Bundesamt
für Sicherheit in der
Informationstechnik

# Aktuelles zur Cyber-Sicherheitslage

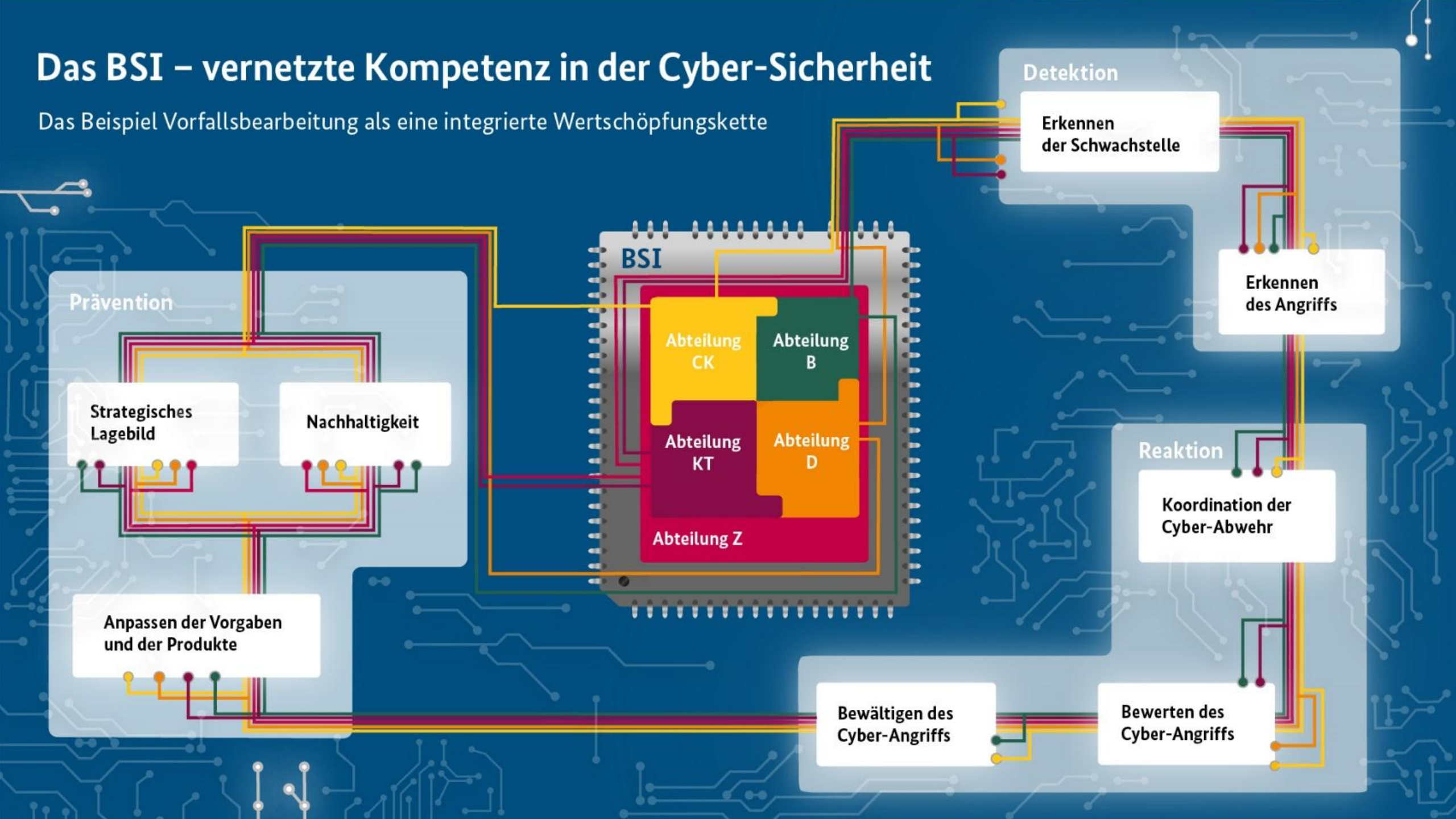
Brandenburg, den 18. Januar 2018

# Das BSI als die nationale Cyber-Sicherheitsbehörde gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft

Bundesamt
für Sicherheit in der
Informationstechnik

# Das BSI – vernetzte Kompetenz in der Cyber-Sicherheit

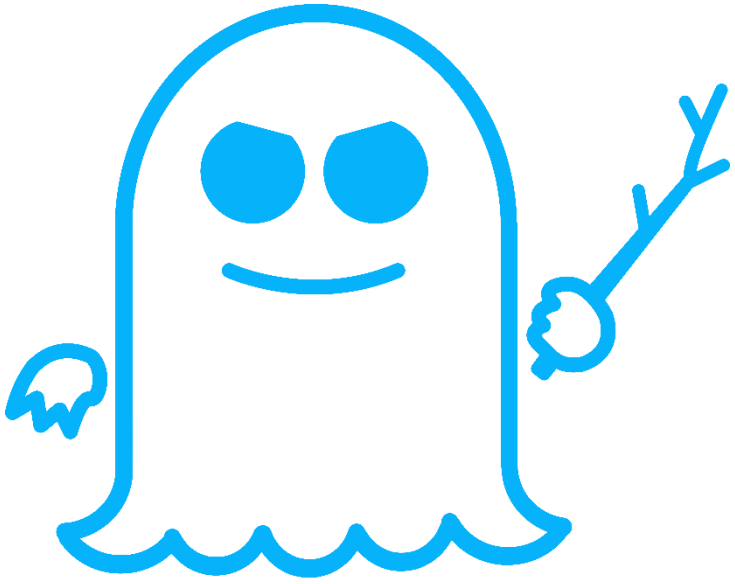
Das Beispiel Vorfallsbearbeitung als eine integrierte Wertschöpfungskette



# Schlagzeilen

Abbildungen: Natascha Eibl, CC0

MELTDOWN



SPECTRE

# BSI-Publikationen zur Lage

# BSI-Publikationen zur Lage

# Aus dem jährlichen Lagebericht

# CEO-Betrug

## CEO-Betrug

**Sachverhalt**

Dem BSI wurden zahlreiche Fälle von CEO-Betrug gemeldet. Zu den Betroffenen zählen auch Unternehmen der Kritischen Infrastrukturen und Behörden. So wurde eine Mitarbeiterin einer deutschen Landesbehörde per Mail „persönlich beauftragt“, eine „vertrauliche Finanztransaktion“ in Höhe von 961.000 Euro durchzuführen. Der Mail-Verkehr, der vorgeblich vom Präsidenten des Amtes stammte, wurde durch einen Anruf einer angeblichen Anwältin begleitet, die der Aufforderung Nachdruck verleihen sollte. Der höchste dem BSI bekannte Schaden in einem Einzelfall belief sich auf einen Verlust von 40 Millionen Euro bei einem Automobilzulieferer. Eine europäische Bank hat allein im ersten Halbjahr 2016 von ihren Kunden 50 Fälle von CEO-Betrug gemeldet bekommen. Insgesamt versuchten die Angreifer dabei, über 20 Millionen Euro zu erbeuten. In 20 dieser Fälle wurde der Angriff bereits im Unternehmen verhindert. Bei 20 weiteren Fällen wurden die Zahlungen durch die Bank aufgehalten oder konnten zurückgeholt werden. In den restlichen zehn bekannten Fällen entstand ein Schaden von insgesamt fünf Millionen Euro. Die Dunkelziffer ist deutlich höher.

# Schadprogramme

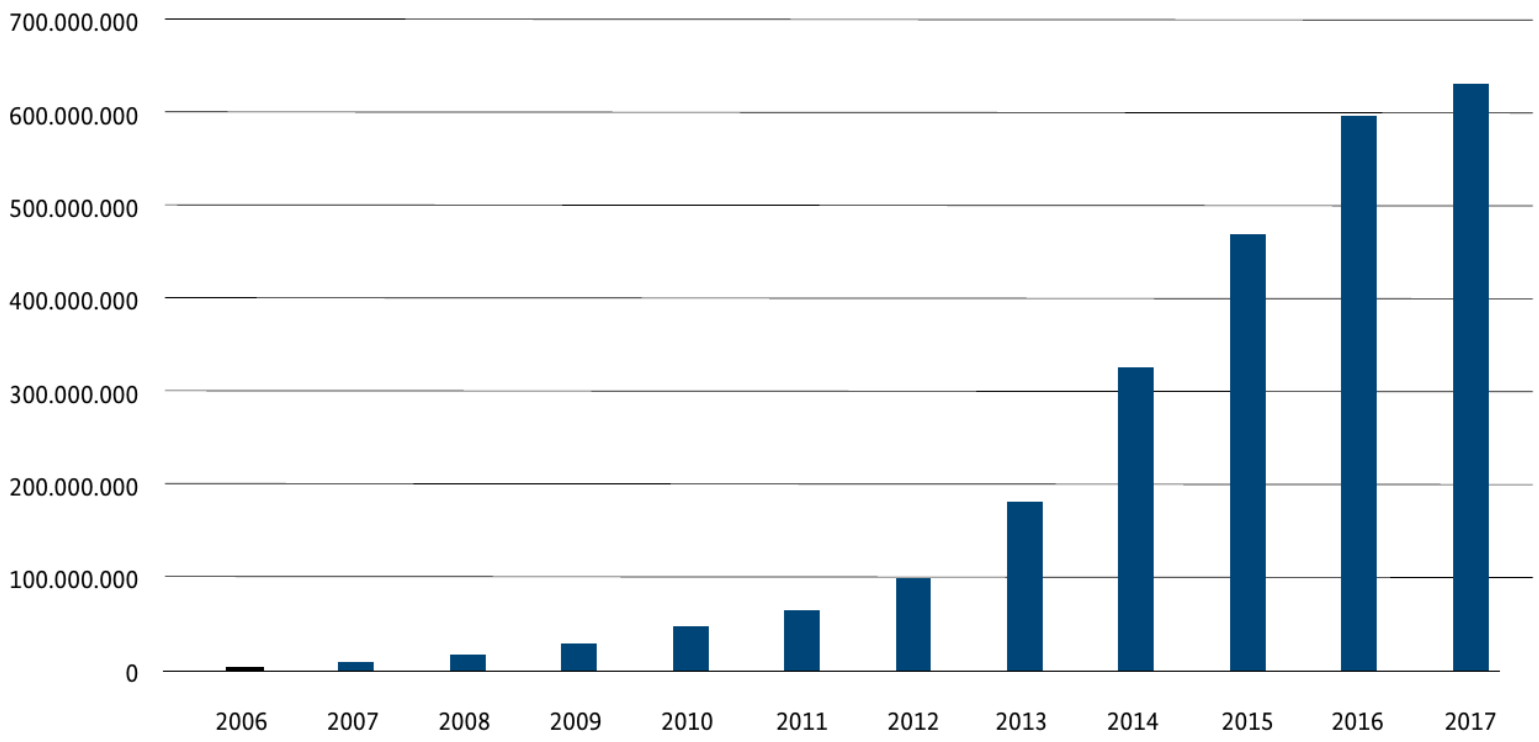



**Abbildung 7** Bekannte Schadprogramme (2017 bis Mai), Quelle: AV-TEST

# WannaCry

## WannaCry

**Sachverhalt**

Mit der Ransomware WannaCry wurde Anfang Mai 2017 eine große Sorge der IT-Sicherheitsgemeinschaft wahr. Ein Schadprogramm, das Dateien verschlüsselt und damit den Betrieb von Systemen und Dienstleistungen bis zur Zahlung einer Erpressungssumme unmöglich macht, kombiniert mit einem Schwachstellen-Scanner, der selbstständig ohne Nutzerinteraktion die Schadsoftware auf andere verwundbare Systeme im internen Netz weiterverbreitet, wurde aktiv. Es war eine „kleine Version“ eines Krypto-Wurms.

# Meldungen aus der Bundesverwaltung

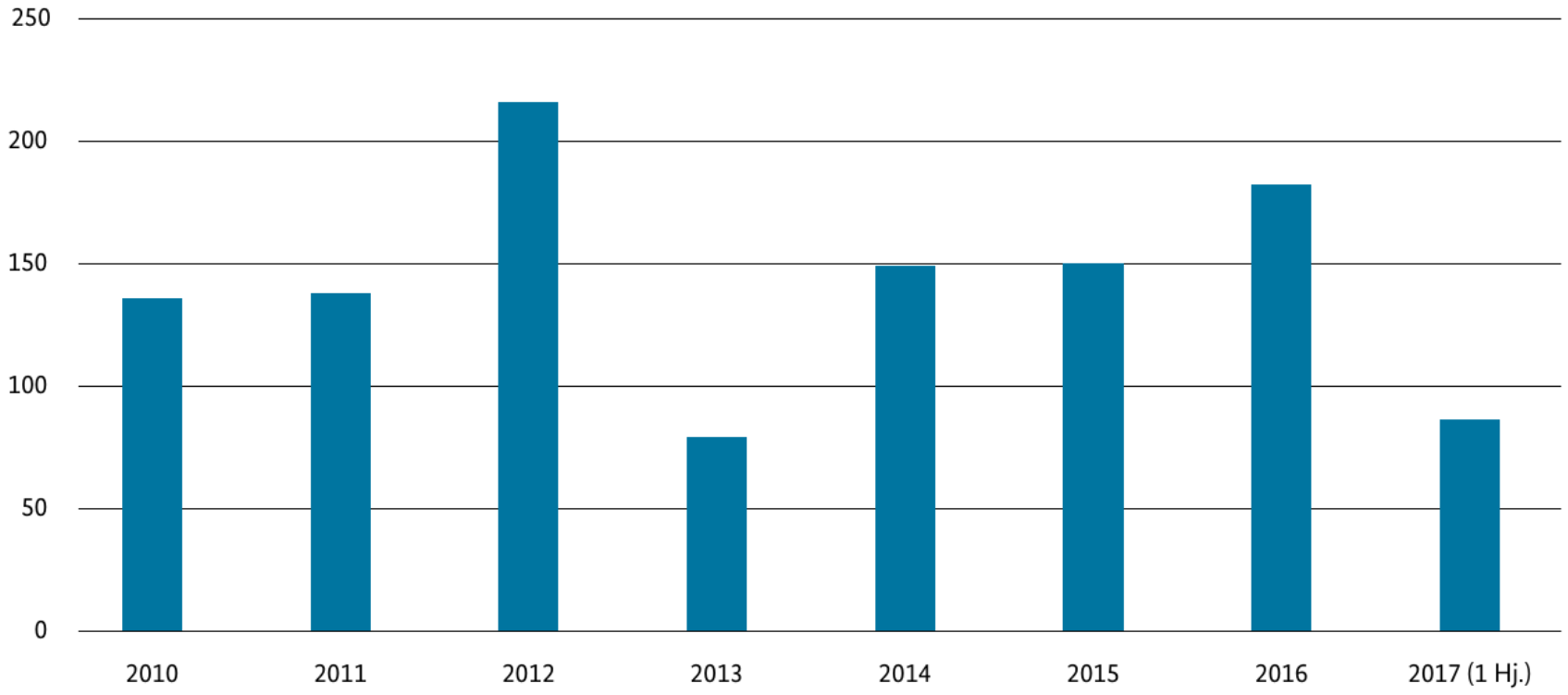



**Abbildung 3** Anzahl der SOFORT-Meldungen nach § 4 Abs. 3 BSIG

Bundesamt
für Sicherheit in der
Informationstechnik

# Spearphishing gegen Spitzenpersonal

## Spearphishing gegen Spitzenpersonal

**Sachverhalt**

Das BSI hat im Juni 2017 professionelle Cyber-Angriffe auf private E-Mail-Postfächer von Funktionsträgern aus Wirtschaft und Verwaltung beobachtet. Bei dieser Angriffskampagne werden täuschend echt erscheinende Spearphishing-Mails an ausgewählte Führungspersonen gesandt. Die Angreifer geben vor, Auffälligkeiten bei der Nutzung des Postfachs beobachtet zu haben oder neue Sicherheitsfunktionalitäten anbieten zu wollen. Der Nutzer wird aufgefordert, einen Link anzuklicken und auf der sich öffnenden Webseite sein Passwort anzugeben. Die Kampagne richtete sich gegen Yahoo- und Gmail-Konten. Bereits 2016 konnte das BSI beobachten, dass Webseiten registriert wurden, die sich für Spearphishing-Angriffe gegen Kunden der deutschen Webmail-Dienstleister gmx.de und web.de eignen und deren Infrastruktur der aktuellen Kampagne ähnelt. Zwar waren diese Domains nicht Ziel der Angriffe im Juni 2017, es zeigt aber, dass die Täter diese Mailprovider auch als möglichen Angriffsweg identifiziert haben.

# Cyber-Spionage-Gruppen

| | |
|---|---|
| **Regierungs-einrichtungen** | APT6/1.php, APT12/NumberedP., APT28/Sofacy, APT29/CozyBear, APT32/OceanLotus, Cadelle/Chafer, Callisto/DancingSal., CharmingKitten, Danti, DarkHotel, Dropping-Elephant, EmissaryPanda, Gamaredon, GazaCybergang, GothicPanda, Greenbug, Groundbait, HammerPanda, Infy, KeyBoy, Longhorn, LotusPanda, Machete, Mofang, Naikon/OverrideP., NanHaiShu, OilRig, Operation-Cleaver, Remsec/ProjectSauron, ScarletMimic, Shamoon, Snake, Suckfly, TidePool/Ke3chang, Transparent-Tribe, TropicTrooper/PirateP., ViceroyTiger |
| **Militär/ Rüstung** | APT28/Sofacy, AridViper, Callisto/DancingSal., CharmingKitten, C-Major/PureStrike, Dropping-Elephant, Gamaredon, GazaCybergang, GothicPanda, HammerPanda, LotusPanda, Machete, Mofang, Naikon/OverrideP., OilRig, Operation-Cleaver, Remsec/ProjectSauron, Snake |
| **Energie** | APT10, APT18/Wekby, APT29/CozyBear, CharmingKitten, ElectricPowder, EmissaryPanda, Greenbug, Kraken/Laziok, Longhorn, Machete, OnionDog, OperationCleaver, Sandworm, Shamoon, TropicTrooper/PirateP. |
| **Opposition** | Ahtapot, APT32/OceanLotus, Bookworm, FlyingDragon, Groundbait, Group5, Infy, Neodymium, Operation-Cleaver, Operation Manul, Promethium, ScarletMimic, Sima, StealthFalcon |
| **Medien** | APT28/Sofacy, APT32/OceanLotus, BugDrop, Callisto/DancingSal., DarkHotel, GazaCybergang, Groundbait, Infy, Operation Manul, Sandworm, ShroudedCrossbow, StealthFalcon, Tick |
| **Finanzen** | APT18/Wekby, APT29/CozyBear, EmissaryPanda, EquationGroup, GazaCybergang, HammerPanda, Longhorn, OilRig, Sandworm, Suckfly |
| **Telko** | APT18/Wekby, Codoso, EmissaryPanda, HammerPanda, Longhorn, Machete, OilRig, Remsec/ProjectSauron |
| **NGO** | APT29/CozyBear, Callisto/DancingSal., CharmingKitten, HammerPanda, Infy, NilePhish, Operation-Cleaver, RocketKitten |
| **Universitäten** | APT10/menuPass, BugDrop, Codoso, Greenbug, DarkHotel, Longhorn, RocketKitten |
| **High-Tech** | APT18/Wekby, CharmingKitten, Codoso, LEAD/Winnti, Tick |
| **Transport/ Logistik** | Cadelle/Chafer, OilRig, OnionDog, Remsec/ProjectSauron, Shamoon |
| **Luft- und Raumfahrt** | APT28, EmissaryPanda, HammerPanda, Greenbug, Longhorn |
| **Gesundheit** | APT10/menuPass, LEAD/Winnti, Suckfly |
| **Kanzleien** | APT29/CozyBear, Codoso, DeepPanda, NanHaiShu |

**Abbildung 5** Auflistung der in verschiedenen Branchen im Berichtszeitraum weltweit aktiven Cyber-Spionage-Gruppen,

# Veraltete Cloud-Software

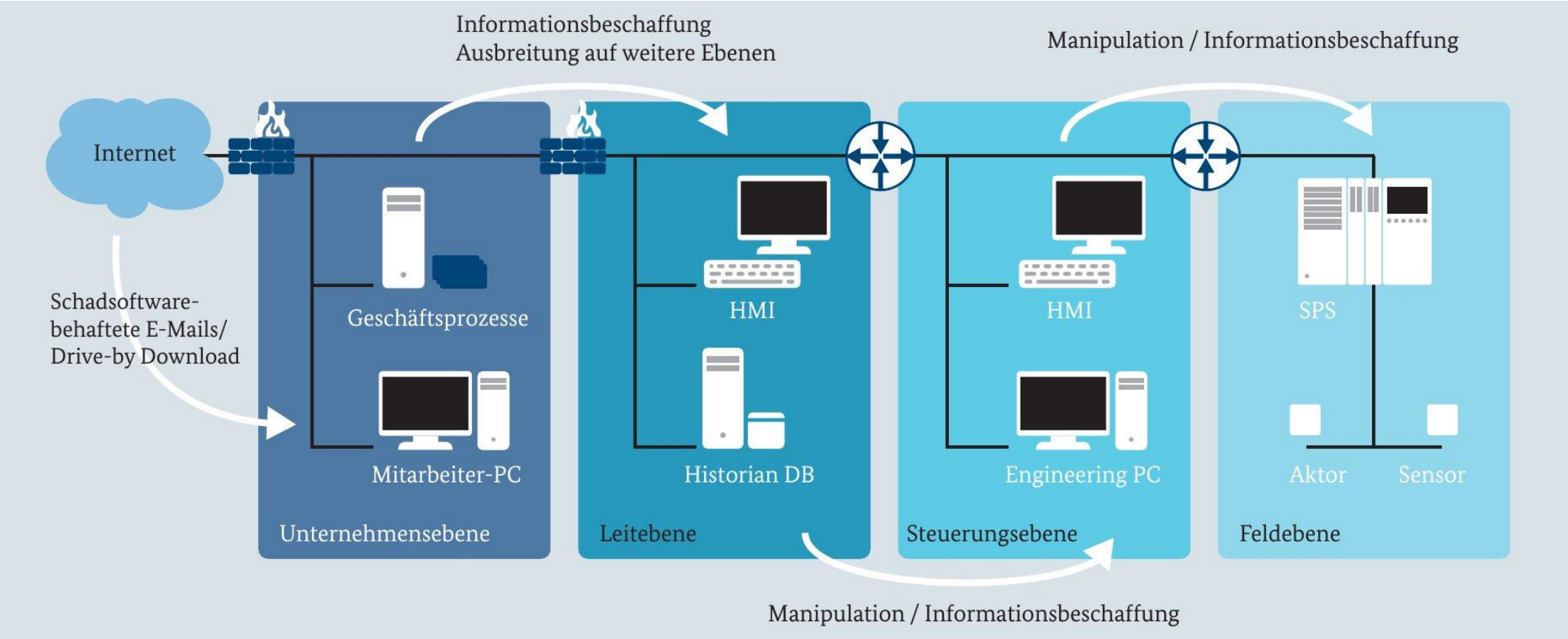
## Veraltete Cloud-Software

**Sachverhalt**

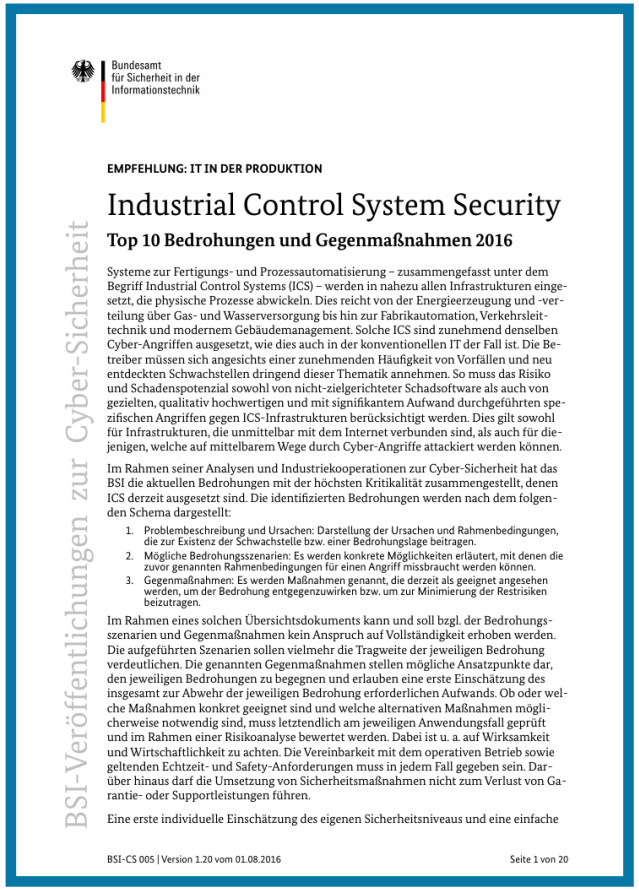
Im Februar 2017 wurde dem BSI bekannt, dass mehrere Zehntausend der in Deutschland betriebenen Private-Cloud-Systeme auf Basis der weit verbreiteten Software ownCloud und Nextcloud mit veralteten Versionen laufen, die nicht mehr von den Herstellern unterstützt werden und teils kritische Sicherheitslücken aufweisen. Unter den Betreibern dieser verwundbaren Cloud-Systeme befanden sich neben Privatnutzern unter anderem viele große und mittelständische Unternehmen, öffentliche und kommunale Einrichtungen, Energieversorger, Krankenhäuser, Ärzte und Rechtsanwälte.

# Industrial Control Systems (ICS)

# Industrial Control Systems (ICS)



# ICS – Top 10 Bedrohungen und Maßnahmen



Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Veröffentlichungen zur Cyber-Sicherheit

EMPFEHLUNG: IT IN DER PRODUKTION

Industrial Control System Security

**Top 10 Bedrohungen und Gegenmaßnahmen 2016**

Systeme zur Fertigungs- und Prozessautomatisierung – zusammengefasst unter dem Begriff Industrial Control Systems (ICS) – werden in nahezu allen Infrastrukturen eingesetzt, die physische Prozesse abwickeln. Dies reicht von der Energieerzeugung und -verteilung über Gas- und Wasserversorgung bis hin zur Fabrikautomation, Verkehrsleittechnik und modernem Gebäudemanagement. Solche ICS sind zunehmend denselben Cyber-Angriffen ausgesetzt, wie dies auch in der konventionellen IT der Fall ist. Die Betreiber müssen sich angesichts einer zunehmenden Häufigkeit von Vorfällen und neu entdeckten Schwachstellen dringend dieser Thematik annehmen. So muss das Risiko und Schadenspotenzial sowohl von nicht-zielgerichteter Schadsoftware als auch von gezielten, qualitativ hochwertigen und mit signifikantem Aufwand durchgeführten spezifischen Angriffen gegen ICS-Infrastrukturen berücksichtigt werden. Dies gilt sowohl für Infrastrukturen, die unmittelbar mit dem Internet verbunden sind, als auch für diejenigen, welche auf mittelbarem Wege durch Cyber-Angriffe attackiert werden können.

Im Rahmen seiner Analysen und Industriekooperationen zur Cyber-Sicherheit hat das BSI die aktuellen Bedrohungen mit der höchsten Kritikalität zusammengestellt, denen ICS derzeit ausgesetzt sind. Die identifizierten Bedrohungen werden nach dem folgenden Schema dargestellt:

1. Problembeschreibung und Ursachen: Darstellung der Ursachen und Rahmenbedingungen, die zur Existenz der Schwachstelle bzw. einer Bedrohungslage beitragen.
2. Mögliche Bedrohungsszenarien: Es werden konkrete Möglichkeiten erläutert, mit denen die zuvor genannten Rahmenbedingungen für einen Angriff missbraucht werden können.
3. Gegenmaßnahmen: Es werden Maßnahmen genannt, die derzeit als geeignet angesehen werden, um der Bedrohung entgegenzuwirken bzw. um zur Minimierung der Restrisiken beizutragen.

Im Rahmen eines solchen Übersichtsdokuments kann und soll bzgl. der Bedrohungsszenarien und Gegenmaßnahmen kein Anspruch auf Vollständigkeit erhoben werden. Die aufgeführten Szenarien sollen vielmehr die Tragweite der jeweiligen Bedrohung verdeutlichen. Die genannten Gegenmaßnahmen stellen mögliche Ansatzpunkte dar, den jeweiligen Bedrohungen zu begegnen und erlauben eine erste Einschätzung des insgesamt zur Abwehr der jeweiligen Bedrohung erforderlichen Aufwands. Ob oder welche Maßnahmen konkret geeignet sind und welche alternativen Maßnahmen möglicherweise notwendig sind, muss letztendlich am jeweiligen Anwendungsfall geprüft und im Rahmen einer Risikoanalyse bewertet werden. Dabei ist u. a. auf Wirksamkeit und Wirtschaftlichkeit zu achten. Die Vereinbarkeit mit dem operativen Betrieb sowie geltenden Echtzeit- und Safety-Anforderungen muss in jedem Fall gegeben sein. Darüber hinaus darf die Umsetzung von Sicherheitsmaßnahmen nicht zum Verlust von Garantie- oder Supportleistungen führen.

Eine erste individuelle Einschätzung des eigenen Sicherheitsniveaus und eine einfache

BSI-CS 005 | Version 1.20 vom 01.08.2016 Seite 1 von 20

1. Bewertung der einzelnen Bedrohungen
   - Verbreitung
   - Exposition
   - Ausnutzbarkeit
   - Detektion
2. Problembeschreibung und Ursachen
3. Mögliche Bedrohungsszenarien
4. Gegenmaßnahmen

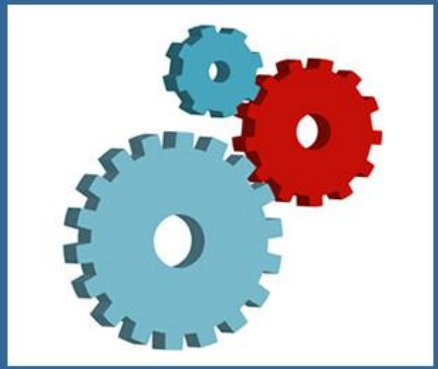
| Nr. (Nr. alt) | Top 10 2016 | Top 10 2014 |
|---|---|---|
| 1 (3) | Social Engineering und Phishing† | Infektion mit Schadsoftware über Internet und Intranet |
| 2 (2) | Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware | Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware |
| 3 (1) | Infektion mit Schadsoftware über Internet und Intranet | Social Engineering |
| 4 (5) | Einbruch über Fernwartungszugänge | Menschliches Fehlverhalten und Sabotage |
| 5 (4) | Menschliches Fehlverhalten und Sabotage | Einbruch über Fernwartungszugänge |
| 6 (6) | Internet-verbundene Steuerungskomponenten | Internet-verbundene Steuerungskomponenten |
| 7 (7) | Technisches Fehlverhalten und höhere Gewalt | Technisches Fehlverhalten und höhere Gewalt |
| 8 (9) | Kompromittierung von Extranet und Cloud-Komponenten | Kompromittierung von Smartphones im Produktionsumfeld |
| 9 (10) | (D)DoS Angriffe | Kompromittierung von Extranet und Cloud-Komponenten |
| 10 (8) | Kompromittierung von Smartphones im Produktionsumfeld | (D)DoS Angriffe |

Legende: †NEU

# Der neue IT-Grundschutz

# IT-Grundschutz

IT-Grundschutz - die Basis für Informationssicherheit - Der vom BSI entwickelte IT-Grundschutz ermöglicht es, notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Viele Arbeitsprozesse werden elektronisch gesteuert und große Mengen von Informationen sind digital gespeichert, werden verarbeitet und in Netzen übermittelt. Damit sind die Institutionen in Wirtschaft und Verwaltung und jeder Bürger von dem einwandfreien Funktionieren der eingesetzten IT abhängig.



## Aktuelles und Veranstaltungen

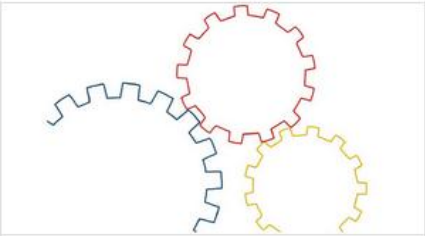
Aktuelles und Veranstaltungen rund um den IT-Grundschutz

## Über den IT-Grundschutz

Allgemeine Informationen über den IT-Grundschutz des BSI.

## IT-Grundschutz-Drafts

Entwürfe zukünftiger IT-Grundschutz-Bausteine und -Umsetzungshinweise



## IT-Grundschutz-Standards

Die BSI-Standards enthalten Empfehlungen zu Methoden, Prozessen, Vorgehensweisen und Maßnahmen zur Informationssicherheit.

## IT-Grundschutz-Kompendium

Das IT-Grundschutz-Kompendium ist die modernisierte Fassung der IT-Grundschutz-Kataloge.

## IT-Grundschutz-Profile

Schablonen, mit denen verschiedene Anwender(-gruppen) selbstständig den IT-Grundschutz auf ihre Bedürfnisse anpassen können.

# Vielen Dank für Ihre Aufmerksamkeit!

## Kontakt

Dr. Harald Niggemann
Cyber Security Strategist

Telefon: 0228 99 9582 5368
E-Mail: harald.niggemann@bsi.bund.de
Web: www.bsi.bund.de

Godesberger Allee 185 - 189
53175 Bonn

Bundesamt
für Sicherheit in der
Informationstechnik