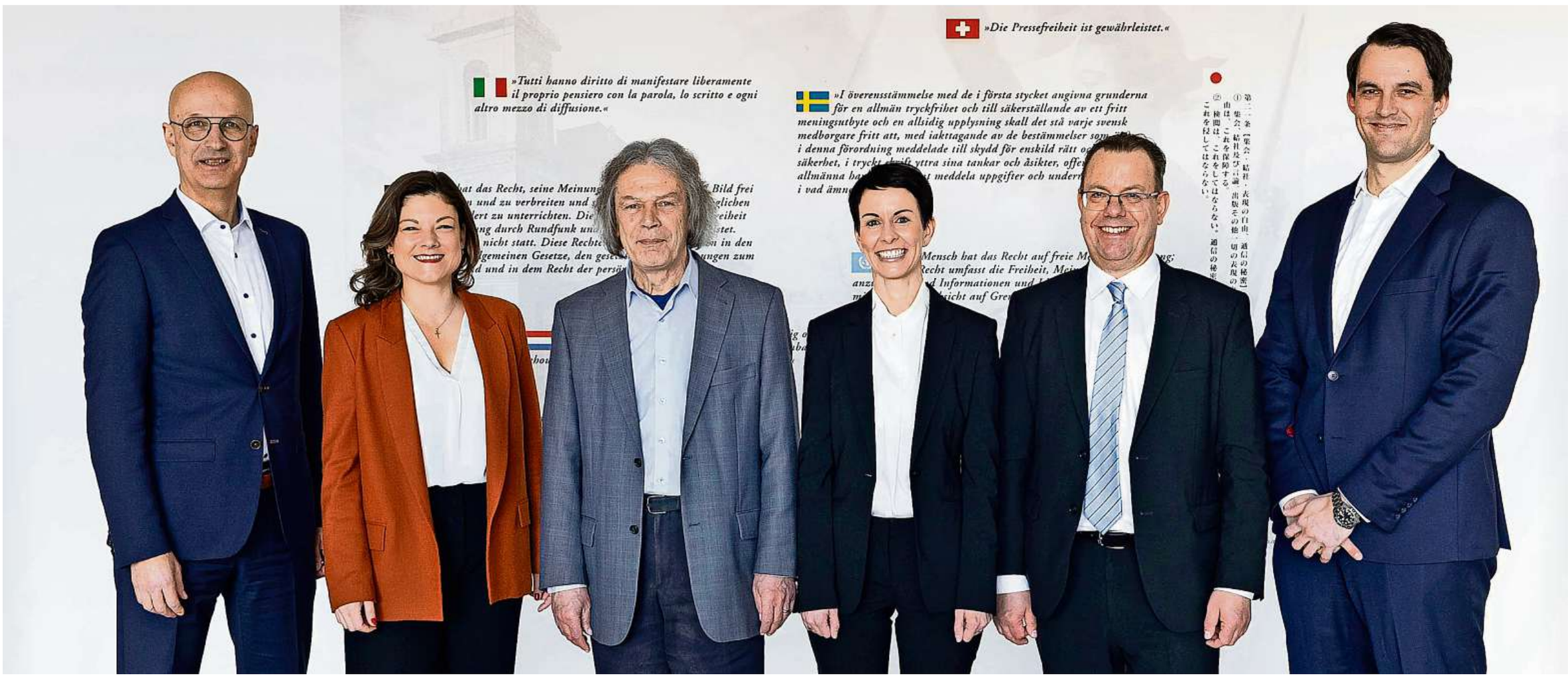

Expertenrunde im Pressehaus Stuttgart zum Thema Cyberkriminalität (v. l. n. r.): Moderator Heimo Fischer, Sonja Fingerle, Dr. Jürgen Bürkle, Antje Münch, Dr. Markus Klinger und Dr. Clemens Birkert Foto: Lichtgut/Leif Piechowski

Cybersicherheit geht jeden etwas an

Die Bedrohung durch Cyberkriminalität nimmt ständig zu. Viele betroffenen Unternehmen reagieren zu spät. Im Pressehaus Stuttgart diskutierten jetzt Experten, wie die Gefahren aus dem Internet eingedämmt werden könnten und wo mögliche rechtliche Risiken bestehen.

Von Ingo Dalcolmo

Cyberkriminalität zählt zu den größten Herausforderungen für Unternehmen, gerade auch für den Mittelstand. Beim diesjährigen Round Table im Vorfeld der 5. Stuttgarter Compliance-Gespräche von Stuttgarter Zeitung und Stuttgarter Nachrichten tauschten führende Experten im Pressehaus Stuttgart ihre Ansichten über Risiken, regulatorische Anforderungen und Strategien zur Cybersicherheit aus. Ihre Einschätzung: das Thema wird immer komplexer und erfordert die Bereitschaft der Unternehmen zum schnellen Handeln.

Eine wachsende Bedrohungslage

Längst treffen Cyberangriffe nicht nur Großunternehmen, sondern auch kleine Mittelständler. Haben viele Unternehmen noch gar nicht begriffen, dass auch für sie die Gefahr eines Angriffes real sei, leitet Moderator Heimo Fischer die Fragerunde ein? Obwohl die statistischen Angaben über Cyberangriffe variiere, bleibe die Gefahr nach wie vor konstant hoch, steigt Dr. Jürgen Bürkle von BRP Renaud in die Diskussion ein. Zwar böten neue Technologien wie Künstliche Intelligenz den Unternehmen Schutz, aber gleichzeitig entstünden neue Angriffsmöglichkeiten. Zudem beruhten viele Sicherheitslücken auf Softwareschwachstellen, ergänzt Antje Münch von Heuking. Die Schäden, die durch derartige Cyberangriffe den Unternehmen entstünden, gingen nicht selten in die Millionen. Zumal die kriminellen Angreifer über immer ausgefeiltere Techniken verfügten.

Die Cyberkriminalität haben mittlerweile zu einem Wettrüsten zwischen den Angreifern einerseits und den Unternehmen andererseits geführt, beobachtet Dr. Markus Klinger von Heuking. Viele Unternehmen würden allerdings bei der Schadensabwehr hinterherhinken. Besonders besorgniserregend seien dabei die unterschiedlichen Angriffsszenarien, angefangen von IT-Diebstahl bis hin zur Desinformation. „Im schlimmsten Fall können Unternehmen nicht mehr agieren, was zu erheblichen wirtschaftlichen Folgen bis hin zur Insolvenz führen kann“, weiß Dr. Clemens Birkert von Oppenländer Rechtsanwälte.

Regulatorische Herausforderungen und Unsicherheiten

Ein weiteres Problem: Die rechtlichen Anforderungen an die Unternehmen in puncto Cybersicherheit nehmen überproportional zu. Zwar würden diese Vorschriften auch die Cyberresilienz fördern, anderseits aber auch Haftungsrisiken erhöhen, wirft Sonja Fingerle von BRP Renaud ein. Deshalb müssten Unternehmen immer umfassender vorsorgen um dabei die wachsende Komplexität der Regularien berücksichtigen. zu können.

Auf der anderen Seite seien viele Unternehmen unsicher, ob sie von bestimmten Vorschriften überhaupt betroffen sind, stellt Dr. Markus Klinger immer wieder fest. Vor allem die langen Übergangsfristen und branchenspezifischen Regularien schafften aktuell viele Unklarheiten. „Besonders kleine und mittelständische Unternehmen kämpfen hier oft damit, die notwendigen Sicherheitsstandards überhaupt zu erfüllen.“

Mitarbeiter als Schlüsselfaktor

„Beschäftigte sind das schwächste Glied in der Sicherheitskette“, sagt Dr. Clemens Birkert. Denn sogenannte Phishingmails würden immer professioneller werden. Entscheidend sei hierbei, wie Unternehmen und ihre Mitarbeiter darauf reagieren. Angst sei hier der falsche Ratgeber.

Dr. Markus Klinger hebt hervor, dass eine positive Fehlerkultur essenziell ist: „Mitarbeiter müssen sensibilisiert werden und wissen, dass sie sofort handeln und Vorfälle melden müssen, damit der Notfallplan anlaufen kann.“ Dazu seien Schulungen und klare Kommunikationswege wichtig. Sich als Unternehmen nicht auf den Notfall vorzubereiten, könne fatale Folgen haben.

Notfallpläne: Ein Muss für jedes Unternehmen

Doch was ist im Fall eines erkannten Cyberangriffs das Wichtigste? Anja Münch: „Das Unternehmen muss zunächst vom Netz genommen werden, um eine Ausbreitung zu verhindern. Dann sollte ein Krisenstab die nächsten Schritte koordinieren.“ Dazu gehörten auch die Informationspflichten gegenüber Kunden, Lieferanten sowie die Einhaltung der gesetzlichen Meldepflichten.

„Notfallpläne müssen aber regelmäßig geübt werden“, sagt Dr. Clemens Birkert. Und: „Ein Plan, der nur digital abgelegt ist, kann im Ernstfall unbrauchbar sein. Es braucht eine analoge Back-up-Infrastruktur und klare Handlungsanweisungen für den Ernstfall.

Umgang mit Erpressungsforderungen

Wird das Unternehmen von Cyberkriminellen erpresst, ist guter Rat teuer. Oder? Der Umgang mit Erpressungsforderungen sei heikel, sind sich Dr. Jürgen Bürkle und Sonja Fingerle einig. Hier gebe es keine universelle Antwort. Es hänge immer vom Einzelfall ab. Wichtig sei aber auch hier, solche Szenarien im Notfallplan zu bedenken. Kein Unternehmen sei heute gegen Cyberangriffe sicher, so der Tenor der Runde im Pressehaus. Auch diejenigen Unternehmen nicht, die schon einmal von einem Cyberangriff betroffenen waren. Antje Münch warnt vor der trügerischen Ruhe: „Je weiter ein Angriff zurückliegt, desto nachsichtiger wird man.“ Deshalb sei ein kontinuierlicher Verbesserungsprozess notwendig, um das Sicherheitsniveau langfristig zu halten und immer wieder anzupassen.

Cybersicherheit als Daueraufgabe

Die Diskussion machte deutlich, dass Cybersicherheit keine einmalige Aufgabe ist. Unternehmen müssen in technische und organisatorische Maßnahmen investieren. Der Mensch bleibt das wichtigste Element. Sensibilisierung, Schulung und eine gelebte Fehlerkultur können den Unterschied ausmachen. Auch die rechtliche Dimension darf nicht unterschätzt werden.

Unternehmen sollten proaktiv handeln, um Haftungsrisiken zu minimieren und im Ernstfall handlungsfähig zu bleiben. Es darf keine Zeit verloren werden – Cybersicherheit beginnt heute und das Thema wird sicherlich auch bei den nächsten Compliance-Round-Tables im Pressehaus Stuttgart für Gesprächsstoff sorgen.

COMPLIANCE-GESPRÄCHE IM MÄRZ

Cyberabwehr ist mehr als Technik – Haftungsrisiken vor und nach einem Angriff
Unternehmen sind erheblichen Cyberrisiken ausgesetzt. Verantwortliche Unternehmer müssen sich entsprechend vorbereiten. Dabei geht es nicht nur um technische Fragen, sondern auch um rechtliche Verpflichtungen. Wie verhält man sich richtig, um den bei einem Angriff eingetretenen unmittelbaren Schaden nicht zu vergrößern oder sich persönlich angreifbar zu machen? Darum geht es bei den 5. Stuttgarter Compliance Gesprächen am 25. März 2025 ab 18 Uhr im Look 21 in Stuttgart. Die Teilnahme ist kostenfrei. Anmeldung unter https://produkte.stuttgarter-zeitung.de/compliance2025/ oder über den QR-Code unten.

Round Table zum Thema Cybersicherheit im Pressehaus Stuttgart mit renommierten Experten aus Stuttgart. Fotos: Lichtgut/Leif Piechowski