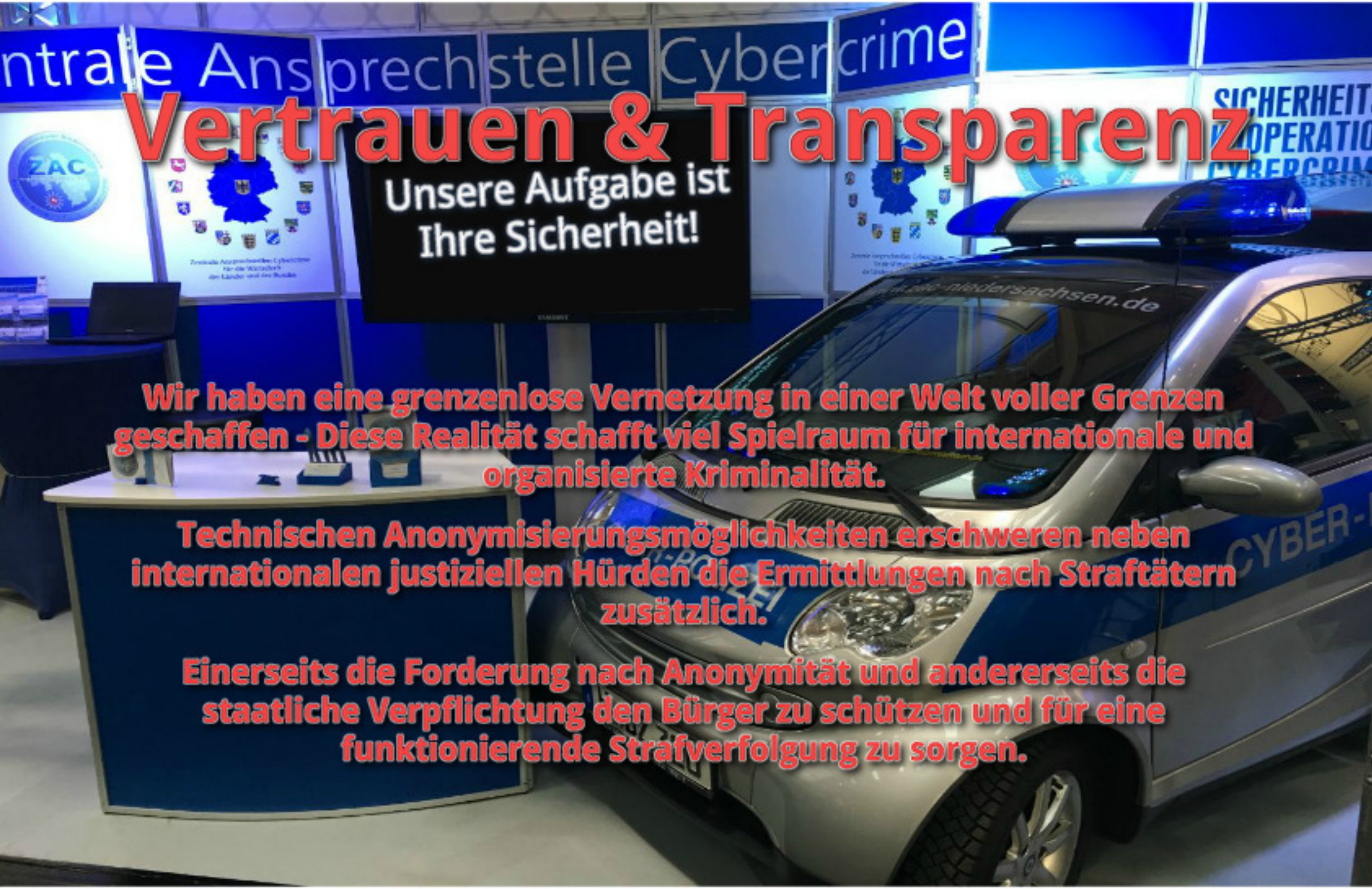
Banken und Polizei an einem Tisch

Jährlicher Banken-Workshop zum Thema "Phishing im Online-Banking"



Fallzahlen aus Niedersachsen:

2013	2014	2015	2016
1010	1620	617	ca. 300 (aktuell)



Vertrauen & Transparenz

Wir haben eine grenzenlose Vernetzung in einer Welt voller Grenzen geschaffen - Diese Realität schafft viel Spielraum für internationale und organisierte Kriminalität.

Technischen Anonymisierungsmöglichkeiten erschweren neben internationalen justiziellen Hürden die Ermittlungen nach Straftätern zusätzlich.

Einerseits die Forderung nach Anonymität und andererseits die staatliche Verpflichtung den Bürger zu schützen und für eine funktionierende Strafverfolgung zu sorgen.

Zentrale Ansprechstellen Cybercrime für die Wirtschaft der Länder und des Bundes