Die Compliance-Experten beim Round Table im Pressehaus Stuttgart (v.l.n.r.:) Antje Münch, Dr. Clemens Birkert, Dr. Christoph Wolf, Sonja Fingerle, Dr. Thomas Weimann und Dr. Markus Klinger.
Foto: Lichtgut/Leif Piechowski

Was tun, wenn Hacker zugeschlagen haben?

Die Digitalisierung bietet Unternehmen sowohl Chancen als auch Risiken. Beim diesjährigen Compliance-Round -Table diskutierten Fachanwälte von renommierten Kanzleien die Herausforderungen im Pressehaus in Stuttgart.

Von Ingo Dalcomo

Die Zahlen des BSI zur IT-Sicherheitslage sind beängstigend", sagt Dr. Clemens Birkert von Oppenländer Rechtsanwälte. Früher waren es Hobbyhacker, heute hat sich die organisierte Kriminalität diesem Thema zugewandt. „Es herrscht Alarmstufe rot", warnt der Rechtsanwalt. Viele Unternehmen merken erst viel zu spät, dass sie Opfer eines Cyberangriffs geworden sind. Dr. Christoph Wolf aus derselben Kanzlei erklärt, dass die Angriffe größtenteils über öffentliche Systeme erfolgen, wie etwa die Unternehmenswebsite oder Online-Formulare zum Datenaustausch. Hat die Corona-Pandemie diese Entwicklung verstärkt, fragt Moderatorin Bianca Menzel?

Für Antje Münch von Heuking Kühn Lüer Wojtek ist die Antwort eindeutig: „Ja." Die Pandemie habe die Digitalisierung in einem Tempo vorangetrieben, bei dem die IT-Sicherheit nicht an erster Stelle stand. Die zunehmende Verbreitung von Homeoffice hat den Cyberkriminellen zusätzliche Angriffsmöglichkeiten eröffnet. „Der Klassiker unter den Angriffsflächen sind nach wie vor die Mitarbeiter", ergänzt Dr. Markus Klinger von derselben Kanzlei. Der sorglose Umgang mit E-Mails sei oft dafür verantwortlich, dass Unternehmen gehackt und erpresst werden. „Wir brauchen in den Unternehmen mehr Prävention", fordert Klinger.

Viele Unternehmen warten viel zu lange, ehe sie Hilfe holen

Sind Bürokratie und Behördenvorschriften schuld an der Zunahme der Cyberkriminalität? Weder Dr. Thomas Weimann von BRP Renaud noch seine Kollegin Sonja Fingerle glauben das. „Die Unternehmen warten in den meisten Fällen viel zu lange, bis sie einen Cyberangriff den Behörden melden.", sagt Fingerle. Das sei ein großer Fehler, denn Schnelligkeit sei entscheidend.

„Der Mensch ist nach wie vor das schwächste Glied in der Kette", sagt Clemens Birkert. Jeder, der mit Daten zu tun hat, muss geschult werden. Das betrifft nicht nur die Mitarbeiter, sondern auch die Geschäftsführung. „An der Spitze fehlt oft noch das Bewusstsein für das Thema IT-Sicherheit", stellt der Rechtsanwalt fest. Oft sind es einfache Angriffe, die Unternehmen schaden, ergänzt Thomas Weimann und nennt Beispiele wie nicht aktualisierte Serversoftware, unsichere Administrator-Passwörter oder einfache Passwörter wie „12345". „Man muss im Unternehmen erwarten können, dass Passwörter schwer sind". Das Problem aus Sicht der Rechtsexperten: Cybersicherheit kostet nicht nur Geld – sondern mindert auch den Komfort.

Sonja Fingerle empfiehlt den Unternehmen, das Thema zur Chefsache zu machen. Viele Lecks entstünden tatsächlich intern. Oft haben zu viele Menschen Zugriff auf zu viele Daten. Neben Präventivmaßnahmen empfiehlt die Rechtsanwältin zusätzlich den Abschluss einer Cyberversicherung, insbesondere im Zusammenhang mit Lösegeldforderungen. Markus Klinger unterstützt diese Empfehlung, da Versicherungen die Unternehmen dazu verpflichten, sich besser gegen Cyberangriffe zu schützen. Ein Cyberangriff ist kein gewöhnlicher Vorfall, sondern betreffe das Herz des Unternehmens.

Die drei Phasen nach einem Cyberangriff

Clemens Birkert teilt das Szenario nach einem Cyberangriff in drei Phasen ein: Analyse, Übergangsbetrieb und Bereinigung. „Die erste Phase ist die schwierigste." Es ist von Vorteil, wenn das Unternehmen bereits interne Prozesse hat, die festlegen, was zu tun ist, wenn ein Mitarbeiter versehentlich auf eine Phishing-E-Mail klickt. Datenforensiker können helfen, zudem Licht ins Dunkel des Angriffs zu bringen.

Oberstes Ziel muss die Prävention sein

Unternehmen, die von einem Cyberangriff betroffen sind, müssen dies innerhalb von 72 Stunden melden. „Das ist ein sehr kurzes Zeitfenster. Aber in diesen drei Tagen kann man viel tun", sagt Christoph Wolf. Das Ziel ist jedoch die Prävention, betont Antje Münch. Dazu gehört auch ein analoger Notfallplan mit wichtigen Telefonnummern. Es ist wichtig, einen Dienstleister zu haben, der das Unternehmen kennt und weiß, wo mögliche Angriffspunkte und IT-Probleme liegen könnten.

Markus Klinger stimmt dem zu. In solchen Situationen ist die Kommunikation wichtig. Oft sind auch Telefon und E-Mail von dem Angriff betroffen. Er empfiehlt, zumindest einen Computer außerhalb des Unternehmensnetzwerks vollständig unabhängig zu halten und zu überlegen, wie telefoniert werden kann, wenn das interne Netzwerk blockiert ist.

Kann Künstliche Intelligenz (KI) helfen, fragt Bianca Menzel? Ob KI trainiert werden darf, Abwehrmechanismen gegen Cyberkriminalität zu entwickeln, ist ein heikles Thema, sagt Clemens Birkert. Bisher gibt es dafür keine rechtliche Grundlage. Für Christoph Wolf ist KI jedoch auch eine Chance, Muster in großen Datenmengen schnell zu erkennen. Antje Münch sieht die Gefahr, dass auch Hacker diese Technologie nutzen.

Zudem kann KI zum Risiko für Unternehmen werden, da die aktuellen Systeme noch sehr intransparent sind. Andererseits können viele Arbeiten nicht mehr manuell erledigt werden, sagt Markus Klinger. Für Sonja Fingerle wird Cybersicherheit in Zukunft ohne Künstliche Intelligenz nicht mehr möglich sein und eine wichtige Rolle spielen.

STUTTGARTER COMPLIANCE GESPRÄCHE

Bei den diesjährigen Stuttgarter Compliance Gesprächen geht es am Dienstag, 24. Oktober 2023 ab 18 Uhr im Look 21 um „Cybersecurity im Zeitalter von Künstlicher Intelligenz und die Compliance-Herausforderungen für Unternehmen". Anmeldung: **stuttgarter-zeitung.de/compliance 2023**

Im Pressehaus Stuttgart diskutierten die Compliance-Experten die Auswirkungen von Cyberangriffen auf Unternehmen und welche Folgen sich daraus ergeben können.
Fotos: Lichtgut/Leif Piechowski