QUELLE: VZP (ALLE)

Die Teilnehmer des VZP-Tages ließen sich über Gefahren und Schäden von Cyber-Kriminalität informieren

VZP-Geschäftsführer Horst Ullrich: Unternehmen, die die Gefahren von Cyber-Attacken kennen und sich entsprechend vorbereiten, sind nicht wehrlos

[VERSICHERUNGEN]

CYBER 4.0 – SCHÄDEN IM IT-BEREICH AUFFANGEN

Im Mai informierte die Versicherungsstelle Zellstoff und Papier GmbH (VZP), Köln, im Rahmen ihres diesjährigen VZP-Tages, welche Gefahren und Schäden durch Hackerangriffe, Erpressungssoftware, Datenklau und andere Formen von Cyber-Kriminalität entstehen können.

Immer mehr Maschinen, Rechner und Produktionsbereiche sind online miteinander vernetzt. Diese Entwicklung eröffnet zwar neue Chancen und Geschäftsmöglichkeiten, birgt aber auch Risiken, wenn es um Cyber-Attacken geht. Um für dieses Thema zu sensibilisieren und das Spektrum an möglichen Herausforderungen und Lösungen aufzuzeigen, hatte die VZP als Referenten Michael Bartsch (Zukunftsforum öffentliche Sicherheit), Hendrik F. Löffler (Funk Risk Consulting), Harald Reisinger (RadarServices Smart IT-Security) und Michael Winte (Industriebereich Professional Risks Funk) eingeladen.

Jüngste Cyber-Attacke in 150 Ländern

Internet-User, die bisher glaubten, Cyber-Angriffe würden nur Behörden, Institutionen und internationale Unternehmen treffen, wurden am 12. Mai dieses Jahres von einem internationalen Phänomen überrascht: Das Schadprogramm „WannaCry“ hatte laut Internet-Lexikon „Wikipedia“ vorrangig Systeme geschädigt, „die den seit März 2017 von Microsoft angebotenen Sicherheits-Patch nicht enthalten“. Das Schadprogramm verschlüsselte Benutzerdaten von Computern und forderte die Nutzer auf, einen bestimmten Betrag in der Kryptowährung Bitcoin zu zahlen, damit die Daten wieder zur Verfügung stehen. Außerdem soll „WannaCry“ auch versuchen, weitere Computer zu infizieren und die „Backdoor“-Software „DoublePulsar“ zu installieren, hieß es in Fachmedien.

Die Folgen dieser Cyber-Attacke: Nach Medienberichten waren mehr als 230.000 Computer in 150 Ländern von dem Erpressungstrojaner infiziert worden, darunter auch die Rechner der Deutschen Bahn, was sich vor allem auf die Anzeigentafeln, aber auch manche Fahrkartenautomaten auswirkte.

Risiken in der Papierwirtschaft

Sollten die digitalen Systeme von Unternehmen der Papierwirtschaft im Visier von Kriminellen sein, so kann das für die betroffenen Zellstoff- und Papierhersteller, weiterverarbeitende Betriebe, Druckereien sowie den Handel unangenehme Folgen haben, die nicht nur die Reputation schädigen. Die Branche ist darauf angewiesen, dass sämtliche Produktionsprozesse reibungslos funktionieren und Termine eingehalten werden. Ein Ausfall der Papiermaschine oder Wellpappenanlage, der Verlust von Kundendaten oder andere Schäden wirken sich in der Regel auf die Wertschöpfung aus.

Aus diesem Grund wurde während der Veranstaltung mehr als einmal betont, dass den Maßnahmen, Methoden und technischen Lösungen zur Erhöhung der Sicherheit gegen Cyber-Angriffe (Cyber-Security) Aufmerksamkeit geschenkt werden sollte. Dazu zählt ein internes Risikomanagement ebenso wie die technische Ausstattung, um nur zwei Beispiele zu nennen.

Risikomanagement

Wie sich ein solches Risikomanagement gestalten könnte, erläuterte Hendrik F. Löffler von der Funk Risk Consulting GmbH, Hamburg. Angesichts der zahlreichen Unsicherheitsfaktoren, denen Unternehmen gegenüberstehen (unter anderem steigende Cyber-Risiken durch die wachsende digitale Vernetzung und Automatisierung von Prozessen oder strategische Änderungsrisiken infolge der Ablösung von Geschäftsmodellen durch neue Technologien), empfiehlt der Fachmann einen Stresstest durch Szenario-Simulation. Dabei werden die auf die Firma einwirkenden möglichen Risiken in Bezug zur Unternehmensplanung gesetzt, um die Auswirkungen auf die finanzielle Situation abschätzen zu können. Wenn es um Risikobewältigungsstrategien geht, erarbeitet die Beratungsfirma gemeinsam mit dem Unternehmen ein bedarfsgerechtes Risikotransferkonzept.

Harald Reisinger (RadarServices Smart IT-Security): Jeden Monat registrieren 45 % der Unternehmen ernste Angriffe; der volkswirtschaftliche Schaden beträgt 50 Mrd. Euro im Jahr

Michael Winte (Industriebereich Professional Risks Funk, Hamburg) stellte „CyberSecure", ein exklusives, modular aufgebautes Versicherungsprodukt, vor

Jeden Monat registrieren 45 % der Unternehmen ernste Angriffe, erfuhren die Anwesenden von Harald Reisinger (RadarServices Smart IT-Security, Wien), der auch den volkswirtschaftlichen Schaden beziffern konnte: 50 Mrd. Euro im Jahr.

Cyber-Angriffe erkennen

Weil die Komplexität der IT durch vertikale und horizontale Integration in die Wertschöpfungsprozesse erheblich zunimmt (was die Angreifbarkeit erhöht) und jedes System praktisch zu jeder Zeit und von jedem Ort über das Internet zugänglich ist, gibt es seiner Ansicht nach keinen 100 %-igen Schutz vor Cyber-Angriffen. Er rät deshalb zu einem strukturierten Vorgehen. Da es nicht möglich ist, ein Eindringen in das System — trotz Firewalls, Antiviren-Programmen, Zertifikaten und Verschlüsselung — zu verhindern, schlägt er die Installation einer Erkennungstechnologie vor, die zeitnah IT-Sicherheitsvorfälle und -risiken ermittelt. Darüber hinaus empfiehlt der Fachmann, der Geschäftsführer einer Firma für „Managed Cyber Security Detection" ist, die Anwendung von Risikomanagementprozessen und die Absicherung des restlichen Risikos, beispielsweise durch entsprechende Versicherungen. Damit die Daten auch im Fall der Fälle nicht verloren sind, rät er, regelmäßig Backups anzufertigen und die Daten offline zu speichern.

Möglichkeiten des Risiko-Transfers

Dass nicht nur Schadprogramme wie „WannaCry" die Unternehmens-IT lahmlegen können, erläuterte Michael Winte (Industriebereich Professional Risks Funk, Hamburg). Höhere Gewalt, technisches Versagen, Sabotage durch Dritte oder die eigenen Mitarbeiter, aber auch Konfigurations- und Bedienfehler im Unternehmen können erhebliche Schäden anrichten. Seinen Angaben zufolge haben die Versicherungen auf diese Situation reagiert und bieten entsprechenden Versicherungsschutz an. Allerdings würden Leistungselemente wie Drittansprüche (Abwehr, Befriedigung, Vertragsstrafen und Bußgelder), Dienstleistungs- und Beratungskosten (IT-Forensik, Daten- und Systemwiederherstellung, Rechts-, Krisen- und PR-Beratung) sowie der Ausgleich für Ertragsausfall, Entschädigung für Wertminderung, Ersatzbeschaffung von Fertigungserzeugnissen und der Ausgleich von Vermögenseinbußen durch Cyber-Betrug nur durch umfangreiche Cyber-Policen gedeckt werden können.

Zusammen mit der Versicherungsstelle Zellstoff und Papier GmbH hat die Funk-Gruppe, die Beratung zum Risk-Management anbietet und einer der größten eigenständigen Versicherungsmakler in Deutschland ist, mit „CyberSecure" ein exklusives, modular aufgebautes Versicherungsprodukt entwickelt. Laut Winte werden Datenschutz- und Vertraulichkeitsverletzungen und deren Folgen ebenso abgesichert wie Schäden aus der Nichtverfügbarkeit der IT-Systeme. Dabei erstreckt sich der Versicherungsschutz auch auf nicht zielgerichtete Cyber-Angriffe; dies bedeutet, dass Hacker Viren in Umlauf bringen und hoffen, dass diese irgendwo andocken. Darüber hinaus bietet „CyberSecure" auch Schutz für Schäden aufgrund technischer Probleme, Fehlbedienung und behördlicher Verfügungen. Mitversichert wird auch Mitarbeiterkriminalität unterhalb der Repräsentantenebene sowohl bei Dritt- als auch bei Eigenschäden. Als versicherte IT-Systeme gelten den Angaben zufolge auch Netzleitsysteme für die Überwachung, Steuerung und Optimierung von Versorgungseinrichtungen und Industrieanlagen (SCADA-Systeme) oder andere industrielle Automationssysteme sowie Cloud-Services.

Als besonderen Vorteil dieser Lösung betonte der Referent auch die Beweislastumkehr des Versicherungsfalls: Weil nicht immer eindeutig festzustellen sei, wer für den Schaden verantwortlich ist, muss der Versicherer nachweisen, dass kein Versicherungsfall vorliegt.

Wie Michael Winte hervorhob, ist vor der Konzeption des individuellen Versicherungsschutzes eine Bedarfs- und Risikoanalyse erforderlich, um die möglichen Risiken für das Unternehmen aufzuzeigen und Risikovermeidungs- und —steuerungsmaßnahmen sowie Notfallpläne zu erarbeiten. Darauf aufbauend werde der Versicherungsschutz an die Risikosituation des jeweiligen Unternehmens angepasst.

VZP-Geschäftsführer Horst Ullrich resümiert am Ende der Veranstaltung: „Der Tag hat deutlich gemacht, dass die Gefahren durch Cyber-Attacken für die Unternehmen der Papierwirtschaft und ihre Partner real sind. Allerdings sind Unternehmen, die die Gefahren kennen und sich entsprechend vorbereiten, nicht wehrlos." | BW