Cyberrisiken

Aktuelle Probleme und Lösungsansätze

Wolf-Dieter Jordan
Geschäftsführer
OWL Vorsorge und Versicherungsservice GmbH Paderborn

Das Internet der Dinge, also die Vernetzung von Alltagsgegenständen und virtuellen Geräten, ist in vollem Gange. Das Leben wird durch Assistenzsysteme immer bequemer. Aber wird es auch sicherer?

Heute ist es bereits zur Gewohnheit geworden, über das Smartphone oder das Tablet per Applikationen Musikanwendungen, die Raumtemperatur oder die Lichtzufuhr zu steuern. Und die Möglichkeiten, über Smartwatches Gesundheitsdaten zu analysieren sowie bei Notfällen an die Ärzte zu senden, bestehen ebenfalls bereits. In Unternehmen werden Fahrzeuge über das Internet gesteuert, um deren wirtschaftliche Leistung zu optimieren. 3D-Drucker sind in der Lage, vielfältige Materialien zu verarbeiten und in Form zu bringen. Man kann davon ausgehen, dass zukünftig alles, was vernetzt werden kann, auch vernetzt sein wird. Schöne neue Welt mit interessanten Möglichkeiten.

Diesen vielfältigen Chancen stehen allerdings auch Risiken gegenüber. Sind diese gefährlicher, als man zunächst vermuten kann?

Welchen Angriffen waren die User bereits ausgesetzt?

Im April 2011 mussten 77 Mio. Abonnenten des Sony PlayStation Networks feststellen, dass nichts mehr ging. Eine Cyberattacke führte zu einem vierwöchigen(!) Ausfall. Alle Datensätze wurden gestohlen. Im Mai 2015 wurde der Bundestag gehackt. Die Angreifer konnten sich so weitreichenden Zugang verschaffen, dass als Konsequenz die vollständige Bundestags-IT ausgetauscht werden musste.

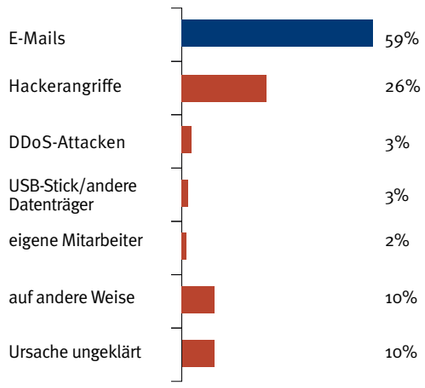
2016 wurden 28 Krankenhäuser in NRW Opfer von Cyberangriffen. Schadsoftware störte die IT-Systeme. Im Lukaskrankenhaus in Neuss führte Ransomware (Schadprogramme, die Daten verschlüsseln und dann einen Entschlüsselungscode gegen Lösegeld anbieten) zum Totalausfall.

Und selbst, wenn das Lösegeld gezahlt wird, meist in Bitcoins, bleibt in vielen Fällen nur die Neuinstallation mit hohem Aufwand an Zeit und Kosten.

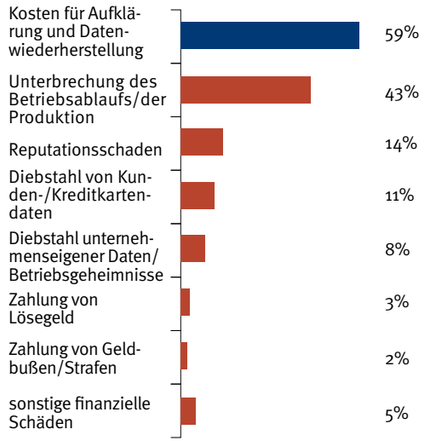
Bei mittelständischen Unternehmen, die in der Bewerbungsphase sind, haben die Hacker oftmals leichtes Spiel. Sie versenden verseuchte E-Mails mit Zip-Dateien getarnt als Bewerbungen, die im Eifer des Tagesgeschäfts geöffnet werden. Und dann verschlüsseln die Schädlinge rasend schnell die vollständige Netzwerkinfrastruktur. Was das für das Unternehmen bedeutet, kann man sich vorstellen.

Der Gesamtverband der deutschen Versicherungswirtschaft e.V. (GDV) hat in Zusammenarbeit mit Forsa im Frühjahr 2018 eine Befragung durchgeführt. In den meisten Fällen (fast 60 %) wurden die Systeme ganz einfach über E-Mails infiziert.

Die Einfallstore
Erfolgreiche Cyberangriffe erfolgten durch…[1]



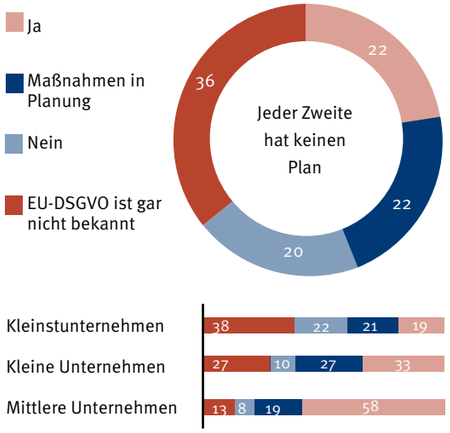
Die Schäden
Die Attacken führten zu wirtschaftlichen Schäden durch…[1]



[1] Mehrfachnennungen möglich

Das bedeutet, dass die Chefs und Mitarbeiter offensichtlich immer noch zu sorglos mit Cyberangriffen umgehen. Die Kosten für die Reinigung und Datenwiederherstellung dürften durch die Einführung der DSGVO (Datenschutz-Grundverordnung) im Mai 2018 noch weiter steigen, denn über 50 % der Unternehmen haben keine weiteren Vorkehrungen getroffen.

Überwiegend planlos
Haben Sie bereits Vorbereitungen zum neuen EU-Datenschutzrecht getroffen?



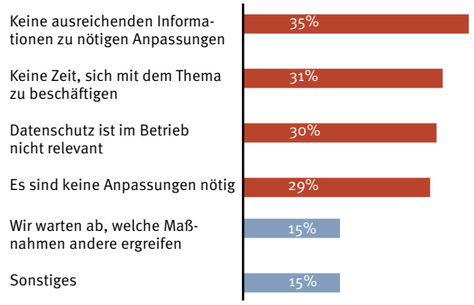
Angaben in Prozent
an 100 % fehlende Angaben: „weiß nicht“

Sehr anfällig für Attacken sind Unternehmen und Selbständige, die mit sensiblen Daten umgehen, wie Steuerberater, Hotels, Onlinehändler oder auch Einrichtungen im Gesundheitswesen, wie Krankenhäuser, Arztpraxen oder Pflegedienste. Wegen fahrlässigen Verhaltens von Mitarbeitern könnten Tablets, Smartphones oder Laptops mit sensiblen Daten ausgespäht werden. Eine Erpressung könnte eine Folge hieraus sein. Insbesondere, wer Kreditkartendaten verarbeitet, muss im Schadenfall mit hohem administrativen Aufwand und Kosten rechnen. Die Geschädigten müssen umfangreich informiert werden und können zudem Schadenersatzansprüche geltend machen.

Welche Maßnahmen sollten Unternehmen umsetzen, um die IT-Sicherheit zu erhöhen?

Unternehmen sind gut beraten, die bestehende Infrastruktur zu analysieren und zeitgemäße Sicherheitsmaßnahmen durch professionelle Systemhäuser zu implementieren. Die Mitarbeiter sollten regelmäßig in den Themen Datensicherheit und Umgang mit E-Mails geschult werden. Darüber hinaus ist eine komplexe Datensicherung mittels verschiedener Datenträger und Generationen, auch Cloudlösungen, zur schnellen Datenwiederherstellung angeraten.

Keine Ahnung, keine Zeit, keine Relevanz
Warum haben Sie bislang keine Vorbereitungen für die neue EU-DSGVO getroffen?



(Quelle: Cyberrisiken im Mittelstand, GDV 2018)

Unternehmen, die im Rahmen des Risikomanagements Cyberangriffskosten versichern wollen, können sog. Cyberpolicen abschließen.

Die versicherten Risiken sind in erster Linie:

- **Eigenschäden**
  Das sind Kosten der Datenwiederherstellung, der Rekonstruktion sowie die Kosten einer Betriebsunterbrechung, bspw. durch Cloud-Ausfall.
- **Fremdschäden**
  Schäden, die z. B. durch Datenmissbrauch und Lieferverzug entstehen sowie die Kosten für das Lahmlegen der IT von Kunden und/oder Zulieferern.
- **Serviceleistungen**
  - IT-Forensik
  - Anwälte für IT- und Datenschutzrecht
  - Soforthilfen im Notfall
  - Cybertraining oder Krisenprävention
  - Maßnahmen, um den Image- oder Reputationsschaden gering zu halten.

Die Versicherungsgesellschaften haben den Markt für Cyberrisiken erst neu entdeckt. Entsprechend unterschiedlich sind die Angebote, die im Markt zu finden sind. Um den optimalen Versicherungsschutz zu finden, sollten sich Unternehmen spezialisierter Versicherungsmakler bedienen, die sich mit den Themen bereits intensiv beschäftigt haben.

FAZIT

Durch die stetig steigende Vernetzung aller möglichen Dinge werden Cyberrisiken weiter stark wachsen. Unternehmen und Mitarbeiter gehen immer noch zu arglos mit den Bedrohungen um. Permanente Sensibilisierung aller Mitarbeiter sowie die professionelle Unterstützung durch IT-Unternehmen bei der Datensicherheit helfen, die Risiken zu managen. Um die Kosten bei Schadenfällen gering zu halten, können sich Unternehmen gegen Cyberrisiken versichern. Bei der Auswahl helfen versierte Versicherungsmakler.