



Wie schütze ich meine IT vor kriminellen Machenschaften? Diese Frage ist nicht nur für große Konzerne, sondern auch für kleine Handwerksbetriebe überlebenswichtig, denn die Anzahl und die Professionalität von Hacker-Angriffen nehmen stetig zu. Grund genug für die Expertenrunde bei „Veka mittags live“ im Dezember, sich auf Spurensuche zu begeben und anhand von realen Beispielen ein aktuelles Bild der Bedrohungslage zu zeichnen. Ihr Fazit: Die Täter gehen mit bemerkenswerter Kreativität vor. Ein wirkungsvoller Schutz ist aber trotzdem möglich.

„Cyberkriminalität ist ein Thema, von dem wenig gesprochen wird – aber es geht uns alle an.“ Mit diesen Worten begrüßte Josef L. Beckhoff, Vorstand Vertrieb und Marketing bei der Veka AG, die Gäste im Studio und die zahlreichen Zuschauenden im Stream zur fünften Ausgabe von Veka mittags live.

Die Diskussion zu diesem sehr wichtigen und aktuellen Thema wurde wieder von Prof. Christian Niemöller (Fachanwalt für Bau- und Architektur-Recht) moderiert und die Experten Helmut Meeth (Geschäftsführer Helmut Meeth GmbH & Co. KG, Präsident VFF), Lars Klaes (Geschäftsführer Klaes GmbH & Co. KG), Dietmar Helmich (CEO Helmich IT-Security GmbH) und Thomas Sauerland (Digital Transformation IT Services, CIO Veka Group) redeten Klartext.

Jeder ist potenziell Gegenstand eines Angriffs

Schon in seinem kurzen Impulsvortrag sagte Sauerland, dass heute jeder davon ausgehen müsse, dass er irgendwo in seinem IT-Umfeld eine „offene Tür“ hat. Und solche Schwach-

stellen würden von Personen mit böser Absicht genutzt. Die Zahl der Angriffe nehme immer weiter zu, und durch die Nutzung von künstlicher Intelligenz werde die Bedrohung in Zukunft noch größer.

Im Jahr 2023 seien allein in Deutschland 68 Fälle bekannt geworden, in denen Hacker Unternehmen erfolgreich mit so- genannter Ransomware erpresst hätten. Das bedeutet, dass die Kriminellen sich Zugang zu den Daten des Unternehmens verschafft und diese verschlüsselt haben. Erst nach der Zahlung eines „Lösegeldes“ wurden die Systeme wieder freigegeben.

„Es wird der Weg des geringsten Widerstands genommen“

Auch Helmich, der sich mit seiner Firma auf die Bekämpfung von Hacker-Angriffen spezialisiert hat, betonte, dass man die Gefahr nicht unterschätzen dürfe. „Im Jahr 2009 haben die Erlöse aus der Cyberkriminalität bereits den weltweiten Drogenhandel überholt“, sagte er. „Das heißt, die Bösewichter, denen wir gegenüberstehen, können sich alle Fachkräfte, alle Geräte, alle Verbindungen, alles wirklich erlauben, weil sie unglaublich viel Geld verdienen.“

Wie professionell und arbeitsteilig die Kriminellen inzwischen vorgehen, beschrieb Klaes, der mit seinem Unternehmen Software für Fenster- und Türenhersteller entwickelt. Einige Hacker hätten sich zum Beispiel darauf spezialisiert, Schwachstellen bei Unternehmen zu finden. Diese so genannten „Access Broker“, so Klaes, verkaufen ihr Wissen dann im Darknet an Erpresser, die anschließend Ransomware-Attacken gegen die betroffenen Unternehmen durchführen.

Früher seien es vor allem größere Unternehmen gewesen, die zum Ziel solcher Angriffe wurden. Die Kriminellen wollten auf diese Weise möglichst große Lösegeldforderungen durchsetzen. Inzwischen habe sich die Strategie aber geändert: „Es wird der Weg des geringsten Widerstands genommen.“ Die Angreifer nähmen jetzt also auch den Mittelstand und sogar kleine Unternehmen ins Visier, weil diese Firmen oft schlechter geschützt seien.

Vorsorge treffen in der IT-Sicherheit

Wie sich ein solcher Angriff aus der Perspektive eines Betroffenen darstellt, beschrieb Meeth. Sein Unternehmen wurde im vergangenen Jahr mit Hilfe einer Ransomware praktisch lahmgelegt. „Wir konnten noch einiges retten. Wenn es dann aber in die Produktionsabläufe geht, für die man Daten braucht, wenn man die einzelnen Arbeitsplätze mit Bildschirmen versorgt hat und nichts funktioniert, das ist eine einzige Katastrophe. Und wir mussten das erleben.“ Nach dem Angriff habe es ein halbes Jahr gedauert, die Systeme wiederherzustellen, und manche Auswirkungen seien immer noch spürbar.

Vor diesem Hintergrund rät Sauerland allen Unternehmen, Vorsorge zu treffen und die IT-Sicherheit anhand von 100 Fragen zu evaluieren. Ein entsprechender Fragebogen ist auf www.veka.de verlinkt. Wenn die Einschätzung positiv ausfällt, ist das Risiko eines Angriffs zumindest deutlich reduziert. Und wenn sich aus der Überprüfung Aufgaben ergeben, kann man sich Unterstützung von Experten holen und aktiv Maßnahmen ergreifen, die für Hacker nur schwer zu überwinden sind. ■

www.veka.de