Hackerangriffe auf Firmen sind permanente Gefahr

Heimische Banken informieren zu Cybersicherheit – Experten geben wichtige Ratschläge

VON MARCUS ALTHAUS

Im Korbacher Kino warnten Jürgen Trumpp von der Sparkasse Waldeck-Frankenberg und Nikolaus Stapels (rechts) vor Hackerangriffen. Im Bürgerhaus Korbach verdeutlichten (rechtes Bild, von links) Andreas Pohl, Carsten Hohmann und Oliver Boselli die digitalen Risiken in der von Katja Patzwaldt (Waldeck-Frankenberger Bank) organisierten Veranstaltung. FOTOS: ALTHAUS

Korbach – Die fortschreitende Digitalisierung bringt eine permanente Gefahr von Cyberattacken mit sich. Rapide zunehmend, finden Angriffe auf Netzwerke und Daten von Unternehmen statt. Um hiesige Firmen für mehr Cybersicherheit zu sensibilisieren, haben die Waldeck-Frankenberger Bank und die Sparkasse Waldeck-Frankenberg jeweils Experten eingeladen, die interessierten Firmen Ratschläge und Impulse für besseren Schutz gaben.

Längst seien Kunden der heimischen Finanzinstitute von Hackerangriffen betroffen, wie die Vorstandsvorsitzenden Jürgen Trumpp (Sparkasse) und Carsten Hohmann (Waldeck-Frankenberger Bank) in den jeweiligen Veranstaltungen im Korbacher Kino und im Bürgerhaus bestätigten. Die Frage sei seit geraumer Zeit nicht mehr, ob ein Unternehmen gehackt werde, sondern wann und in welchem Umfang. Wer glaube, nur interessante oder bedeutsame Daten seien das Ziel, der irrt. Kriminelle Cyber-Attacken störten immer die Betriebsabläufe, blockierten Computer und Systeme und könnten dadurch Unternehmen in finanzielle Schieflage oder die Insolvenz treiben.

Längst seien es keine einzelnen Computernerds mehr, die sich wahllos Firmen als Ziele heraussuchen. Mittels Schadprogrammen werde millionenfach und dauerhaft versucht, Schwachstellen bei Unternehmen und Privatpersonen zu finden.

„Man muss kein umfassender IT-Spezialist sein“, wie Nikolaus Stapels, Cybersicherheitsexperte, beschreibt. Die nötige Software für Angriffe werde im Darknet verkauft. Ab zehn Dollar könne sich jeder damit ausrüsten, der Identitäten ausspionieren wolle. Ab 50 Dollar gebe es Zugänge zu Firmen. „Deswegen wurde auch das FBI in den USA von einem 16-Jährigen gehackt.“ Für manche Jugendlichen sei es ein Wettbewerb. Die kriminellen „Hacker-Banden“ hingegen hätten mittlerweile Organisationsstrukturen wie Unternehmen und agierten weltweit in einem für sie extrem lukrativen Markt. Auch einige Staaten hätten früh aufgerüstet und setzten Cyberangriffe und -abwehr gezielt ein.

Andreas Pohl, IT-Securitymanager aus Mengeringhausen, sagte: „China hat für die Cyberabwehr eine Million Angestellte, Russland 450 000, die USA 250 000, während Deutschland nur über wenige Tausend verfügt. Das Sicherheitsniveau hat sich hierzulande in den vergangenen zehn Jahren nicht geändert, aber die Gefahren haben extrem zugenommen.“ Die Telekom erzeuge in Echtzeit absichtlich verlockende Ziele, die für potenzielle Angreifer attraktiv erscheinen, aber keinerlei echte Infos preisgeben. Auf diese Weise erhalte das Unternehmen Erkenntnisse über Angriffsmuster. Am Freitag, 26. April 2024, gegen 12.20 Uhr, wurden so mehr als 200 000 Alarme in 60 Sekunden registriert.

Deutschland sei, neben den USA, das digital meist angegriffene Land der Welt, mit weitem Abstand zu seinen europäischen Nachbarn. Frankreich und Großbritannien erlitten gemeinsam nur einen Bruchteil der Attacken in dem Telekom-Monitoring.

Das Thema ernst nehmen

„Das Thema muss ernst genommen werden“, fordert Oliver Boselli. Der Experte für Cyberversicherungen macht immer noch die Erfahrung, dass das Risiko unterschätzt wird. Er rät jedem Unternehmer, seine IT-Sicherheit regelmäßig überprüfen zu lassen. Dies sei der erste Schritt zur Prävention. Deutschlands Versicherer gehen von mehreren Hundert Milliarden Euro Gesamtschäden im Jahr aus. „Die Gefahr, gehackt zu werden, ist größer als die eines Brandes, und die Schadenssummen übertreffen die Schäden, die jährlich bei allen Pkw-Unfällen gemeinsam verursacht werden“, so Boselli. Zu den betroffenen Firmen zählen alle Betriebsgrößen: Kleinbetriebe, Mittelstand und Konzerne. Mal gehe es darum, das System lahmzulegen, um Lösegeld zu erpressen. Mal werden Adressen von Großkunden ausspioniert, um dort weiter ansetzen zu können.

Boselli: „Es ist der moderne Einbruch, nur dass Sie bei einem Gebäude die Position aller Zugänge kennen und absichern können, während sich im digitalen Firmennetzwerk die Positionen der Zugänge ständig ändern.“ Die meisten Angriffe kommen per E-Mail. „Es gibt immer einen Mitarbeiter, der den Link oder Anhang anklickt“, so Nikolaus Stapels. Mittels künstlicher Intelligenz sei es noch einfacher, Kundenkorrespondenz fehlerfrei nachzuahmen. Jede Firma sollte daher Richtlinien festlegen, Mitarbeiter schulen, regelmäßig Passwörter ändern, Antivirenprogramme und Firewalls richtig einsetzen, wichtige Daten verschlüsseln und jeden Tag Datensicherung betreiben. Es gelte, die Kosten und den Nutzen einer Cyberversicherung abzuwägen, die im Notfall Experten zur Verfügung stellen, um das System wieder einsatzfähig zu machen.

„Rechnen Sie sich aus, was es Sie kostet, wenn ihr Unternehmen vier bis sechs Wochen nicht handlungsfähig ist und ihre Betriebskosten weiter bezahlt werden müssen“, sagte Andreas Pohl. ma