Artikel für Informatikspektrum 5.12.2018

Cyberverantwortung

Cyber…all unsichtbar

Cyber Threat, Cyber Security, Cyber risk….Cyber ist heute in aller Munde!

Man hört und liest viel, zum Beispiel, dass ein Spital keinen Zugriff mehr auf Daten hatte und erpresst wurde. Erst nach erfolgter Geldzahlung, wurde der Datenzugriff wieder entsperrt. Offenbar wurden die Daten mit einer Ransomware, einer speziellen Software, die mit einem Email zugeschickt wurde, verschlüsselt. Ein unaufmerksamer Mitarbeiter hatte die Email geöffnet….

Das Wort Cyber kommt übrigens ursprünglich aus dem Griechischen, oder heute Englischen (Cybernetics) und bedeutet Tätigkeit und Wissenschaft im Umgang mit Navigieren und Steuern.

Und dieses Navigieren findet heute in der digitalen Welt statt, oder sollte zumindest in der digitalen Welt stattfinden. Und genau hier liegt auch das Problem, resp. die Herausforderung für Unternehmungen.
Im Zentrum und Basis der unternehmerischen Tätigkeit und somit das wesentliche Assett ist die Information. Diese wird heute fast ausschliesslich digital bearbeitet, gelagert, archiviert und weitergeleitet. Und genau so wie in der physischen Welt Bedrohungen und Risiken allgegenwärtig sind, ist das auch in der virtuellen Welt der Fall. Es gibt nur einen sehr unangenehmen Unterschied: die Risiken sind unsichtbar und somit auch wenig vorhersehbar und vorstellbar für die Verantwortlichen.

Informationslandkarte und Innovationsschutz

Viele Unternehmungen und deren verantwortliche Personen haben kaum einen Überblick über die für sie relevanten Informationen und wo und in welcher Beziehung sie davon auch abhängig sind. Sinnvoll wäre die Erstellung einer Landkarte, wo ersichtlich ist, welche Informationen wo vorhanden sind und welche in welchen Produkten verwendet werden. Daraus wird auch gleich klar, ob im Unternehmen entsprechende Verantwortlichkeiten bestimmt sind und wo gegebenenfalls Abhängigkeiten von Dritten (Providern) bestehen. Insbesondere bei unternehmensübergreifenden Businessprozessen oder der Einbindung von Infos in IoT bestehen übergreifende Abhängigkeiten und somit Risiken.
Es gilt diese Informationen von Zugriffen Dritter oder Wirtschaftsspionage unbedingt geheim zu halten und dazu sind entsprechende technische Vorkehrungen zu treffen.

Geheimhaltung

Im Aussenverhältnis sind Unternehmungen und Organisationen aus vertraglichen (NDA) oder gesetzlichen Gründen zur Geheimhaltung verpflichtet. Es gibt aber durchaus gute Gründe, weshalb eine Unternehmung auch aus Eigeninteresse Informationen geheim halten und schützen will und muss. Es gilt Wettbewerbsvorteile zu schützen oder auch die Funktionsweise von Produkten, die auch datenbasiert arbeiten, zu sichern. Eine Herausforderung ist auch hier wieder die Vernetzung von Prozessen und Produkten über Unternehmens- und Landesgrenzen hinweg. Daraus entstehen ganz neue und oftmals sehr komplexe Abhängigkeiten und Risikofelder.

Im Bereich von Geheimhaltungen zum Beispiel ist es zentral, dass man sich gut überlegt, wie weit der Kreis der Geheimhaltung sinnvollerweise gezogen werden darf mittels Einbezug von Providern und inwieweit die betroffenen Personen und Unternehmungen über die damit einhergehenden Risiken informiert werden müssen.

Staatliche Interventionen

Sobald staatliche Interessen, auch häufig kurzfristig und politisch motiviert, ins Spiel kommen, sind Informationen mit einer anderen Dimension von Risiken konfrontiert. Mit der Staatsräson rechtfertigen insbesondere Geheimdienste, allen voran der NSA, das Ausspionieren von Informationen. Die

Rechtsstaatlichkeit, die sich eigentlich auf dem Stadtgebiet absolut erstreckt, wird auch durch den Cloud-Act verletzt. Demgemäss müssen Informationen, die sich bei einem amerikanischen oder übers Mutterhaus zu einem amerikanischen Konzern gehörenden Provider befinden herausgegeben werden, wenn dies ein amerikanisches Gericht verfügt. Dies sind ganz neue Risikokategorien, denen es mittels Providerstrategien zu begegnen gilt.

Post und Email

Die klassische Papierpost gehört in vielen Bereichen schon der Vergangenheit an. Es wird gemailt, und dies zumeist unverschlüsselt und unsigniert. Die oben beschriebenen Risiken stellen sich natürlich hier tagtätlich. Interessant ist, dass gerade hier die digitale Welt sogar noch bessere Lösungen anbietet als die traditionelle.
Dazu eignen sich folgende Formen: die gewöhnliche, die verschlüsselte, die signierte und die eingeschriebene Email. Alle vier Formen eignen sich für die schnelle Zustellung. Jedoch kann nur bei der signierten und eingeschriebenen Email die Nichtabstreitbarkeit des Absenders, die Integrität und deren Inhalt sichergestellt werden. Die verschlüsselte und die eingeschriebene Email sind als vertraulich einzustufen. Jedoch kann nur die eingeschriebene Email die Nichtabstreitbarkeit des Empfangs gewährleisten und kann im Gegensatz zum eingeschriebenen Brief schneller zugestellt werden, ihr Inhalt ist nachweisbar und der Absender kann nicht bestritten werden.

Verantwortung

Die Führungsverantwortlichen von Organisationen und Unternehmungen sind zu sorgfältiger Tätigkeit verpflichtet und damit verbunden auch zur Reduktion von Risiken. Das erforderliche Spezialwissen fehlt aber noch weitgehend, die digitale Welt und deren Risiken sind noch so neu, dass man oftmals nicht einmal die richtigen Fragen stellen kann. Hier ist guter Rat im wahrsten Sinne des Wortes teuer…, aber man kommt nicht darum herum, sich bei kompetenten Externen Hilfe zu holen.

Fazit

Die Cyberverantwortung obliegt den Unternehmen. Die immer zunehmende Digitalisierung bringt Risiken mit sich, welche es zu beseitigen oder minimieren gilt. Während man sich eine Übersicht verschafft, wo welche Daten bearbeitet werden und an wen diese gelangen (sollen), ist der Staat immer im Hinterkopf zu bewahren. Dieser argumentiert oftmals mit dem überwiegenden öffentlichen Interesse, um an Daten zu gelangen. Im Bereich der Kommunikationsmittel ist die eingeschriebene Email als sicherstes Kommunikationsmittel einzustufen und damit ein geeignetes Mittel, um die Cyberverantwortung wahrzunehmen.

Ursula Sury ist selbständige Rechtsanwältin in Luzern, Zug und Zürich (CH) und Vizedirektorin an der Hochschule Luzern - Informatik. Sie ist zudem Dozentin für Informatikrecht, Datenschutzrecht und Digitalisierungsrecht.