2. CYBER SECURITY

Cyber Security ist eines der meist behandelten Themen im Geschäftsumfeld – und das seit Jahren. Diese Attraktion ist jedoch leicht zu begründen, schließlich geht es bei dem Thema Sicherheit um nicht weniger als um Angst, Vertrauen und eben auch um Geld. Bei diesem Thema wird der Mensch schnell aufmerksam. Dabei ist es nicht einfach, das Thema Cyber Security scharf abzugrenzen. Wie ist Cyber Security definiert, wie Internetsicherheit, Informationssicherheit oder Datenschutz? Werden 100 Personen bezüglich der Überschneidungen und Unterschiede dieser Themenbereiche gefragt, so ist die Wahrscheinlichkeit nicht niedrig, auch 100 unterschiedliche Antworten zu erhalten.

Cyber Security ist unter anderem deshalb ein so kompliziertes und eben auch interessantes Thema, weil es auf so vielen unterschiedlichen Ebenen behandelt werden kann. Cyber Security ist selbstverständlich technischer Natur, aber ebenso hat es eine organisatorische Dimension: Nur wenn eine Maßnahme auch wirklich in einen Prozess integriert werden kann, wird diese verwendet. Darüber hinaus gibt es eine politische Ebene („wessen" Datenschutzgesetze werden beim Surfen angewendet) und eben auch eine menschlich-soziale: Der Anwender muss die Maßnahmen auch wollen, keine Berührungsängste haben und sie insbesondere auch verstehen.

Auch innerhalb der beispielhaft vorgestellten Ebenen gibt es einen schwierigen Kompromiss zu finden: Im Grunde hat man es stets mit einem „Wähle zwei: Sicherheit, Nutzbarkeit, Kosten" zu tun. Möchte man eine sichere und einfach zu bedienende Lösung haben, so wird sie teuer sein. Möchte man eine einfach zu bedienende und günstige Lösung haben, so wird die nicht sicher sein. Und schließlich wird eine günstige und sichere Lösung nur schwer anzuwenden sein. Sowohl für Unternehmen als auch für Privatanwender gilt es nun, einen möglichst passenden Weg zu beschreiten.

Eine dritte inhärente Schwierigkeit beim Thema Cyber Security ist die Dynamik. Die Welt wird immer schneller und so ist eine „sichere" Maßnahme schon bald wieder unsicher. Stets muss nicht nur auf das eigene System geschaut werden, sondern auch der „Feind" im Blick behalten werden. Und auch der Ausdruck „sichere Maßnahme" ist schon gewagt, da es hundertprozentige Sicherheit eben nicht gibt. Um von einer Sicherheit zu sprechen, müsste man es formell beweisen. Einfacher ist es für einen Angreifer, da dieser nur ein einziges Gegenbeispiel benötigt, um eine postulierte Sicherheit zu zerstören.

Das Oberthema Cybersicherheit haben alle Beiträge gemeinsam. Aber ebenso facettenreich wie das Thema Cybersicherheit sind auch die einzelnen Beiträge selbst. Sie reichen von prozessorientiertem Datenschutz und Governance bis zu den vielfältig eingesetzten digitalen Identitäten und konkreten Ausprägungen angewandter Sicherheit.

INHALT