**BB IT SECURITY Basics - 2022-12-01**

German Version

**Zusammenfassung der wichtigsten Maßnahmen für: Vertraulichkeit, Verfügbarkeit und Integrität digitaler Daten.**

# Backup (Datensicherheit gg. Verlust)

* Sollte automatisiert gehen (damit es auch wirklich regelmäßig gemacht wird, und auch damit es keine Produktivitätsbremse ist)
* Datenträger beschriften oder Excelsheet machen: Was ist wo gesichert, denn:
	+ sobald ein Datenträger kaputt ist, kann man auch nicht mehr schauen was drauf war.
* Idealerweise: Backupdatenträger an anderem Ort lagern

# Updates (Security gg. Cyberangriffe)

* (Automatische) Updates aktivieren:
	+ Windows
	+ Produktivsoftware

# Policy (Richtlinien und Schulung)

* Grundsätzlich gute Regeln hier wären zB:
	+ Keine USB Sticks von zuhause am Firmen-PC anschließen
	+ Vorsicht bei Phishing-Mails: Besonders auf Absender und Domains von Links achten.

# Zusätzliche Maßnahmen (Virenschutz, etc.)

* Produktivsysteme als Images sichern zu einem Zeitpunkt, zu dem sie reibungslos funktionieren. zB Mit „Macrium Reflect“.
* Windows Defender aktivieren inkl. „Echtzeitschutz“, „Cloudbasierter Schutz“ und „Manipulationsschutz“ (meist als Virenschutz ausreichend)

# Vertraulichkeit von (Patienten-)Daten

* Keine öffentlichen Hosts für vertrauliche Daten verwenden wie Google Cloud, GitHub, Windows Clouddienste, Dropbox, etc.
* Keine Vertraulichen Informationen via Email

Und wenn doch: verschlüsselt. Schlüsselaustausch entweder persönlich, via verschlüsselter Dienste wie Signal oder PGP (Mailverschlüsselung), oder Schlüsselinfrastruktur wie e-Card (Bürgerkarte), Handysignatur nutzen.