



Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik

Stefan Becker
Referatsleiter Cyber-Sicherheit für die Wirtschaft

Brühl, 10.Juli 2019

Entwicklung der Digitalisierung

...mehr Datenübertragung

2016	2021
108.000 TB pro Std ¹	400.000 TB pro Std ¹

...mehr Geschwindigkeit

2016	2021
27 Mbps (fix) 7 Mbps (mobil) ¹	53 Mbps (fix) 20 Mbps (mobil) ¹

...mehr Geräte

2016	2021
fünf webfähige Geräte p.K. in D ¹	neun webfähige Geräte p.K. in D ¹

...mehr Vernetzung

2016	2021
6 Mrd. M2M fähige Geräte ¹	14 Mrd. M2M fähige Geräte ¹

...mehr Angriffe

2016	2021
1,3 Mio. DDoS Angriffe >1 Gbps	3,1 Mio DDoS Angriffe >1 Gbps

¹ Quelle: CISCO VNI, 2017

Technologien für die Digitalisierung

>> Synergieeffekte
Cloud Computing
>> Zentralisierung der Daten
>> Permanenter Zugriff

>> Kryptowährungen
Blockchain
>> Direkte Koordinierung von Geräten
>> Distributed Ledger

>> potenzierte Rechenleistung
Quantencomputer
>> Quantenkryptografie
>> Post-Quantum

>> Vernetzung im Cyberraum
Internet der Dinge
>> Komplexität durch Integration
>> Allgegenwärtigkeit

>> wissensbasierte Systeme
KI – Künstliche Intelligenz
>> Neue Problemlösungsmöglichkeiten
>> Deep Learning

>> Datengenerierung und Kontrolle
Big Data
>> ungeahnte Auswertungsmöglichkeiten
>> Data Mining

>> Hohe Downloadgeschwindigkeit
5G Mobilfunkstandard
>> Verbesserte Servicequalität

>> Neue Datengewinnung
Sensorik & Aktorik
>> Automatisierte Steuerung

Anwendungen der Digitalisierung

>> Vernetze Lieferketten
Industrie 4.0 / Smart Factory
>> Vernetztes Arbeitsumfeld
>> Smart Factory

>> autonome Haushaltsroboter
Vernetztes Zuhause
>> Vernetzte Haushaltssensoren
>> Smart TV

>> automatisierte Versorgung
Intelligente Stromnetze
>> Vernetztes Arbeitsumfeld
>> Smart Meter

>> intelligente Ampelschaltung
Vernetzte Stadt
>> Interagierende Infrastruktur
>> Smart City

>> selbstfahrende Autos
Vernetzte Autos
>> Interaktion mit Infrastruktur
>> Smart Car

>> automatisierte Versorgung
Vernetztes Gesundheitswesen
>> Neue Möglichkeiten durch Datenauswertung
>> eHealth

Digitalisierung und Technologieentwicklung

Sichtbare Chancen,
unsichtbare Bedrohungen



Ransomware

- Weiterhin **zahlreiche neue Ransomware-Varianten**
- **Diversifizierung** der Angriffsvektoren, **Verbreitung** über SPAM, Exploit-Kits, Drive-by-Exploits, Web-Server-Schwachstellen, Würmer, Fernwartungs-Software, Erraten von Passwörtern an öffentl. zugängl. Endpunkten
- Trend zu **gezielten Angriffe auf Unternehmen hält an**

Massenangriffe

Bedrohungslage



Quelle: BSI

Schadprogramme

- Neue Varianten in immer kürzeren Abständen erschweren die Erkennung durch (klassische) AV-Produkte
- Täglich ca. **390.000** neue Schadprogramm-Varianten
- Mehr als **770 Millionen Varianten** bekannt
- Mobile Endgeräte:
 - fast ausschließlich für Google Android
 - Mehr als **28 Millionen** verschiedene Schadprogramme
 - Pro Monat **690.000** neue Varianten für Android

Mobile Endgeräte im Visier

Bedrohungslage



IT-Sicherheitsvorfälle



Unbefugte Veröffentlichung von persönlichen Daten – „Politleaks“

- Veröffentlichung hunderter gestohlener Datensätze von Prominenten und Politikern
- Angriff erfolgte überwiegend auf private und persönliche Accounts der Betroffenen
- Januar 2019

Update: Unbefugte Veröffentlichung von persönlichen Daten und Dokumenten im Internet

Ort Bonn
Datum 05.01.2019

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist Anfang Dezember 2018 von einem Mitglied des deutschen Bundestages darüber informiert worden, dass dieser fragwürdige Bewegungen auf privaten und personalisierten E-Mail- und Social-Media-Accounts festgestellt habe. Das BSI hat diesen Fall sehr ernst genommen und ihn in das Nationale Cyber-Abwehrzentrum eingebracht. Zu diesem Zeitpunkt gingen alle Beteiligten von einem Einzelfall aus.

Das BSI hat dem betroffenen MdB Unterstützung angeboten und war mit einem Mobile Incident Response Team vor Ort. Von einer geplanten oder getätigten Veröffentlichung der gestohlenen Informationen oder einem Zusammenhang mit den durch den Twitter-Account "G0d" (@_orbit) veröffentlichten Daten hatte das BSI bis zur Nacht vom 3. auf den 4. Januar 2019 keine Kenntnis. Erst durch das Bekanntwerden der Veröffentlichung der Datensätze über den Twitter-Account "G0d" am 3. Januar 2019, konnte das BSI in weiterer Analyse am 4. Januar 2019 diesen und vier weitere Fälle, die dem BSI im Verlauf des Jahres 2018 bekannt geworden sind, in diesen Zusammenhang stellen.

Anfang Dezember 2018 war in keiner Weise absehbar, dass es weitere Fälle gegeben hat. Ein Zusammenhang der oben genannten Einzelfälle konnte erst im Nachhinein durch die Analyse der Gesamtheit der aktuell im ganzen veröffentlichten Datensätze festgestellt werden.

Quelle: [bsi.bund.de](https://www.bsi.bund.de)

IT-Sicherheitsvorfälle



Windows-Schwachstelle: BSI warnt vor möglichen wurmartigen Angriffen

- Kritische Schwachstelle im Remote-Desktop-Protocol-Dienst (RDP)
- Ermöglicht wurmartigen Angriff
- Mai 2019

Windows-Schwachstelle: BSI warnt vor möglichen wurmartigen Angriffen

Ort	Bonn
Datum	15.05.2019

Für das Microsoft-Betriebssystem Windows besteht eine kritische Schwachstelle im Remote-Desktop-Protocol-Dienst (RDP). Die Schwachstelle ist aus der Ferne und ohne Zutun des Nutzers ausnutzbar und ermöglicht daher einen Angriff mit Schadsoftware, die sich wurmartig selbstständig weiterverbreitet. Dies hat [Microsoft mitgeteilt](#). Sicherheitsupdates für unterschiedliche Windows-Versionen stehen bereits zur Verfügung. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) rät Anwenderinnen und Anwendern, den [jeweiligen Patch](#) möglichst umgehend einzuspielen. Betroffen sind alle Windows- und Windows-Server-Versionen bis einschließlich Windows 7 und Windows-Server 2008. Microsoft hat auch für [Windows-Versionen, die grundsätzlich nicht mehr unterstützt werden, Patches zur Verfügung gestellt](#), so etwa für Windows XP. Windows 10 ist Microsoft zufolge nicht betroffen. Das BSI hat eine Cyber-Sicherheitswarnung mit detaillierten Handlungsempfehlungen an Betreiber Kritischer Infrastrukturen und die Teilnehmer der [Allianz für Cyber-Sicherheit](#) ausgesprochen.

"Diese kritische Schwachstelle kann zu ähnlich verheerenden Angriffen führen, wie wir sie 2017 mit WannaCry erleben mussten. Windows-Anwender sollten daher die vorhandenen Updates umgehend installieren, bevor es zu größeren Schäden kommt. Das BSI stellt derzeit eine Vielzahl an kritischen Schwachstellen fest, nicht zuletzt in aktueller Chip-Hardware. Es zeigt sich erneut, wie wichtig Software-Qualität ist und welche Bedeutung security-by-design und security-by-default einnehmen müssen. Durch die zunehmende Digitalisierung wird sich unsere Welt immer stärker vernetzen und

Quelle: [bsi.bund.de](https://www.bsi.bund.de)



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

Produkte und Dienstleistungen des BSI



Nationales Verbindungswesen des BSI

Koalitionsvertrag 2018

- Ausbau des BSI als nationale Cyber-Sicherheitsbehörde und als Beratungsstelle für Unternehmen, Bund und Länder

Aufgaben

- Regelmäßige Präsenz im Verbindungsbüro in Hamburg
- Bessere Erreichbarkeit für Bundesbehörden, Länder und die
- Wirtschaft
- Vermittlung von fachlichen Ansprechpartnern im BSI
- Beratung zum Produkt- und Dienstleistungsportfolio des BSI

Nationales Verbindungswesen



Informationssicherheit in der Praxis – IT-Grundschutz des BSI

IT-Grundschutz ist ein ganzheitlicher Ansatz.



Fazit

- Cyber-Sicherheit ist Voraussetzung für die erfolgreiche Digitalisierung
- Die Bedrohungslage bleibt auf hohem Niveau angespannt
- Das BSI gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft

