Expertentische 3:
„Safety und Security“
Experte: Michael Hilser, EUPROCONS
Moderation: Michael Starz, ms-procon

Einstiegsfrage an den Experten:
Beim Thema Safety und Security fallen einem spontan Stichworte
wie Edward Snowden oder NSA ein. Ist das nur ein Thema für Geheimdienste und den Bundestag oder gibt es einen Zusammenhang zu Unternehmen im Allgemeinen?
Experten-Antwort:
Die Stichworte Safety und Security liegen näher bei den Unternehmen als viele Unternehmer das wahrhaben wollen. Nehmen wir das Beispiel Plagiate. Viele namhafte Unternehme wie beispielsweise Stihl oder Hansgrohe vernichten regelmäßig Plagiate ihrer eigenen Produkte. Ob Motorsäge, Duschkopf, Kugelschreiber, Parfüm oder Sonnenbrille, es gibt eigentlich nichts, was nicht kopiert wird. Die Innovationskosten trägt der Erfinder, der Nachahmer kassiert aber bei den Gewinnmöglichkeiten mit.
Als zweites Beispiel möchte ich auf den Datenschutz aufmerksam machen. Die unternehmenseigenen Daten sowie Kunden- und Lieferantendaten können in die falschen Hände geraten. Es gibt Vorschriften für den Umgang mit Daten. Ein Datenabfluss ist meist mit einem erheblichen Imageschaden verbunden.

Frage an den Experten:
Welche Bedeutung hat Safety und Security im Kontext mit Unternehmen 4.0 – was ist der Unterschied zum ‚klassischen‘ Unternehmen ohne das 4.0?
Experten-Antwort:
Im Unterschied zum „klassischen“ Unternehmen steigt im Unternehmen 4.0 der Grad der digitalen Vernetzung mit neuen digitalen Schnittstellen. Im Gegensatz zu den analogen Einbruchsspuren fällt ein digitaler Angriff meist erst sehr spät auf. Es wird ja nichts mitgenommen, sondern die Daten werden lediglich kopiert.

Frage an den Experten:
Die beiden Schlagworte lauten Safety und Security – beides wird
üblicherweise mit Sicherheit übersetzt. Ist es nicht dasselbe – und wenn nein, worin besteht der Unterschied?
Experten-Antwort:
Das ist richtig. Die deutsche Sprache macht hier keinen Unterschied. Im Englischen unterscheidet man zwischen Safety und Security.
Safety ist der Schutz vor Gefahren. Klassischerweise gehört der Arbeitsschutz in diese Kategorie, aber auch der Gesundheitsschutz oder etwa die Produktsicherheit. Unter Security versteht gezielte Angriffe von außen. Das kann analog geschehen oder digital. Ein analoger Angriff wäre zum Beispiel ein Einbruch oder ein freundliches Gespräch auf einer Messe mit Mitarbeiterinnen und Mitarbeiter mit dem Ziel, etwas über das entsprechende Unternehmen zu erfahren. Ein digitaler Angriff wäre ein Trojaner, ein Bot Netz oder ein sonstiges Eindringen in ein Unternehmensnetzwerk.

Frage an den Experten:
Das Handelsblatt berichtete vor wenigen Tagen, dass es einen Massenangriff auf Cisco-Router gegeben habe, der über ein Jahr nicht entdeckt wurde und von IT-Sicherheitsfirmen kommentiert wurde mit „Wir haben so etwas noch nie gesehen“. Ist so etwas heutzutage normales Geschäftsrisiko? Wie kann sich ein Unternehmen dagegen wappnen?
Experten-Antwort:
Ein Eindringen in Netzwerke wird häufig sehr spät oder gar nicht entdeckt. Selbst IT-Sicherheitsfirmen werden von solchen Angriffen immer wieder überrascht.

Sehr schwierig sind etwa Zugriffe zu identifizieren, wenn sie von firmeneigenen Mitarbeiterinnen und Mitarbeitern getätigt werden. Dieses Risiko ist nicht zu unterschätzen. Das Bundesamt und die Landesämter für Verfassungsschutz weisen regelmäßig darauf hin, dass ein wesentlicher Teil des Abflusses von Know-how durch unternehmenseigenes Personal geschieht. Aus diesem Grund gehören Personalauswahl und Personalführung unabdingbar zu einem Unternehmenssicherheitskonzept.
Um das Risiko von Angriffen auf digitale Daten zu verringern, bekommt das Informationsmanagement innerhalb des Unternehmens eine ganz neue und zentrale Bedeutung. Die Firmen müssen sich Gedanken darüber machen, welche Daten vorhanden sind, welche Daten wo benötigt und gespeichert werden und wer darauf Zugriff haben darf.

Frage an den Experten:
Im Focus 11.08.2015 lautete eine Titelzeile: „Mittelstand in Angst – wir brauchen mehr Datensicherheit". Berichtet wurde unter anderem, dass nur ein Drittel deutscher Unternehmen gut geschützt wären und pro Jahr ein Schaden von 51 Milliarden Euro entstehen würde. Als einer der zunehmenden Risikofaktoren wurden verlorene und gestohlene mobile Endgeräte wie Smartphones, Tablets oder Laptops genannt, die auf den sieben großen Flughäfen wöchentlich zu Tausenden den Besitzer wechseln würden. Ist das lediglich ein journalistischer Aufreißer oder stellt das tatsächlich eine zunehmende Bedrohung dar?
Experten-Antwort:
Wenn man viel unterwegs ist, dann kann es auch einmal passieren, dass ein Smartphone verlorengeht oder gezielt geklaut wird. Damit muss man rechnen und deshalb ist die Aufmachung durchaus gerechtfertigt und die Zahlen wohl kaum überzogen.
Als Konsequenz muss sich jedes Unternehmen fragen, was darf auf dem Smartphone gespeichert sein oder welche Zugriffe werden über das Smartphone erlaubt. Viele kleine und mittelgroße Unternehmen glauben, sie seien viel zu uninteressant, um angegriffen zu werden. Das ist eine fatale Fehleinschätzung. Für potenzielle Angreifer spielt die Größe des Unternehmens gar keine Rolle. Es geht lediglich darum, ob das Unternehmen ein Produkt oder eine Dienstleistung hat, die zu vermarkten ist. Selbst kleine Unternehmen haben heute eine Internetseite. Über die Suchmaschinen werden diese Firmen schnell gefunden. Diese Arglosigkeit kleiner Unternehmen erhöht die Angreifbarkeit dramatisch.

Frage an den Experten:
Was kann denn passieren, wenn man sich nicht schützt?
Experten-Antwort:
Wenn ein Angriff auf ein Unternehmen erfolgreich war, entsteht zunächst ein Imageschaden. Allein das Ansehen des Unternehmens wieder aufzupolieren, kann teuer werden. Das sehen wir einmal mehr bei der Diskussion um die Vorgänge bei VW. Da werden viele teure Werbemaßnahmen erforderlich werden. Das hat man ja bereits bei den Mitarbeitermotivationsreisen in der Versicherungsbranche gesehen. Die ERGO-Versicherung hat nicht aus reinstem Vergnügen über einen längeren Zeitraum Werbung zur teuersten Werbezeit direkt vor den Hauptnachrichten platziert.
Eine weitere Folge sind Plagiate, also ist die Abwanderung der Kundschaft zum günstigeren Anbieter. Langfristig kann das kein Unternehmen verschmerzen.
Es können aber auch Schadensersatzfälle entstehen, wenn man nicht gerichtsfest nachweisen kann, dass es sich bei einem mangelhaften Plagiat um ein Produkt einer dritten Firma handelt und nicht der eigenen.
Digitale Angriffe können nicht zuletzt zu Produktionsausfällen oder Manipulationen führen.

Frage an den Experten: Was würden Sie also mittelständischen Unternehmen raten, damit sie sich sicher fühlen können?
Experten-Antwort:
Zunächst sollte man sich wissen, dass es keine absolute Sicherheit gibt. Allerdings sollte man sich

darüber im Klaren sein, dass das Überleben des Unternehmens von dessen Wettbewerbsfähigkeit abhängt. Jedes Unternehmen braucht einen gewissen Vorsprung vor den Konkurrenten. Eine Distanz kann man aufrechterhalten, wenn man sich bewusst ist, dass jedes Unternehmen angreifbar ist. Die Unternehmensleitung - und das ist ganz wichtig, dass sich der „Kopf“ des Unternehmens der Gefahren bewusst ist - muss gezielt die Risiken aufdecken und bewerten. Dann sind die geeigneten individuellen Entscheidungen zu treffen und die entsprechenden Maßnahmen umzusetzen. Jedes Unternehmen braucht ein Unternehmenssicherheitskonzept hinter dem die Geschäftsführung auch steht.

Frage an den Experten:
Und was kostet das alles?
Experten-Antwort:
Das kann man nicht pauschal sagen. Am Anfang stehen sicher Gespräche mit der Geschäftsleitung. Hier kann man klären, was ist schon an Schutz vorhanden. Dann sollten alle Mitarbeiterinnen und Mitarbeiter in entsprechenden Schulungen einbezogen werden. Viel Schutz kann schon erreicht werden, wenn man sich bewusst ist, wo man angreifbar ist und sich dementsprechend verhält. Unter dem Strich kann man festhalten, dass in vielen Fällen die Kosten geringer sind, als man sich das zunächst vorstellt. Das Risiko kann oftmals schon mit weniger aufwändigen Maßnahmen deutlich reduzieren.

Frage an den Experten:
Welche Bezugspunkte sehen Sie zur Offensive Mittelstand?
Experten-Antwort:
Die Offensive Mittelstand hat als Grundlage einen ziemlich guten Unternehmenscheck. In meiner Beratung gehe ich gezielt auf die einzelnen Themenfelder ein. Die Erfahrung zeigt, dass gerade erfolgreiche kleine Unternehmen Angreifern oftmals Tür und Tor für potenzielle Wettbewerber öffnen und damit ihre eigene Zukunftssicherung gefährden. Diese Gefahr können sie verringern, wenn sie einige Spielregeln beachten.