David Deutschmann

4. Kommunaler IT-Sicherheitskongress 2017

„Umsetzung der Leitlinie für Informationssicherheit des IT-Planungsrats in Kommunalverwaltungen“

LAND BRANDENBURG

Brandenburgischer IT-Dienstleister

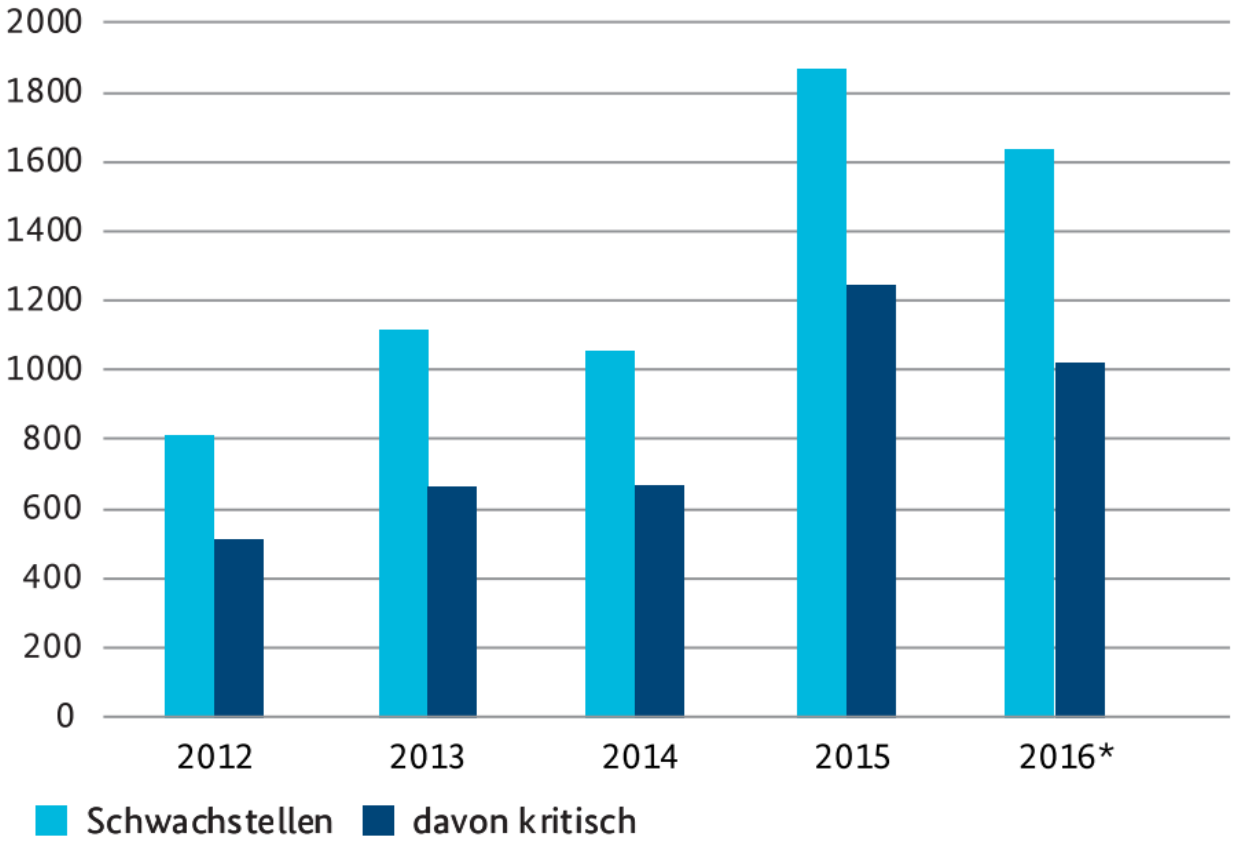
Das CERT-Brandenburg und die Kommunen

4. Kommunaler IT-Sicherheitskongress

Berlin, 08 + 09.05.2017

Brandenburgischer IT-Dienstleister (ZIT-BB)
14480 Potsdam, Steinstraße 104-106
David Deutschmann, CERT-Brandenburg

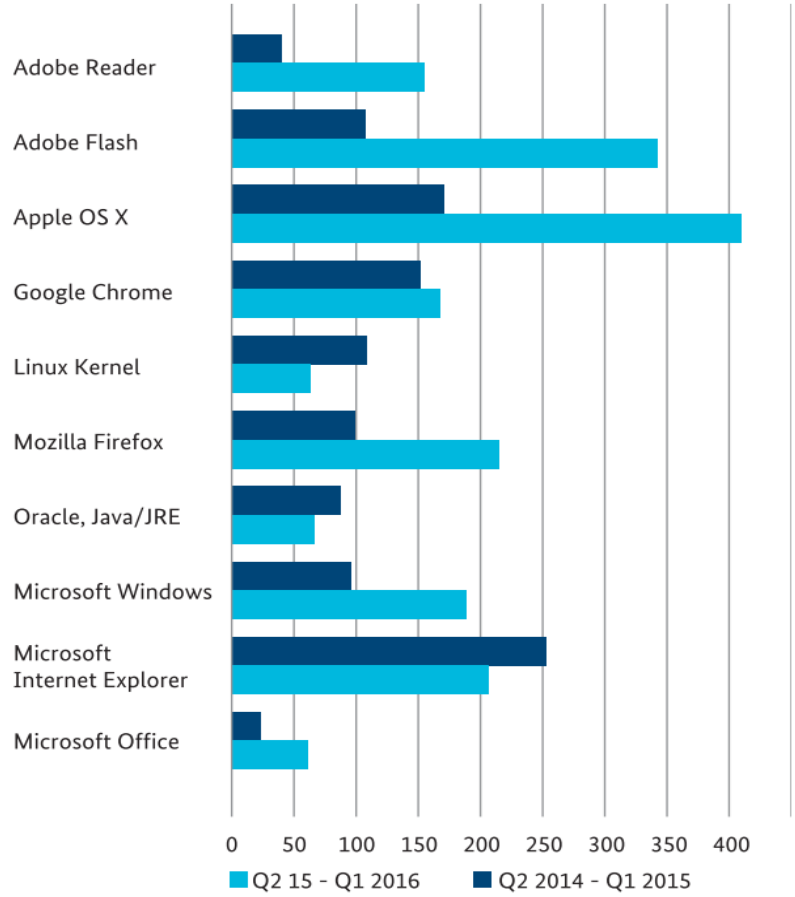
Schwachstellen in Softwareprodukten



Entwicklung Schwachstellen in Softwareprodukten (Quelle: BSI Lagebericht 2016)

- **Softwareprodukte werden immer komplexer**
- **Komplexität kann potentielle Sicherheitsvorfälle nach sich ziehen**

Schwachstellen in ausgewählten Softwareprodukten



Entwicklung Schwachstellen in Softwareprodukten (Quelle: BSI Lagebericht 2016)

- **Statistik zeigt Millionenfach genutzte Software und deren Schwachstellen**
- **besonders im Fokus Adobe Flash**

LAND BRANDENBURG

Brandenburgischer IT-Dienstleister

Schwachstellen in Hardwareprodukten

SPIEGEL ONLINE

Attacke auf Router

Telekom-Hack hätte viel schlimmer kommen können

Sicherheitslücke durch offene USB-Ports für Netzstruktur

taz.de

Hacker-Angriff am Wochenende

Twitter, Paypal, Spotify lahmgelegt

Cyber-Angriff

Sicherheitslücke bei Netgear: Router für Angriffe anfällig

Deutsche Wirtschafts Nachrichten

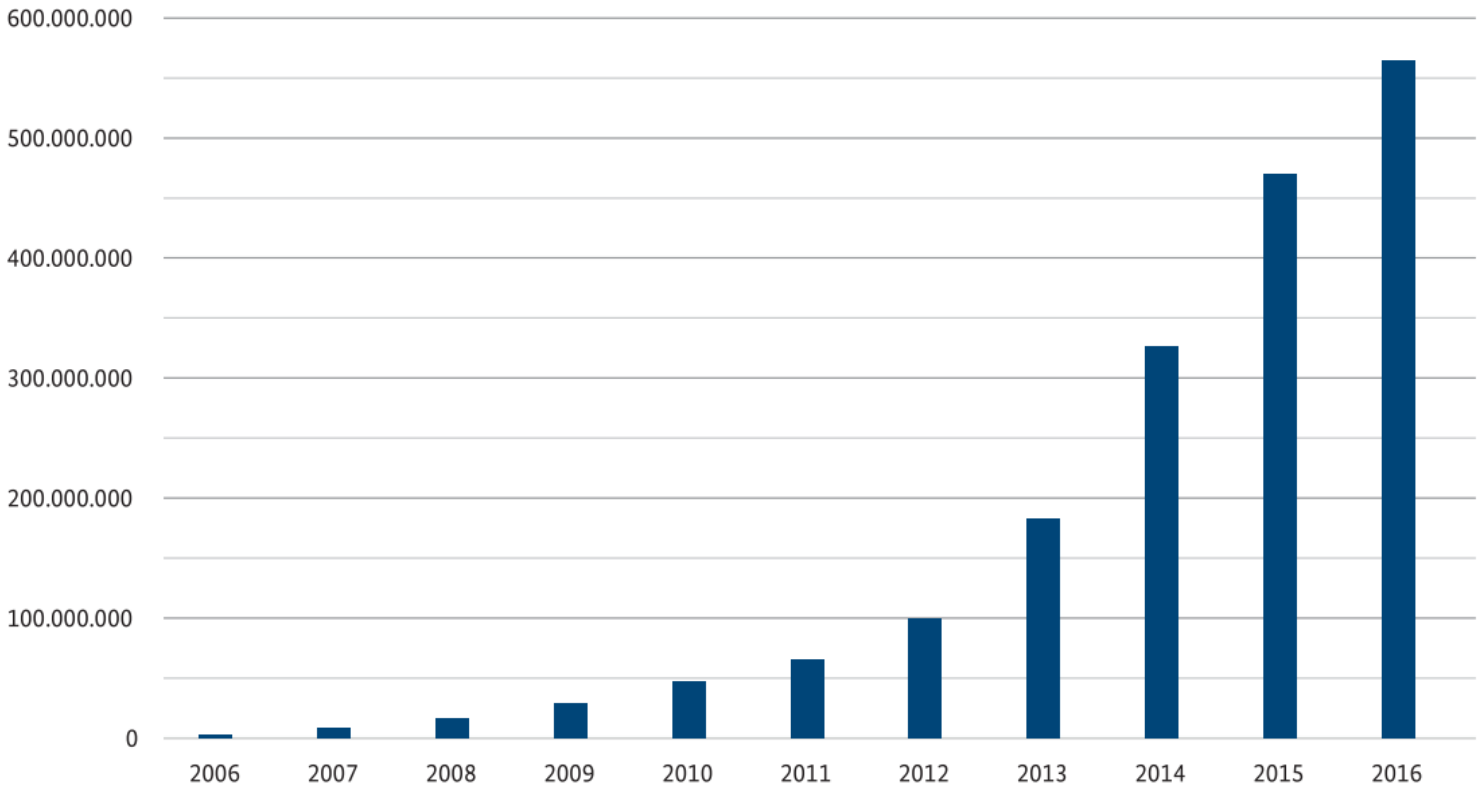
Veröffentlicht: 14.12.16, 09:33 Uhr

In einigen Router-Modellen der Firma Netgear wurde eine kritische Sicherheitslücke entdeckt. Das BSI vergibt Risikostufe 5.

Varianten von Angriffen auf die IT-Infrastruktur

- Schadsoftware
- Verschlüsselungstrojaner
- Spam
- Social Engineering
- Advanced Persistent Threats
- Botnetze
- DDoS
- Drive-by-Exploits und Exploit Kits
- Identitätsdiebstahl
- Seitenkanalangriffe u. w.

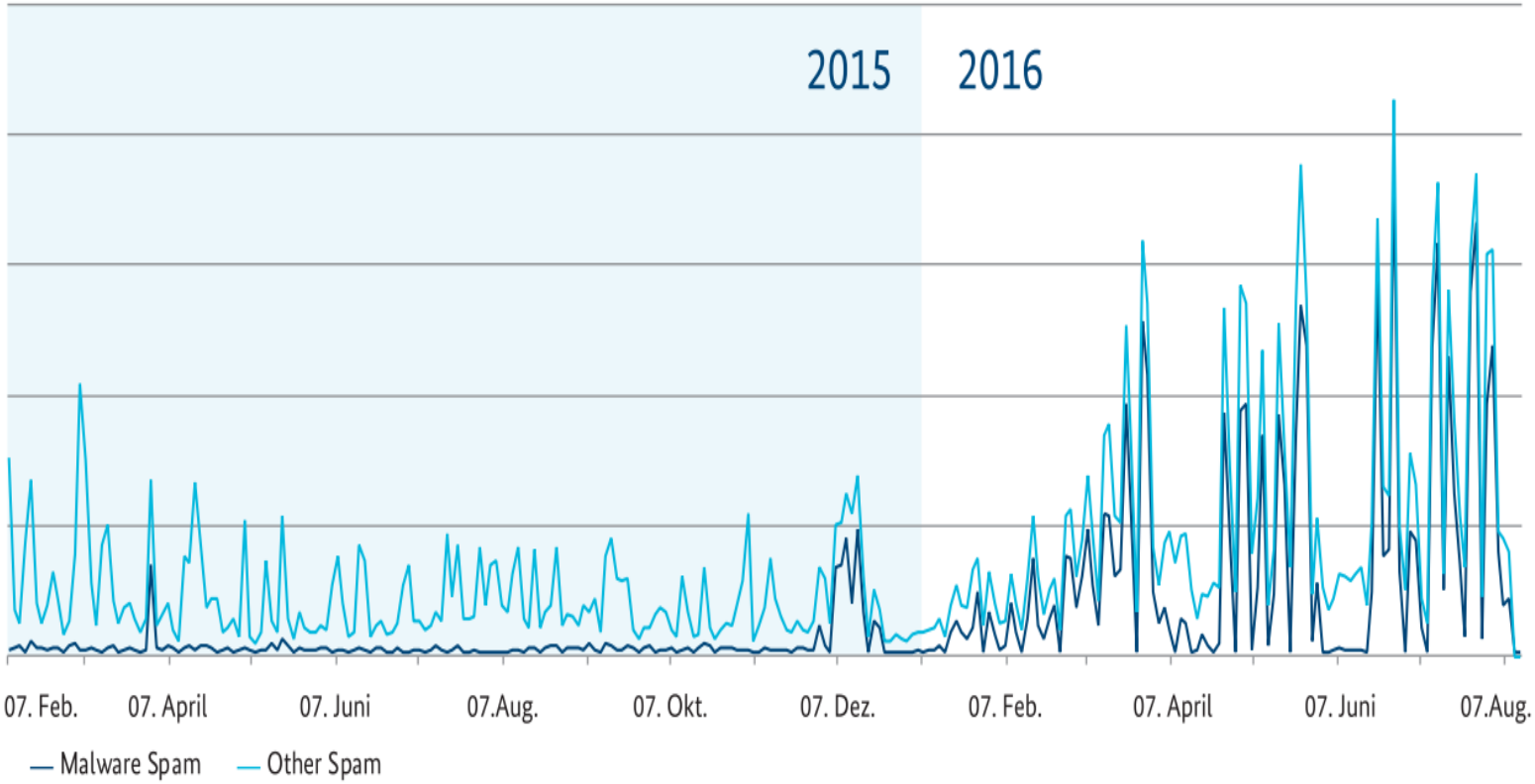
Entwicklung bekannter Schadprogramme



Bekannte Schadprogramme (Quelle: BSI Lagebericht 2016)

- **täglich bis zu 380.000 neue Schad-programme**
- **häufigste Infektionswege:**
  - **E-Mail Anhänge**
  - **unbemerkte Infektion auf Webseiten**
  - **Werbebanner**

Angriffe durch Spam

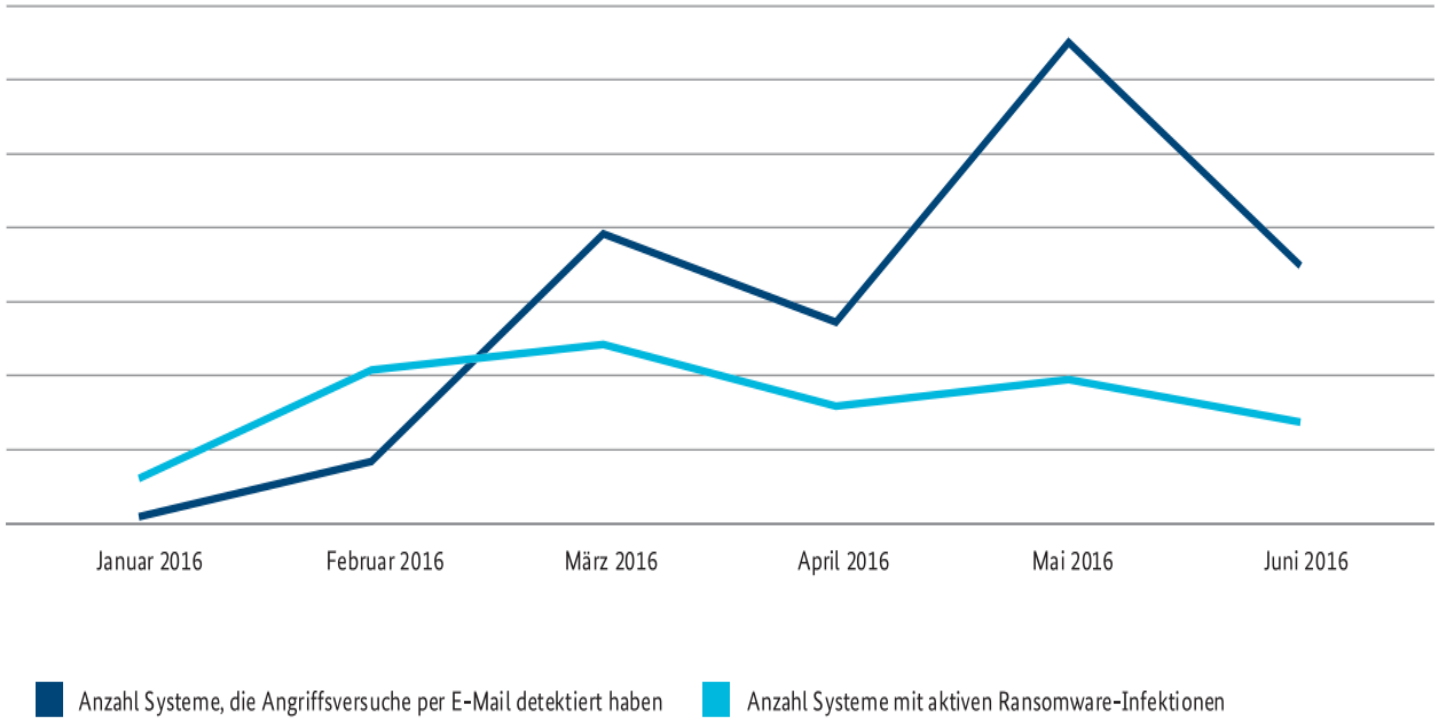


Spam-Verlauf pro Woche in Deutschland (Quelle: BSI Lagebericht 2016)

- **infiziertes Dokument lädt Schadcode aus dem Internet nach oder „liefert dies teilweise sogar schon mit“**
- **2016 mehr Schadcode-Spam als „normale“ Spam**

Angriffe durch Ransomware

(Erpressungstrojaner, Kryptotrojaner, Verschlüsselungstrojaner)



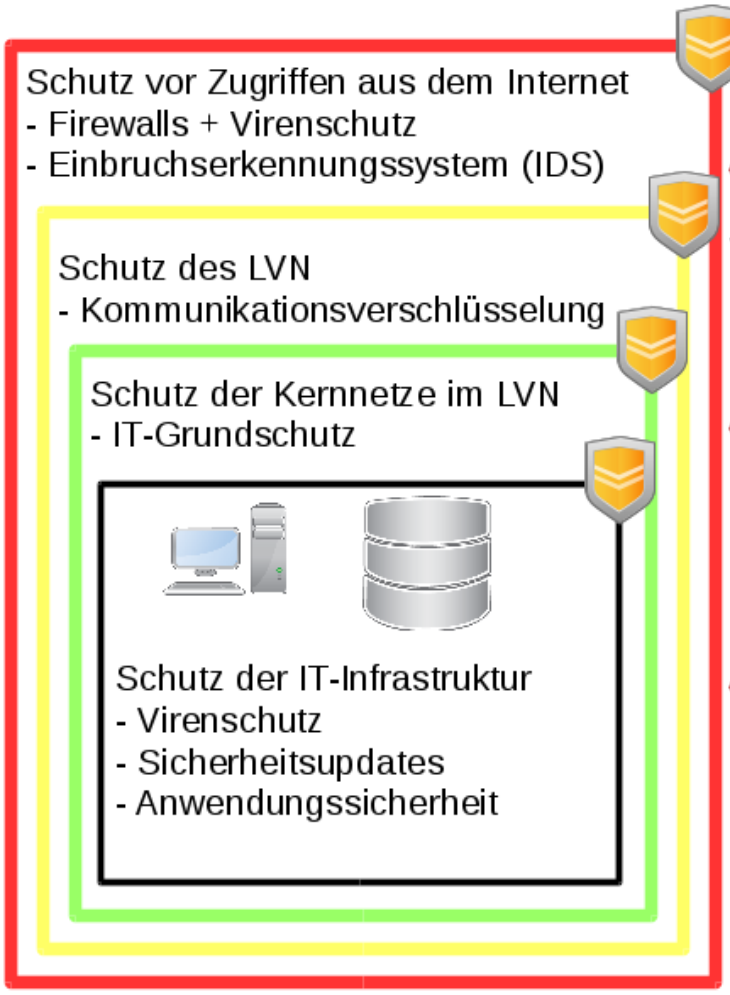
Ransomware Detektionen und Infektionen in Deutschland (Quelle: BSI Lagebericht 2016)

- **infizieren Computer, sperren diesen und erpressen Geld für Entsperrung**
- **Anwendung stark steigend**

LAND BRANDENBURG

Brandenburgischer IT-Dienstleister

IT-Infrastruktur der Landesverwaltung Brandenburg
Bedrohungen und Schutz



Viren
> 500 / Monat (Peak >2000)

Einbruchserkennungssystem (IDS)
~ 200 aggregierte Events / Woche

Mailsystem
~ 50.000 (Spam, RBL, Viren) / Monat

Märkische Allgemeine

BKA warnt vor Internetkriminalität

Mehr als 40 Millionen Euro Schaden durch Banden im Netz – im Darknet floriert der Schwarzmarkt

DIE WELT

ERPRESSER entern Computer

Geld her oder Daten weg: So funktioniert die Verschlüsselungsmasche der Hacker

Hacker-Angriff auf den Bundestag: Generalbundesanwalt übernimmt Ermittlungen

SPIEGEL ONLINE - 20.01.2016

Frankfurter Allgemeine

Deutschland ist Hauptzielland von Cyberkriminalität

Geschätzter Schaden von 1,6 Prozent des Bruttosozialprodukts / Münch: Nicht verniedlichen

DER SPIEGEL

Russische Hacker unter falscher Flagge

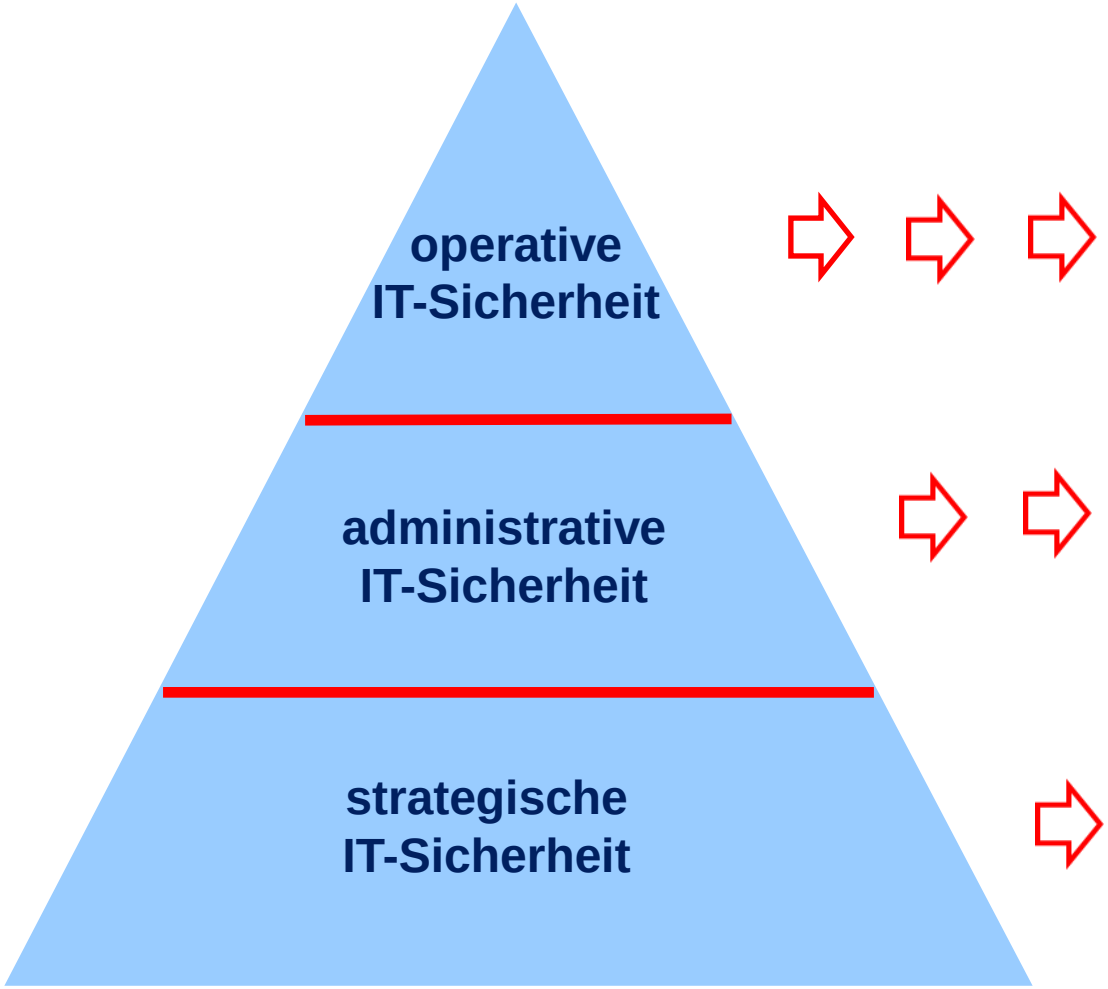
Deutsche Sicherheitsbehörden: „Islamischer Staat" ist nicht zu komplexen Computerattacken fähig.

Süddeutsche Zeitung

Fette Beute, kleines Risiko

Warum es so schwierig ist, gegen die neue Art von Computer-Attacken vorzugehen

IT-Sicherheitspyramide



- ➡ Umsetzung von Richtlinien
- ➡ Bearbeitung von Sicherheitsvorfällen CERT-Brandenburg im ZIT-BB (Computer Emergency Response Team)

- ➡ Informationssicherheitsmanagement-Team der Landesverwaltung
- ➡ Kompetenzzentrum IT-Sicherheit (CERT), Standardisierung im ZIT-BB (Dezernat 2.1)

- ➡ Informationssicherheitsleitlinie der Landesverwaltung und dessen Fortentwicklung (Beschluss 05.05.2014)
- ➡ Aufbau der Informationssicherheits-organisation (ISMT)

LAND BRANDENBURG

Brandenburgischer IT-Dienstleister

Kernaufgaben des Computer Emergency Response Teams CERT

- Bearbeitung von Sicherheitsvorfällen (Security Incident Response)
- Koordinierung von Schwachstellen
- Aufbau und/oder Betrieb zentraler Sicherheitsinfrastruktur
- Beratung und Sensibilisierung

VCV VerwaltungsCERTVerbund

LAND BRANDENBURG

Brandenburgischer IT-Dienstleister

Leistungsspektrum des CERT-Brandenburg

Allgemeine Dienstleistungen

- Unterstützung der Arbeit des Informationssicherheits-managementteams (ISMT)
- Mitarbeit bei der Erstellung von IT-Systemrichtlinien
- Betreiben eines Warn- und Informationsdienstes
- Betreiben einer Datenbank über Sicherheitsvorfälle
- Öffentlichkeitsarbeit

Präventive Dienstleistungen

- Betrieb technischer Sicherheitssysteme (IDS, Virenschutzmanagement, Logmanagement, IDM / PKI)
- Durchführung von Penetrationstests
- Verfolgung technologischer Trends
- Entwurf und Abstimmung landesweiter Richtlinien

Aktive Dienstleistungen

- Analyse eingehender Vorfallsmeldungen
- Erstellung von Empfehlungen
- Bearbeitung von Sicherheitsvorfällen
- Aktive Alarmierung bei akuten Gefährdungen
- Warnungen + Eskalation

Zusammenarbeit mit den Kommunen

- **Bereitstellung von CERT-Informationen auf Dialog Brandenburg**
- **über Sicherheitsvorfälle informieren**
- **Schulungen vom ZIT-BB zur Informationssicherheit**
- **Abgestimmte Maßnahmen vor „Großereignissen“**

Ziel: Gegenseitiger Informationsaustausch, denn Hacker kennen keine Verwaltungsgrenzen.

LAND BRANDENBURG

Brandenburgischer IT-Dienstleister

Vielen Dank für Ihr Interesse

Brandenburgischer IT-Dienstleister
14480 Potsdam, Steinstraße 104-106