Oberösterreichische Versicherung AG

medieninformation

Hackerangriffe

Was tun, wenn im Unternehmen plötzlich nichts mehr geht?

Linz (17. Mai 2022) ***`Hacker legen Firma lahm´. Für manche Unternehmen ist diese Meldung nichts neues. Sie haben selbst Erfahrung mit einem Cyber-Angriff gemacht. Neben dem finanziellen Schaden verlieren Betriebe dabei nicht nur den Zugang zu ihren Unternehmensdaten, auch ganze IT-gesteuerte Produktionen stehen still.***

Im Rahmen einer Podiumsdiskussion, veranstaltet von der Oberösterreichischen Versicherung, erklärt der IT-Forensiker Jürgen Weiss, wie komplex ein solcher Angriff vor sich geht. Nach solch einem Ransomware-Angriff muss zudem schnell gehandelt werden.

„Die Verbrecher geben keine Verschnaufpause. Es kommt sehr rasch ein Link für einen Tor-Browser - links steht der geforderte Betrag, in der Mitte läuft der Countdown, rechts ist angegeben, ab wann sich der erpresste Betrag verdoppeln wird“, so Weiss, Geschäftsführer von Ares Cyber Intelligence.

Notfallplan unbedingt erforderlich

Gibt es keinen Notfallplan, sind das Management eines Unternehmens und ihre IT-Abteilungen in dieser Situation meist komplett überfordert. Laut Weiss muss vieles gleichzeitig bedacht werden: „Wie viel kostet ein Tag Stillstand? Was ist alles betroffen, ist es möglich, Daten zu retten?"

Neben Ruhe bewahren ist es wichtig, dass das Management folgenden Schritte setzt: Fakten sammeln, Optionen entwickeln, Risiko der Optionen einschätzen, sich für eine entscheiden und umsetzen und schließlich die Wirksamkeit überprüfen. Auch die Krisenkommunikation darf nicht vergessen werden: extern nicht kommunizieren, um die Verhandlungsposition nicht zu

Rückfragen: **Mag. Toril Fosen | Pressesprecherin** | fon. +4357891-71590 | mail. t.fosen@ooev.at

gefährden, intern sind aber Mitarbeiter und Partner zu informieren, um Unsicherheiten entgegenzusteuern.

Neben einem guten Notfallplan muss das Unternehmen auch auf ein gutes IT-System schauen. Vielen Geschäftsführern ist nicht bewusst, dass sie bei einem Schaden Haftung übernehmen müssen, wenn die IT den Anforderungen des Unternehmens nicht entspricht.

„Wir hatten einen Datenverlust von fünf Tagen. Die rasche Erledigung verdanken wir einem externen Expertenteam aus Forensikern und IT-Beratern. Es tabuisieren viele betroffene Unternehmer das Thema. Im ersten Moment ist das okay. Wichtig ist aber die Kommunikation im Nachhinein. Ich möchte damit anderen Unternehmen einen Anstoß geben, sich mit dem Thema auseinanderzusetzen. Die Situation ist alles andere als angenehm“, sagt Florian Hütthaler, Chef der Hütthaler KG.

Schutzschirm Cyber-Versicherung

Eine Cyber-Versicherung kann keinen Hackerangriff abwehren, aber den Schaden minimieren. Sie sorgt dank ihrer Assistanceleistungen und dem daran geknüpften Expertennetzwerk dafür, dass bereits im Vorfeld Sicherheitslücken erkannt werden und im Fall eines Angriffs rasch fachkundige Hilfe kommt. Eine gute Cyber-Versicherung kommt zudem für den Eigenschaden auf und haftet auch gegenüber Dritten, wie Kunden oder Lieferanten und übernimmt die Kosten für die datenschutzrechtlich verpflichtende Meldung des Data Breach gegenüber der Datenschutzbehörde. Ein IT-Sicherheitspaket ist also ähnlich wie eine Feuerversicherung aus dem Schutzschirm jedes Unternehmens nicht mehr wegzudenken.

Rückfragen: **Mag. Toril Fosen | Pressesprecherin** | fon. +4357891-71590 | mail. t.fosen@ooev.at

Bildtext:

Foto 1: Vorstandsdirektorin Kathrin Kühtreiber-Leitner und Leiter des Kompetenzteams Gewerbe Reinhard Weissengruber befassen sich im Rahmen einer Veranstaltung der Oberösterreichischen Versicherung mit IT-Sicherheit.

Foto 2: IT-Forensiker Jürgen Weiss klärt im Rahmen der Veranstaltung über Risiken und Auswirkungen von Hackerangriffen auf.

Foto 3: Unternehmer Florian Hütthaler berichtet über seine Erfahrungen mit Cyber-Attacken und möchte andere Unternehmen anregen, sich mit dem Thema zu befassen.

Fotorechte: Oberösterreichische Versicherung/Abdruck honorarfrei

Rückfragen: **Mag. Toril Fosen | Pressesprecherin** | fon. +4357891-71590 | mail. t.fosen@ooev.at