www.compliance-berater.de

CB

Compliance Berater

12 / 2018

Betriebs-Berater Compliance

5.12.2018 | 6.Jg
Seiten 437–480

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

CB-VERANSTALTUNGSBERICHT

Roundtable Cybercrime

Cybercrime hat Relevanz für jedes Unternehmen. Denn die zunehmende Digitalisierung bringt viele Vereinfachungen, schafft aber auch neue Einfallstore für Betrüger. Das bekommen jährlich fast 80 Prozent aller deutschen Unternehmen zu spüren. Ein guter Grund für die intensive Diskussion mit Jörg Bielefeld, Partner, BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH, Peter Danil, Bundesamt für Sicherheit in der Informationstechnik (BSI), und Peter Zawilla, Geschäftsführer, FMS Fraud & Compliance Management Services GmbH, beim Roundtable Cybercrime in den Räumlichkeiten der BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH am 22.10.2018 in Frankfurt am Main.

Peter Danil stellte zunächst den Bericht zur Lage der IT-Sicherheit 2018 des BSI vor, das erst wenige Tage zuvor veröffentlicht worden war. „Ich möchte Ihnen auf keinen Fall Angst machen", stieg er angesichts der eher besorgniserregenden Zahlen des Berichts in seinen Vortrag ein und appellierte an die Roundtable-Teilnehmer, „die enormen Chancen der Digitalisierung" zu sehen. Bis zu neun internetfähige Geräte (darunter auch Kühlschränke und Fernsehapparate) werde es pro Person in Deutschland in naher Zukunft geben. „Für die Wirtschaft ergeben sich daraus gewaltige Wertschöpfungspotentiale", sagte Danil. Doch den „sichtbaren Chancen" stünden eben auch „unsichtbare Bedrohungen" entgegen: „Statistisch gesehen werden Sie zu 70 bis 80 Prozent in nächster Zeit Opfer eines Cyberangriffs", sagte Danil und ergänzte: „Wer bisher noch nicht Opfer eines Cyberangriffs war, hat es möglicherweise nur noch nicht bemerkt." Denn durchschnittlich brauche es 243 Tage, um festzustellen, dass man angegriffen wurde. Das ist viel Zeit, in der die Täter z. B. Daten absaugen können. Die Dimension der Cyberkriminalität spiegelt sich auch in den täglich im Durchschnitt rund 390.000 neuen Schadprogrammen wieder. Die Bedrohung durch diese sog. Malware (Trojaner, Viren) wird inzwischen durch einen weiteren Schwachpunkt erhöht: Die Hardware. „Das ist neu", erklärte Danil. Wie bedeutend die Rolle der Hardware ist, haben jüngst die Prozessorschwachstellen Spectre und Meltdown gezeigt: Diese Sicherheitslücken erlauben es Angreifern, sensible Speicherbereiche des Computers auszulesen. Passwörter, E-Mail-Nachrichten oder Chatinhalte können so aus den eigentlich nicht zugänglichen Speicherbereichen fremder Programme und aus dem im Grunde geschützten Speicherbereich des Betriebssystems extrahiert werden.

Jörg Bielefeld riet dazu, den Nutzen von Präventionsmaßnahmen auch im Hinblick auf Haftungsfragen nicht zu unterschätzen.

Das Haupteinfallstor sind dennoch nach wie vor E-Mails, über deren Anhänge 80 Prozent aller Angriffe beginnen. „Das ist eine enorme Zahl mit Blick auf den Faktor Mensch, der damit sehr zentral und entscheidend für Ihren Präventionserfolg ist", verdeutlichte Danil den Roundtable-Teilnehmern die Bedeutung dieser „Schwachstelle". Oft sei daher nicht die Frage nach dem höchsten Sicherheitsstandard entscheidend, sondern das Augenmerk auf den Menschen. Hier seien dann meist die einfachsten Dinge wirksam:

- Bei ungewöhnlichen E-Mail-Anfragen stutzig werden und sich rückversichern, wer dahinter steckt: Chief or Thief?
- Keine gefundenen USB-Sticks in den Rechner stecken. Es gibt „Datenschleusen", durch die man solche USB-Sticks vorher laufen lassen kann.
- Sicherheits-Updates nicht verschieben. Täter werden die Lücke nutzen, sobald sie bekannt ist.
- Dem Passwort-Klau/Phishing über gefakte Webseiten-Oberflächen vorbeugen.

Auf die Frage eines Teilnehmers, inwieweit die Behörden proaktiven Schutz bieten, verwies Danil auf die intensive Präventionsarbeit des BSI: „Unsere Aufgabe ist es, Awareness zu schaffen, aufzuklären und zu sensibilisieren. Unternehmen können sich dazu bei uns mit allen notwendigen Informationen versorgen." Über die Allianz für Cyber-

Peter Danil gab einen Einblick in die Dimensionen von Cyberangriffen.

Peter Zawilla legte besonderes Augenmerk darauf, für den Schadenfall die richtigen Kontakte bereit zu halten.

Sicherheit (www.allianz-fuer-cybersicherheit.de) bietet das BSI der Wirtschaft eine kostenlose Plattform für den Austausch von Informationen und Erfahrungen rund um das Thema Informationssicherheit. Die Initiative zählt derzeit 3.000 teilnehmende Unternehmen.

Danil wies darauf hin, dass nicht nur die Schutz-, sondern auch gute Back-up-Maßnahmen entscheidend seien, um gegen Cyberangriffe bzw. deren Auswirkungen gewappnet zu sein: „Wir können von Virenscannern keinen 100prozentigen Schutz erwarten. Darum sollten wir keinesfalls Back-up-Lösungen vergessen, die bei der Schadensbegrenzung helfen, indem sie Daten sichern, die für die betrieblichen Abläufe notwendig sind. Zawilla riet darüber hinaus dazu, für den Schadenfall auch eine Art Handlungsanweisung bereit zu halten. „Überlegen Sie sich schon präventiv, an wen Sie sich wenden, falls Sie zum Opfer eines Cyberangriffs werden. Bauen Sie sich schon vorher ein gutes Netzwerk auf, um den Schaden dann so gering wie möglich zu halten."

Ein Teilnehmer berichtete daraufhin von schlechten Erfahrungen mit seiner ersten Anlaufstelle, der Polizei, die ihm bei einem Cyberangriff nicht weiterhelfen konnte. Danil schilderte die Ansprüche und Herausforderungen der Polizei im Umgang mit Cybercrime. Die Polizeien vieler Bundesländer haben Kompetenzzentren eingerichtet, die in der Regel bei den Landeskriminalämtern angesiedelt sind. Diese zentralen Ansprechstellen für Cybercrime (ZAC) sind über Hotlines erreichbar. „Und auch wenn Ihre Anzeige bei der Polizei nicht in jedem Fall zur Überführung der Täter führt, können sie davon ausgehen, dass die Polizei darum bemüht ist, jeden weiteren Schaden für Ihr Unternehmen zu minimieren und Sie bestmöglich zu unterstützen. Letztendlich schlägt sich jede Anzeige auch in einem realistischen Abbild der Lage nieder und diese Statistiken liegen zahlreichen, auch politischen Prozessen, zugrunde."

Zawilla riet dazu, dem Thema Cybersicherheit erst noch eine Risikoanalyse vorzuschalten: „Welches Cyberrisiko habe ich überhaupt? Wo sind die Schwachstellen in meinem Unternehmen." Er verwies darauf, dass zielgerichtete und wirksame Präventionsmaßnahmen nur dann implementiert werden können, wenn zuvor die konkrete unternehmensspezifische Risikosituation erhoben worden und transparent ist. Eine derartige Analyse sei zwar aufwendig, aber lohnend. Auch Zawilla betonte darüber hinaus, dass der „Schlüsselfaktor Mitarbeiter" und dessen individuelle Aufmerksamkeit sowie jeweiliges Kontrollbewusstsein maßgeblich für das tatsächliche Schutzniveau eines Unternehmens sind.

Auch die Frage nach den Kosten bewegte die Teilnehmer. Hinzu komme, dass oft schon die Komplexität des Sachverhalts „Cybersicherheit" als so hinderlich empfunden werde, dass die Betroffenen am Ende überhaupt nichts tun. Danil stimmte dem zu und appellierte an die Anwesenden: „Cybersicherheit ist Chefsache!" Es helfe nicht, wenn zwar einige Mitarbeiter im Unternehmen das Thema durchdringen, der Chef aber die notwendigen organisatorischen oder technischen Maßnahmen nicht unterstütze. Bielefeld riet, die Thematik aus Geschäftsleitersicht zu betrachten. Denn die Verantwortlichen in den Unternehmen müssten sich heutzutage durchaus fragen lassen, ob sie bestimmte Angriffe – etwa auch durch CEO-Fraud – nicht hätten kommen sehen und verhindern können. „Sie müssen Ihrem Chef verdeutlichen, dass Prävention ihn enthaften kann. Dann ist er mit Sicherheit auch eher dazu bereit, Geld für Cybersicherheit auszugeben."

Christina Kahlen-Pappas

Fotos: Maria Belz/Sonja Pörtner