Corona treibt die Angst vor Cyberangriffen im Mittelstand

W&W Standort in Ludwigsburg © Wüstenrot & Württembergische AG

Videokonferenzen, Daten in der Cloud, Onlineshops – mit Ausbruch der Corona-Krise haben viele Unternehmen im Schnellverfahren auf digital umgestellt. Für Cyberkriminelle bieten sich dadurch neue Einfallstore. Entsprechend groß ist die Angst vor Internetkriminalität, insbesondere bei kleinen und mittleren Unternehmen. Hierzu hat die Württembergische Versicherung AG 200 Entscheiderinnen und Entscheider im deutschen Mittelstand befragt: Über 70 Prozent von ihnen befürchten, in den kommenden Monaten Opfer eines Hackerangriffs zu werden.

Neue technologische Entwicklungen, hohe Homeoffice-Quoten und Videostreaming bergen sowohl im Privatbereich als auch in Unternehmen neue Gefahren. Mittelständler sind bekannt für ihr Spezialwissen und großes Know-how. Dass sie zudem oft nicht so gut vor Cyberrisiken geschützt sind wie große Konzerne, macht sie zu attraktiven Zielen für Hacker: Viele Unternehmen haben in der Corona-Pandemie von einem Tag auf den anderen ganze Abteilungen ins Homeoffice geschickt. Häufig ist die IT dafür nicht ausreichend abgesichert, was sich Kriminelle zunutze machen. Dabei können selbst kleine Angriffe Unternehmen massiv schaden: Neben hohen Kosten für die IT-Forensik, Datenwiederherstellung oder Betriebsunterbrechung stehen auch die Reputation sowie das Vertrauen von Kundinnen und Kunden auf dem Spiel. Nach den Ergebnissen der Erhebung durch die Württembergische werden die Risiken von Cyberkriminalität durchaus gesehen: Knapp die Hälfte der Befragten macht sich Sorgen vor Angriffen in den kommenden Monaten; weitere 25 Prozent sind sogar sehr besorgt.

Angriffe erfolgen meist über E-Mail und WLAN

55 Prozent der Befragten gaben an, dass ihr Unternehmen bereits Opfer eines Hackerangriffs geworden ist: 17 Prozent hat es seit Beginn der Pandemie und 38 Prozent schon vor der Corona-

Krise getroffen. Am häufigsten spekulieren Kriminelle darauf, dass Mitarbeiterinnen und Mitarbeiter der Betriebe unaufmerksam sind: 40 Prozent der befragten Mittelständler wurden per E-Mail angegriffen, bei 37 Prozent gab es eine Cyberattacke über eine WLAN-Verbindung, und bei 34 Prozent der Befragten haben Hacker das Firmennetzwerk bedroht. Auch das Ausspähen sensibler Daten wie Passwörter oder Kreditkartennummern, das sogenannte Phishing, kommt häufig vor.

VPN-Verschlüsselung auf Platz 1 der Sicherheitsmaßnahmen

In 74 Prozent der befragten mittelständischen Unternehmen wurden seit Beginn der Pandemie zusätzliche Sicherheitsvorkehrungen getroffen. In den meisten Fällen sind hierfür die VPN-Verschlüsselungstechnik verbessert (60 Prozent) und ein IT-Sicherheitskonzept aufgebaut worden (58 Prozent). Über die Hälfte der Befragten hat zusätzliche WLAN-Schutzvorrichtungen getroffen oder die Daten besser verschlüsselt. Wurden keine zusätzlichen Sicherheitsmaßnahmen getroffen, begründeten die Befragten dies in der Regel damit, dass ihr Unternehmen bereits gut geschützt sei oder sie sich erst noch mit IT-Sicherheitsmaßnahmen beschäftigen müssten. Da das Homeoffice viele Angriffsmöglichkeiten bietet, empfiehlt die Württembergische eine sichere VPN-Verbindung, die Nutzung der WOA-2-Verschlüsselung beim WLAN und das Unterlassen von privatem Surfen auf dem Firmengerät. Die Erfahrung zeige, dass Kriminelle die Unaufmerksamkeit der Beschäftigten nutzen und diese gezielt bei der mobilen Arbeit angreifen.

„Als Partner des Mittelstands unterstützt die Württembergische ihre Cyberversicherungskundinnen und -kunden mit einer kostenlosen Lernplattform. In Präventionstrainings geben IT-Profis Tipps, damit Sicherheitslücken gar nicht erst entstehen“, sagt Jens Lison, Vorstand der Württembergischen Versicherung.

Praktische Übungen und fortlaufende E-Mail-Phishing-Simulationen sind wesentliche Bestandteile des Cyber-Portals der Württembergischen. Laut der Erhebung haben 45 Prozent der interviewten Mittelständler bereits damit begonnen, ihre Belegschaft stärker für das Thema zu sensibilisieren.

Anwaltliche Unterstützung im Ernstfall gefragt

Spezielle Cyberversicherungen sind wichtig, da Versicherungslösungen wie die Haftpflichtversicherung nicht ausreichen, um Unternehmen vor den finanziellen Folgen eines Cyberangriffs zu schützen. Das Bewusstsein für eine Absicherung gegen Gefahren aus dem Internet mit einer Cyberversicherung hat zugenommen: 62 Prozent der Befragten gaben an, dass ihr Unternehmen bereits über eine solche Police verfügt. Die meisten von ihnen haben diese in den vergangenen drei Jahren abgeschlossen.

Im Schadensfall spielt schnelles Handeln eine entscheidende Rolle. 88 Prozent der Befragten wünschen sich dann vor allem die Unterstützung durch Anwälte zum Beispiel bei Haftpflichtansprüchen Dritter. Laut der Erhebung wird auch die Kostenübernahme bei Ertragsausfällen durch eine Betriebsunterbrechung, die Kostenübernahme für den Austausch von Hardware, die Möglichkeit zu forensischen Untersuchungen zur Ursachenermittlung sowie Datenschutz-Beratung und Präventionstraining als wichtig erachtet. „Schnelle Hilfe ist im Schadenfall unerlässlich. Bei der Württembergischen können sich Kundinnen und Kunden auf unsere 24-Stunden-Servicehotline verlassen. Mittelständische Unternehmen sollten bei ihrer Absicherung zudem darauf achten, dass diese genau zum Betrieb und zur Branche passt“, sagt Lison.

Über die Befragung

Für die Erhebung hat das Marktforschungsinstitut Appinio im ersten Halbjahr 2021 im Auftrag der Württembergischen Versicherung 200 Geschäftsführer, Inhaber und Experten im deutschen Mittelstand befragt, die sich mit Cyberrisiken und Sicherheitsvorkehrungen auseinandersetzen.

Über 70 Prozent der Befragten sind aus Unternehmen mit weniger als 500 Mitarbeiterinnen und Mitarbeitern.