IT-Sicherheit

Verlässliches Schutzschild der Digitalisierung

Bitkom-Positionen für ein digitales Deutschland

1. Status Quo

- Die Digitalisierung nimmt immer weiter zu und die zu schützenden Infrastrukturen werden immer komplexer. Zudem werden jeden Tag neue Sicherheitsvorfälle bekannt, die die betroffenen vor neue Herausforderungen stellt.
- Nicht mehr nur Hacker und die organisierte Kriminalität, auch ausländische Staaten können eine Bedrohung für die Sicherheit von Daten und Informationssystemen darstellen.
- Der Cyberraum ist ein lukratives Betätigungsfeld für Kriminelle.

2. Ziele

- **Eigene Infrastrukturen absichern**: Handlungsspielräume aller Akteure (Staat, Wirtschaft, Bürger) müssen erkannt und genutzt werden.
- **Verschlüsselung umfassend einsetzen**: IT-Sicherheit muss durch die Möglichkeit der Verschlüsselung wirksam gewährleistet werden können.
- **Informationsaustausch erweitern**: Informationen müssen zur Verteidigung gegen Angreifer ausgetauscht werden. Die brancheninterne sowie branchenübergreifende Zusammenarbeit muss genauso intensiviert werden, wie die Zusammenarbeit zwischen Staat, Behörden und Wirtschaft.
- **Cyber-Kriminalität muss durch fehlende Anreize unattraktiver werden.**
- **Akutem Fachkräftemangel im Bereiche der IT-Security schneller begegnen**: Es müssen deutlich mehr Fachkräfte in diesem Bereich als IT-Sicherheitsexperten, ggf. auch mit branchenspezifischen Ausprägungen, ausgebildet werden.

»Die Verschlüsselung von Netzwerkverbindungen sollte zum Standard gehören, wird bislang aber nur von 83 Prozent der Unternehmen eingesetzt. Nur 48 Prozent der Industriebetriebe verschlüsseln Daten auf Datenträgern und 46 Prozent ihre elektronische Kommunikation per E-Mail.[1]«

Stand: 24.01.2018

bitkom

3. Politische Vorschläge

- **Normen für Cybersecurity auf zwischenstaatlicher Ebene etablieren**: Auf internationaler Ebene soll die Bundesregierung sich für die Etablierung von Normen im Cyberraum einsetzen. Diese könnten neben Leitlinien für ein verantwortungsvolles Verhalten im Cyberraum auch eine Selbstverpflichtung im Umgang mit Cyberwaffen enthalten.
- **Digitale Souveränität stärken**: Es müssen ministerienübergreifende und abgestimmte Maßnahmen zur Erhöhung der Digitalen Souveränität ergriffen werden. Dabei ist das Begriffsverständnis wie vom Bitkom im Februar 2015 definiert zu verwenden[2]:

  1 Digitale Souveränität bedeutet die Fähigkeit zu selbstbestimmtem Handeln und Entscheiden im digitalen Raum;

  2 Digital souveräne Systeme verfügen bei digitalen Schlüsseltechnologien und –kompetenzen, entsprechenden Diensten und Plattformen über eigene Fähigkeiten auf internationalem Spitzenniveau.

  Es geht insbesondere um die Wahrnehmung der staatlichen Schutzfunktion, für genutzte Daten in Deutschland und in der EU sowie die Etablierung und Erhaltung technischer Kompetenzen zur Bewertung der IT-Sicherheit von Produkten und Diensten.

- **Schlüsselrolle des BSI für die nationale Informationssicherheits-Wirtschaft anerkennen und umsetzen**: Die Wirtschaft braucht ein starkes und gut ausgestattetes BSI als Partner und Unterstützer. Wir fordern daher, auch den zweiten Korb des IT-Sicherheitsgesetzes mit weiteren Ressourcen für das Bundesamt zu verbinden. Durch die zunehmende Breite der Aufgaben des BSI und die fortschreitende Digitalisierung halten wir eine Verdoppelung der Personal- und Finanzausstattung des BSI innerhalb der kommenden Legislaturperiode für erforderlich.
- **IT-Sicherheit muss sicher bleiben**: Wir brauchen auch weiterhin ein starkes Bekenntnis zu den Krypto-Eckpunkten aus dem Jahr 1999. Mit Blick auf die notwendigen Aktivtäten der Sicherheitsbehörden im Rahmen von »Zitis« halten wir einen klaren Rechtsrahmen und wirksame Kontrollen für unumgänglich um die nötige Legitimation und gesellschaftliche Akzeptanz zu schaffen.
- **Ausreichend hochqualifizierte Fachkräfte ausbilden**: Es müssen mehr IT-Sicherheitsexperten ausgebildet werden. Des Weiteren müssen die Studiengänge entsprechend attraktiv und praxisnah in den jeweiligen Anwenderbranchen ausgestaltet werden, um auch nötiges Branchenwissen im Kontext der IT-Sicherheit zu vermitteln. Berufsbegleitendes Studieren kann hier ein wichtiges Element sein.

69%

Zwei von drei Industrieunternehmen sind in Deutschland in den vergangenen zwei Jahren Opfer von Datendiebstahl, Wirtschaftsspionage oder Sabotage geworden.[1]

22,35

Milliarden Euro Schaden pro Jahr.[1]

1 Bitkom-Studie »Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie« (2016)
2 https://www.bitkom.org/noindex/Publikationen/2015/Positionspapiere/Digitale-Souveraenitaet/BITKOM-Position-Digitale-Souveraenitaet.pdf

Ihr Ansprechpartner

Teresa Ritter | Referentin Sicherheitspolitik
T 030 27576-203 | t.ritter@bitkom.org

Albrechtstraße 10 | 10117 Berlin
www.bitkom.org

bitkom