März 2019

Was tun gegen Cyber-Risiken?

Nach langer Diskussion gibt es jetzt zwischen Bund und Ländern die Einigung auf den Digitalpakt Schule. Auch wenn es bisher kein erkennbares didaktisches Konzept für die Nutzung digitaler Medien im Unterricht zu geben scheint, zeigt dies eindeutig, dass sich in den knapp sechs Jahren, nachdem die Bundeskanzlerin das Internet als „Neuland" entdeckt hat, viel verändert hat.[1] Die großen Vorteile des Internets mit einer ständigen Verfügbarkeit fast aller Informationen dieser Welt bietet auf der Gegenseite aber auch neue Risiken.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) schreibt dazu Anfang 2019: „Die Gefährdungslage ist weiterhin hoch. Im Vergleich zum vorangegangen Berichtszeitraum hat sie sich weiter verschärft und ist zudem vielschichtiger geworden. Es gibt nach wie vor eine hohe Dynamik der Angreifer bei der Weiterentwicklung von Schadprogrammen und Angriffswegen. Darüber hinaus gibt es z. B. mit den entdeckten Schwachstellen in Hardware eine neue Qualität der Bedrohung, wie bei den Sicherheitslücken Spectre/Meltdown und Spectre NG, die ohne einen Austausch der Hardware nicht vollständig geschlossen werden können."[2] Hier ein paar Beispiele:

- 2015 wurde das ukrainische Energienetz attackiert
- 2017 kam es zu einem Angriff auf das Auswärtige Amt
- 2018 standen u.a. Energieversorger in Deutschland im Fokus

Während solche Cyberangriffe meist in der Öffentlichkeit nur begrenzt wahrgenommen werden, ist sicherlich der globale Einsatz der Schadsoftware „Wannacry" unvergessen, die 2017 u.a. Verbindungstafeln an Bahnhöfen befallen hat und über die sehr breit berichtet worden ist. Quasi täglich gibt das BSI neue Sicherheitswarnungen für Privatpersonen und kleine Unternehmen heraus.[3] Was aber bedeutet es für Unternehmen und Privatpersonen, wenn sie Opfer eines solchen Cyberangriffs werden? Wie kann man sich gegen die Folgen absichern?

Wie Sie es von uns kennen, werden wir uns auf den finanziellen Aspekt dieser Fragestellung beschränken. Fragen der technischen und organisatorischen Sicherheit sollten Sie mit Ihrem IT-ler besprechen. Spezielle Cyber-Absicherungen, die schon teils für weniger als 10 Euro monatlich erhältlich sind, können den finanziellen Verlust weitgehend absichern:

Typische Risiken für Privatpersonen und Unterstützung durch die Cyber-Versicherung sind[4]:

- Betrug im Internethandel: Wird eine schon bezahlte Ware nicht geliefert, wird der Kaufpreis erstattet.
- Beschädigung von Daten oder Hardware durch Cyberangriffe: Im Rahmen von Höchstgrenzen werden Kosten zur Reparatur und Datenwiederherstellung übernommen.
- Veröffentlichung privater Daten: Anwaltliche Beratung und Erstunterstützung bei der Löschung der Daten
- Inanspruchnahme durch Weiterverbreitung von Schadsoftware: Kostenübernahme für Schadensersatz im Rahmen der Höchstgrenzen
- Cybermobbing: Psychologische Erstberatung

[1] Vgl. http://www.spiegel.de/netzwelt/netzpolitik/kanzlerin-merkel-nennt-bei-obama-besuch-das-internet-neuland-a-906673.html
[2] Vgl. https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html
[3] Vgl. https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Buerger-CERT/Sicherheitshinweise/Sicherheitshinweise_node.html
[4] Die Beispiele der Übernahme durch die Versicherung stammen von unseren Kooperationspartnern, deren Cyber-Policen wir empfehlen können. Bitte prüfen Sie Ihren individuell vereinbarten Schutz!

Anschrift
Dr. König und Kollegen GmbH
Eisenbahnstrasse 27
52459 Inden

Telefon
02465 - 304 825
Fax
02465 - 300 997

Email
info@koenig-kanzlei.de
Internet
www.koenig-kanzlei.de

Bankverbindung
Deutsche Bank Düren
BIC/SWIFT: DEUTDEDB395
IBAN: DE82395700240809595200

USt-IdNr.
DE815387385

- Smart-Home-Angriffe: Übernahme Reparatur und Schadensersatzansprüche im Rahmen von Höchstgrenzen

Bei Firmen kommen durch die zunehmende Vernetzung zwischen Anbietern, Kunden, Diestleistern und Datenbanken noch ergänzende Risiken hinzu. Einerseits Verluste durch Produktionseinschränkungen, zudem Reputationsrisiken und abschließend erhöhte Haftungsregeln, beispielsweise aus der neuen Datenschutzgrundverordnung (DSGVO). Allein die möglichen Bußgelder für Verstöße gegen das DSGVO können bis zu 4% der weltweiten Jahresumsätze betragen.[5] Folglich gibt es für Unternehmen spezialisierte Absicherungen und unterteilte Cyber-Betriebsunterbrechungsversicherung, Cyber-Eigenschadensversicherung und Cyber-Haftpflichtversicherung. Da laut einer Studie des Branchenverbands Bitkom in den letzten zwei Jahren jedes zweite deutsche Unternehmen einen IT-Angriff erleiden musste und viele hohe Schäden verzeichneten, empfiehlt sich die Umsetzung von IT-Sicherheitsstrategien und die Absicherung der Risiken.[6] Wenn es Kriminellen beispielsweise gelingen sollte, in die Datenbanksysteme eines Unternehmens einzubrechen und Daten zu entwenden, Produktionssysteme lahmzulegen oder Lieferketten zu stören, kommen die Versicherer für die Gesamtheit der Schäden oder Teile davon auf. Zudem übernehmen Cyber-Absicherungen oftmals auch die Kosten für die Wiederherstellung der Daten und zur Schließung der Lecks in den IT-Systemen.

Fazit:
Ob Privatperson oder Unternehmen. Die Chancen der Digitalisierung werden in der Breite sehr gerne genutzt. Die damit einhergehenden zusätzlichen Herausforderungen oder die dadurch neu entstehenden Risiken werden bisher noch zu häufig verdrängt.
Wie bei der Nutzung von Kraftfahrzeugen eine Kfz-Versicherung Standard ist, oder jede Person eine Privathaftpflichtversicherung haben sollte, empfiehlt sich auch im Bereich IT für Privatpersonen und Unternehmen eine Absicherung gegen die Risiken aus dem Cyberraum zu nutzen.
Sollten auch Sie einen solchen Schutz abschließen wollen, stehen wir Ihnen gerne für Fragen zur Verfügung.

Ihr

Dr. Michael König

[5] Vgl. Art. 83 DSGVO
[6] Vgl. https://www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutzstudie-2018.html

Anschrift
Dr. König und Kollegen GmbH
Eisenbahnstrasse 27
52459 Inden

Telefon
02465 - 304 825
Fax
02465 - 300 997

Email
info@koenig-kanzlei.de
Internet
www.koenig-kanzlei.de

Bankverbindung
Deutsche Bank Düren
BIC/SWIFT: DEUTDEDB395
IBAN: DE82395700240809595200

USt-IdNr.
DE815387385