Gesunder Menschenverstand gepaart mit dem richtigen Informationsfluss sorgt für IT-Sicherheit in kleinen und mittleren Unternehmen. Bild: sdecoret/Fotolia

Schutz vor Cyberangriffen für KMU

Kein Kritis – *keine Hilfe*

IT-Sicherheit | Um die Infrastruktur Deutschlands zu sichern, wurden das IT-Sicherheitsgesetz und die Verordnung zur Bestimmung kritischer Infrastrukturen entwickelt. Aber was tun Unternehmen, die nicht unter dieses Gesetz fallen?

Für Unternehmen, die in Branchen etabliert sind, die kritische Infrastrukturen bedienen, wurde der Begriff Kritis geprägt. Diese Unternehmen sichern mit ihrem Einsatz die Grundversorgung der Gesellschaft und müssen deshalb bestimmte IT-Standards erfüllen, um zu verhindern, dass Cyberangriffe das wirtschaftliche und soziale Leben gefährden. Dazu werden sie sogenannten Kritis-Sektoren zugeteilt: IT und Telekommunikation, Energie, Wasser, Ernährung, Gesundheit, Staat und Verwaltung, Transport und Verkehr, Finanz- und Versicherungswesen sowie Medien und Kultur. Anhand dieser Sektoren und der Kritis-Verordnung des Bundesamts für Sicherheit in der Informationstechnik (BSI) (§ 10 BSI-Gesetz), kann ein Unternehmer feststellen, ob sein Betrieb darunter fällt. Denn zwischenzeitlich sind immer mehr Firmen betroffen.

Zählt ein Unternehmen gemäß der Kriterien zum Kritis-Bereich unterliegt es dem sogenannten IT-Sicherheitsgesetz (IT-Sig). Das heißt, diese Betriebe müssen Mindeststandards für ihre IT-Sicherheit nachweisen – in der Regel mithilfe eines Informationssicherheitsmanagementsystems (ISMS). Das ISMS fasst feste Regeln und Verfahren zusammen, nach denen das einzelne Unternehmen agiert, um eine höchstmögliche IT-Sicherheit zu gewährleisten. Diese Standards werden durch „geeignete Maßnahmen", wie etwa Zertifizierungen oder Audits, nachgewiesen. Unterstützung hierfür gibt das BSI unter: www.bsi.bund.de.

Kein Äquivalent zu IT-Sig für Nicht-Kritis

Doch dieses Gesetz weist einen Denkfehler auf. Denn die Wirtschaft und Infrastruktur eines Landes ist untereinander vernetzt, so dass es sogar durch ein Nicht-Kritis-Unternehmen zu einem Dominoeffekt kommen kann. Und so wird sich der eine oder andere Nicht-Kritis-Unternehmer fragen: „Und wo bleiben wir?" Tatsächlich gibt es für Nicht-Kritis-Unternehmen bisher kein passendes gesetzliches Äquivalent zum IT-Sig, um mit Kritis-Unternehmen in puncto Sicherheit mithalten zu können. Das macht es für viele kleine und mittlere Betriebe schwer, aufgrund fehlender IT-Abteilungen für sich einen entsprechenden Schutz aufzubauen. Während der Konsumgüterkonzern Beiersdorf durch einen Hackerangriff aktuell einen Millionenschaden zu verbuchen hat – und dennoch weiter existiert, kann eine Blockade des Netzwerkes eines KMU schnell zu dessen Insolvenz führen.

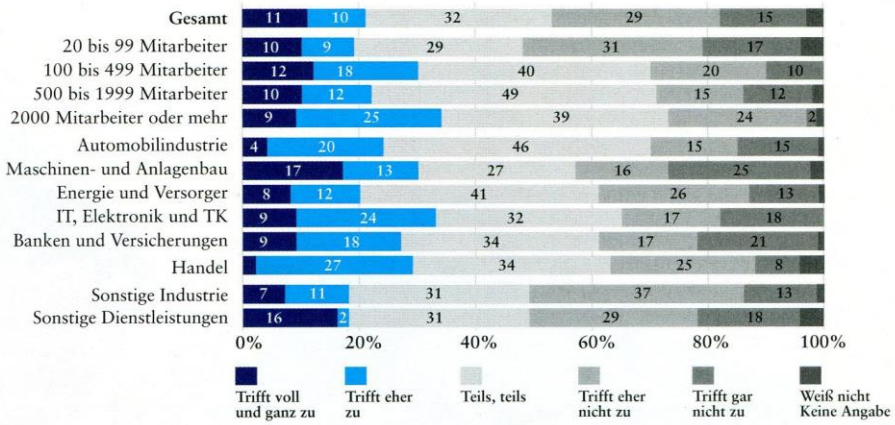
Zwar ist den Unternehmen dieses Dilemma bewusst, doch fühlen sie sich oft überfordert, tun nichts und trauen sich nicht, bei ihrer Digitalisierung voranzuschreiten. So

verzichten überdurchschnittlich viele Maschinen- und Anlagenbauer laut der Studie „IT-Sicherheit im Rahmen der Digitalisierung" der Bundesdruckerei aus dem Jahr 2016 auf Umsatz, weil sie „aus Angst vor Cyberattacken ihre Prozesse, Produkte und Services langsamer digitalisieren". Auf jedes sechste Unternehmen dieser Branche, und damit 17 % trifft diese Aussage „voll und ganz zu", auf 13 % trifft sie „eher zu" und auf weitere 27 % teilweise. Für die Studie hat das Marktforschungsunternehmen Bitkom Research 556 Führungskräfte befragt, die in ihrem Unternehmen für IT-Sicherheit verantwortlich sind.

Auch wenn sich kein Systemangriff ereignet, finden indirekt trotzdem Cyberangriffe statt, denn „egal, ob IT-Sicherheitsbedenken berechtigt, übertrieben oder vorgeschoben sind: Fakt ist, sie haben volkswirtschaftliche Auswirkungen und verzögern die notwendige Digitalisierung der deutschen Wirtschaft", sagt Ulrich Hamann, Vorsitzender der Geschäftsführung der Bundesdruckerei.

Doch wie können sich Unternehmen konkret schützen? An erster Stelle steht der gesunde Menschenverstand. Hier muss es Standard sein, dass Mitarbeiter Firmencomputer nicht privat nutzen, keine E-Mail-Anhänge von unbekannten Absendern öffnen, keine Links in Mails von unbekannten Absendern anklicken, keine unbekannten Websites anfahren, da sowohl Websites als auch auf ihnen befindliche Werbebanner mit Schadsoftware verseucht sein können. Alle Betriebssysteme, Browser, Firewalls und Antischad-Softwareprogramme sollten durch Updates aktuell gehalten werden. Das sind die Basics der IT-Sicherheit.

IT-Sicherheit im Rahmen der Digitalisierung



Zu langsame Digitalisierung aus Furcht vor Cyberangriffen führt zu Umsatzverlusten bei jedem fünften Unternehmen. Das zeigt eine Studie der Bundesdruckerei. Bild: obs/Bundesdruckerei

Schutz mit ISMS oder Beitritt zu UP Kritis

Eine weitere Möglichkeit ist, sich auch als Nicht-Kritis-Unternehmen den Standard des IT-Sicherheitsgesetzes zu eigen zu machen. Ein nächster Schritt könnte die Implementierung eines eigenen ISMS sein – mithilfe externer Dienstleister. Ein weiterer Schritt wäre der Beitritt zu UP Kritis. Das ist eine öffentlich-private Kooperation zwischen Betreibern kritischer Infrastrukturen, dazugehörigen Verbänden und staatlichen Stellen. Sie hat sogenannte Single Points of Contact (SPOC) implementiert, die als Meldestellen und Bindeglieder zwischen Kritis-Unternehmen und dem BSI-Lagezentrum fungieren. Zentrale Aufgabe der SPOC ist die schnelle Informationsweiterleitung und Alarmierung der angeschlossenen Unternehmen und des Lagezentrums über aktuelle IT-Sicherheitslagen. Sie bieten Branchen- und Themenarbeitskreise an und nehmen auch Unternehmen auf, die nicht von der Kritis-Verordnung betroffen sind. Die Vorteile für diese Unternehmen liegen darin, alle Warn- und Lageinformationen zu erhalten und sich unter Umständen den SPOC anzuschließen.

Um gerade Angriffen über Einfallstore in Form von veralteten Betriebssystemen – wie jüngst die Cyberattacken mit der Ransomware Wannacry – vorzubeugen, sollten Unternehmen überlegen, auf ein anderes Betriebssystem umzusteigen. Denn 95 % aller Schadsoftware und damit fast alle alle Cyberangriffe haben es auf Windows abgesehen. Die Cyberkriminellen haben hier leichtes Spiel und nutzen sowohl die Bequemlichkeit als auch die Bedenken der Anwender vor Neuem. Möglich wäre beispielsweise ein Systemwechsel hin zu einem offenen Standard, wie Linux. Linux lässt sich genauso einfach einsetzen wie Windows. Die Oberfläche ist ähnlich, die Einarbeitung dauert nicht lange und die Systempflege ist nicht komplizierter. Außerdem sind die Dateien nicht nur mit Windows kompatibel, sondern lassen sich auch in den Windows-Standard konvertieren. ●

Die Verordnungen im Überblick:

- IT-Sicherheitsgesetz: Mit dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sig) will die Bundesregierung die IT-Systeme und digitalen Infrastrukturen Deutschlands zu den sichersten weltweit machen.
- Ziele: Kritische Infrastrukturen in Deutschland vor Cyberangriffen schützen, die Versorgungssicherheit der Bevölkerung gewährleisten und die Wirtschaft Deutschlands sichern.
- BSI-Kritis V: Die Verordnung des BSI zur Bestimmung kritischer Infrastrukturen regelt, welche Unternehmen aus den relevanten Sektoren unter das IT-Sicherheitsgesetz fallen.

Hertha-Margarethe Kerz
Fachjournalistin in Hamburg