
BLOCK 01
BLOCK 01
BLOCK 01
BLOCK 01
BLOCK 01

Cyber-Sicherheit

Digitale Informations- und Kommunikationstechnik darf kein rechtsfreier Raum werden!

Computerkriminalität oder Cyberkriminalität (engl. Cybercrime) nimmt in den letzten Jahren deutlich zu. Gleichzeitig nehmen auch unsere Aktivitäten im Rahmen der digitalen Informations- und Kommunikationstechnik zu. Wir heben unser Geld am Bankautomaten ab, wir verschicken E-Mails, wir planen Bahnstrecken, Straßenverkehr und Flugverbindungen. Behörden speichern persönliche Daten der Bürger, Energieversorger, Automobilhersteller, Kreditinstitute und Telekommunikationsanbieter sind in ihren Abläufen komplett digitalisiert. Unser Zeitalter ist von der globalen Vernetzung geprägt. Diese Vernetzung wird immer weiter ausgebaut. Das digitale Netz, in dem wir uns befinden, wird immer größer. Es wird aber leider nicht stärker. Es wird immer anfälliger für Angriffe und Übergriffe auf unseren Datenverkehr, wie der WannaCry-Hackerangriff uns erschreckend vor Augen geführt hat. Natürlich ist die Vernetzung längst unverzichtbar für uns alle geworden. Aber was unverzichtbar ist, muss geschützt werden. Was unverzichtbar ist, muss sicher sein. Wenn wir von Innerer Sicherheit sprechen und eine erfolgreiche Sicherheitspolitik machen wollen, dann darf die Forderung nach mehr Sicherheit für unsere Computersysteme nicht hinten anstehen. Heutzutage muss der Schutz vor einem Angriff auf unser digitales Netz die gleiche Priorität haben wie vor einem Terroranschlag. Cyberangriffe auf unsere Daten sind Terroranschläge auf digitaler Ebene.

Unsere Positionen:

- Risiken, die Vernetzung angreifen zu können, müssen minimal gehalten werden
- Förderung regelmäßigen Einspielens von Softwareupdates, um vorhandene Sicherheitslücken im System vorzeitig zu schließen
- Sicherheitsbehörden müssen deutlich nachrüsten
- Aufstockung des IT Personals der Sicherheitsbehörden
- Umgang mit den persönlichen Daten muss sensibel und sicherheitsbewusst sein