Die fünften Stuttgarter Compliance Gespräche von Stuttgarter Zeitung und Stutttgarter Nachrichten fanden erneut großen Zuspruch. Foto: Nico Bosch/

Cybersicherheit – das geht alle an

Fünfte Compliance Gespräche von Stuttgarter Zeitung und Stuttgarter Nachrichten – Vorfälle durch Schad-Software nehmen zu – Beispiele aus Unternehmen machen die Notwendigkeit der Vorsorge deutlich.

Von Petra Mostbacher-Dix

Cyber-Verbrechen und -Sicherheit in moderner Informationstechnik und elektronischen Infrastrukturen: Was etwas sperrig klingt, ist doch ein Thema, das jeden von uns tagtäglich betreffen kann. Grund genug, es bei den fünften Compliance Gesprächen von Stuttgarter Zeitung und Stuttgarter Nachrichten im Look21 erneut intensiv zu beleuchten.

„Wir sprechen nicht mehr vom ob, sondern vom wann. Ihr Unternehmen wird betroffen sein“, so eindeutig und klar beschrieb Lars Widany in seinem Impulsvortrag, warum Cyber-Kriminalität für jede Firma, unabhängig von der Größe, ein Thema ist. Widany ist als Business Development Manager Cyber verantwortlich für die vertriebliche Steuerung des Cyber-Geschäfts beim Risikomanagement-, Versicherungsmakler- und Beratungsunternehmen Willis Towers Watson (WTW). Er bringt viel Expertise im Bereich der Cyber-Risikobewertung und der Platzierung von komplexen Cyber-Programmen mit.

Die Schadenssumme für die deutsche Wirtschaft durch Cyberkriminalität erreichte 2024 einen Rekordwert von 266,6 Milliarden Euro, wobei allein 13,4 Milliarden Euro auf Erpressung mit gestohlenen oder mit verschlüsselten Daten entfielen.

Wie er erläuterte, liege die Wachstumsrate der jährlich weltweit erzeugten Datenmenge binnen der vergangenen fünf Jahre bei 4,46 Prozent. Laut Bitkom, dem Branchenverband der deutschen Informations- und Telekommunikationsbranche, sahen 65 Prozent der Unternehmen im Vorjahr ihre geschäftliche Existenz durch Cyberangriffe bedroht. Die Schadenssumme für die deutsche Wirtschaft durch Cyberkriminalität erreichte demnach einen Rekordwert von 266,6 Milliarden Euro, wobei allein 13,4 Milliarden Euro auf Erpressung mit gestohlenen oder mit verschlüsselten Daten entfielen.

Es gelte, Sicherheitsniveaus zu optimieren, Risikomanagementprozesse zu etablieren, Verbraucher, inländische und innereuropäische Wirtschaft zu schützen, so Widany. In der Europäischen Union (EU) wird mit Verordnungen und Richtlinien auf die wachsende Gefährdung reagiert, etwa mit dem Cyber Resilience Act (CRA). Der CRA zielt darauf ab, die Cybersicherheit von Produkten mit digitalen Elementen und Funktionen in der EU zu verbessern. Er legt verbindliche Sicherheitsstandards für alle in der EU hergestellten, importierten oder vertriebenen Hardware- und Softwareprodukte fest. Oder der NIS-2-Richtlinie. Mit ihr wird ein einheitlicher Rechtsrahmen für die Aufrechterhaltung der Cybersicherheit in 18 kritischen Sektoren in der EU geschaffen.

Laut Directors’ and Officers’ Survey Report 2024, einer großen Befragung von WTW in mehr als 50 Ländern, nehmen Manager in Deutschland Cyber-Risiken als bedeutendstes Haftungsrisiko wahr, so Widany. Und er kann diese Einschätzung mit drastischen Beispielen auch deutlich machen. Bei einem deutschen Unternehmen, Weltmarktführer in einem chemischen Spezialsegment mit rund 1600 Beschäftigten und einem damaligen Jahresumsatz von einer Milliarde Euro, sei von einem Tag auf den anderen alles ausgefallen, nicht einmal mehr die Kaffeemaschine habe funktioniert. „Ein Mitarbeiter klickte freitags auf einen Mailanhang, am kommenden Montag waren alle Systeme und Datenbanken zweifach verschlüsselt, das geforderte Lösegeld zur Entschlüsselung war eine siebenstellige Summe“, sagte Widany.

Produktion, Lager, Logistik und Finanzwesen seien beeinträchtigt gewesen, es drohten Lieferverzugsfolgen, die gesamte technische Struktur habe neu aufgebaut werden müssen. Glück im Unglück: Die Produktion mit älteren Maschinen war lediglich im geringen Umfang miteinander vernetzt. „Wir mussten 68 länderspezifische Datenschutzregelungen prüfen“, schilderte der Risikomanagement-Experte. Auch Szenarien wie eine mögliche Insolvenz, drohender Personalabbau sowie eine 24/7-Mehrarbeit der IT-Abteilung seien im Raum gestanden.

Dennoch sei alles gut ausgegangen. Jahresumsatz inzwischen? Drei Milliarden Euro. „Das Lösegeld wurde auf einen für das Unternehmen leistbaren sechsstelligen Betrag heruntergehandelt, zahlbar in Bitcoin“, antwortete Widany auf eine entsprechende Publikumsfrage. Denn derlei sei längst ein Geschäftsmodell: Die Erpresserfirmen hätten oft hunderte Beschäftigte, säßen meist in Russland, auch in Asien. „In Russland ist Cyber-Crime nicht strafbar, außer gegen russische Firmen.“ Die Kidnapper leiten sie da durch, ein toller Service, den sollten manche Dienstleistungsunternehmen haben.“

Widanys Ausführungen machten eines ganz deutlich: Die IT-Sicherheitslage in Deutschland ist besorgniserregend, wie auch der aktuelle Bericht des Bundesamtes für Sicherheit und Informationstechnik dokumentierte. Klar ist: Unternehmen stehen nicht nur vor wachsenden technischen Herausforderungen, sondern auch vor steigenden rechtlichen Anforderungen, da die Geschäftsführer zunehmend persönlich in die Pflicht genommen werden.

Aber wie kann Abhilfe geschaffen werden? Das war Thema der folgenden Diskussion, die Rechtsanwalt Dr. Jürgen Bürkle moderierte (Partner bei BRP Renaud). Auf dem Podium saßen Dr. Thomas Weimann, Fachanwalt für Informationstechnologierecht (ebenfalls BRP Renaud), Dr. Markus Klinger, Informationstechnologierechtler bei Heuking sowie Dr. Clemens Birkert, bei Oppenländer Rechtsanwälte spezialisiert auf Datenschutz- und IT-Recht. Lars Widany komplettierte das Podium.

Unternehmen müssten mehr tun für die „Chefsache Cybersicherheit“, vom Netzwerk bis zur Versicherung, da waren sich alle Fachleute einig. Größtes Risiko? Das ist der Faktor Mensch. Den Phishing-Mails und sogenannte Malware kämen dank KI täuschend echt daher. Wichtig sei, auch in digitalen Zeiten einen Notfallplan ausgedruckt bereit zu haben. Auch Mitarbeiter-Schulungen, Trockenübungen des Ernstfalls seien geboten. Es könnte auch mal ein „White-Hat-Hacker“, der Schwachstellen austestet, eingesetzt werden. Als solcher wird ein Angreifer bezeichnet, der sich in Systeme hackt, aber keinen Schaden anrichtet, sondern ganz im Gegenteil im Interesse des Angegriffenen handelt.

> Unternehmen müssen mehr tun für die „Chefsache Cybersicherheit“, vom Netzwerk bis zur Versicherung. Das größte Risiko stellt der Faktor Mensch dar.

Auch Stand-alone-Rechner ohne Schnittstelle zum System können eine gewissen Handlungsfähigkeit im Notfall gewährleisten. „Netzstecker ziehen, aber nicht Stromstecker! Und das Landeskriminalamt einschalten“, unterstrich Widany die Ausführungen aller. Auch das: „Bei Cybersicherheit geht es ebenso ums Geld, und um das Budget für die Unternehmens-IT.“

Ein spannender und lehrreicher Abend mit einer Problematik, die nach Meinung vieler Besucherinnen und Besucher die Wirtschaft – und jeden einzelnen – noch länger beschäftigen wird.

Compliance Gespräche STUTTGART

Lars Widany (Willis Towers Watson) als Keynote-Speaker (Foto oben) gab einen detaillierten Einblick in die Themen Cyber-Sicherheit und Cyber-Kriminalität. In der von Dr. Jürgen Bürkle (im rechten Foto ganz links) moderierten Podiumsdiskussion gaben Dr. Markus Klinger (Heuking), Dr. Clemens Birkert (Oppenländer Rechtsanwälte), Dr. Thomas Weimann (BRP Renaud) und Lars Widany Einblicke in die Praxis. Fotos: Bosch/Pfeil