# Es kann jeden treffen

IM RAHMEN DES ONLINE-FORMATS „VEKA MITTAGS LIVE" DISKUTIEREN EXPERTEN IM DEZEMBER ÜBER HACKER-ANGRIFFE UND CYBER-KRIMINALITÄT. IHR FAZIT: DIE TÄTER GEHEN MIT BEMERKENSWERTER KREATIVITÄT VOR. EIN WIRKUNGSVOLLER SCHUTZ IST ABER MÖGLICH.


**Die Expertenrunde redete Klartext (v.l.): Dietmar Helmich (CEO Helmich IT-Security GmbH), Lars Klaes (GF, Klaes GmbH & Co. KG, Softwareunternehmen für Fenster und Türen), Helmut Meeth (GF Helmut Meeth GmbH & Co. KG, Präsident VFF), Josef L. Beckhoff (Vorstand Vertrieb und Marketing Veka), Christian Niemöller (Fachanwalt für Bau- und Architektur-Recht) und Thomas Sauerland (Digital Transformation IT Services, CIO Veka Group).**

**„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 extrem spannenden Thema wurde wieder von Prof. Christian Niemöller (Fachanwalt für Bau- und Architektur-Recht) moderiert, und die Experten Helmut Meeth (Geschäftsführer der Helmut Meeth GmbH & Co. KG und Präsident des Verbandes Fenster+Fassade), Lars Klaes (Geschäftsführer, Klaes GmbH & Co. KG, Softwareunternehmen für Fenster und Türen), Dietmar Helmich (CEO Helmich IT-Security GmbH) und Thomas Sauerland (Digital Transformation IT Services, CIO VEKA Group) redeten Tacheles.

## JEDER IST POTENZIELL GEGENSTAND EINES ANGRIFFS

Schon in seinem kurzen Impulsvortrag sagte Thomas Sauerland, der bei Veka für die IT-Sicherheit zuständig ist, dass heute jeder davon ausgehen müsse, dass er irgendwo in seinem IT-Umfeld eine „offene Tür" hat. Und solche Schwachstellen 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" (engl. „Ransom") wurden die Systeme wieder freigegeben.

Auch Dieter 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 gegenübersitzen, 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 Lars Klaes, der mit seinem Unternehmen Software für Fenster- und Türenhersteller entwickelt. 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 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.

## DIE PERSPEKTIVE EINES BETROFFENEN

Wie sich ein solcher Angriff aus der Perspektive eines Betroffenen darstellt, beschrieb VFF-Präsident Helmut 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.

### 100 FRAGEN ZUR IT-SICHERHEIT

**Thomas Sauerland, CIO bei Veka, rät 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.**