»OBSERVER«

Die Presse
Unabhängige Tageszeitung für Österreich
Wien, am 26.03.2021, 312x/Jahr, Seite: 20
Druckauflage: 61 480, Größe: 87,72%, easyAPQ: _
Auftr.: 5859, Clip: 13468555, SB: Attensam

www.observer.at

Als Lösegeld wurden 40 Bitcoins gefordert

Cyberangriff. Hausbetreuer Attensam wurde vor Weihnachten gehackt und erpresst. Oliver Attensam räumt noch immer den Schaden auf. Er erzählt vom Kampf um die Daten.

VON HANS PLEININGER

Ich habe immer gedacht, dass wir zu klein und unbedeutend sind, dass uns einer hackt und erpresst“, sagt der Wiener Unternehmer Oliver Attensam, der mit seiner Hausbetreuung Attensam rund 100 Millionen Euro umsetzt und mehr als 1500 Beschäftigte hat. Falsch gedacht: In der Nacht zum 28. November vergangenen Jahres wurde Attensams Familienunternehmen gehackt. „Alle unsere Daten waren verschlüsselt. Wir konnten nichts mehr machen.“

Nach kurzer Zeit hat Attensam eine Nachricht bekommen: „Für ein gewisses Lösegeld wird wieder alles entschlüsselt.“ Die Erpresser haben von Attensam 40 Bitcoins gefordert. Der damalige Bitcoin-Kurs war rund 17.000 Euro, das macht eine Erpressersumme von etwa 680.000 Euro aus. „Die Erpresser wissen genau, was man zahlen kann. Die Schmerzgrenze wird offensichtlich so ausgewählt, dass einer, der mit dem Rücken zur Wand steht, diese Summe auch aufbringen kann.“

Vom Erpresser, der schlechtes, aber verständliches Englisch gesprochen habe, erzählt Attensam, dass er freundlich war und gemeint hat, dass „wir das das nicht persönlich nehmen sollen“. Das sei sein Geschäftsmodell. Wenn einzahlt wird, sei ihm ganz wichtig, dass alles wieder funktioniert, denn er habe eine Reputation zu verteidigen. „So eine Aussage, das muss man erst einmal verdauen“, sagt Attensam.

Zum Zeitpunkt der Lösegeldforderung hatte sich Attensam schon Cyber-Crime-Spezialisten in die Firma geholt. Diese haben kurzfristig die Führung des Unternehmens übernommen und die Kommunikation mit den Erpressern aufgenommen. Die Profis haben eine Erweiterung der Zahlungsfrist bekommen. „Normalerweise hat man nur 24 Stunden Zeit zu zahlen, dann ist alles weg“, sagt Attensam. Durch die gewonnene Zeit konnte man analysieren, was passiert war, und beurteilen, ob von irgendwoher die Daten zu bekommen sein könnten oder man chancenlos war.

Unternehmer Oliver Attensam: „Die Erpresser wissen genau, was man zahlen kann.“
[Attensam/Peter Rigaud]

Glück im Unglück

Vornweg: Attensam zahlte kein Lösegeld. Denn in der Datensuche erwies sich als „Riesenglück“, dass Attensam vor einem Jahr auf ein neues Backupkonzept umstellte, „das parallel mitgelaufen ist“, sagt der Firmenchef. Bei diesem Sicherungssystem hat der Eindringling nur den Lesekopf und Sicherungen auch nur bedingt zerstört - und somit nicht alle Daten vernichtet. „Das war unsere Überlebenschance“, sagt Attensam. In den Backups fanden sich 30 Terabytes Rohdaten, die irgendwo abgelegt waren.

„Als wir erkannt haben, wir haben eine Chance, haben wir mit dem Erpresser nicht mehr groß kommuniziert. Wir haben nur noch auf Zeit gespielt“, sagt Attensam. „Denn wir wussten damals nicht, was er alles von uns hat.“ Heute weiß Attensam, dass der Erpresser alle Daten verschlüsselt hatte, aber dass keine Daten extrahiert wurden. „Gott sei Dank war unsere EDV-Technik gut genug aufgestellt, dass man Daten nicht herausbekommen hat.“

Die Suche und Rekonstruktion der Daten-Files dauerte: Eine erste Datensicherheit hatte Attensam nach sechs Wochen. Rückblickend habe man bei der Rekonstruktion der Datenbank alles bis auf eine Woche geschafft.

Attensam weiß heute auch, wie sich die Cyberkriminellen Zugang verschafft haben. Es seien zwei Ursachen gewesen: „Vor etwa einem Jahr hat bei Microsoft eine Lücke bestanden. Da konnte etwas passieren“, sagt Attensam. „Den zweiten Fehler haben wir gemacht - im ersten Lockdown vor einem Jahr, als wir 200 externe Home-Arbeitsplätze auf die Beine gestellt haben, haben wir die Passwort-Administration abgesenkt.“ Beides habe dazu geführt, dass sich jemand von außen in das System einnisten und Passwörter absaugen konnte und „sich monatelang in unserem System bewegen konnte, als wäre er ein Attensam-EDV-Mitarbeiter“.

Aus dem Angriff hat Attensam viel gelernt: „Keine Daten aus dem Unternehmen herauszugeben ist völliger Blödsinn.“ Besser sei es, Daten bei namhaften EDV-Unternehmen wie Google oder Apple auszulagern. „Da ist es tausendmal sicherer, die werden tausendmal am Tag beschossen.“ Auch im eigenen EDV-System hat Attensam Schotten eingerichtet, damit man nicht mehr überall hinkommt.

Solang der Erpresser im Spiel war, war bei Attensam Nachrichtensperre. „Wir haben gesagt, wir haben Server-Probleme.“ Als klar war, dass Attensam kein Lösegeld zahlen wird, „haben wir voll auf Kommunikation gesetzt“. Es den wichtigsten Kunden und Lieferanten mitgeteilt, und auch den Mitarbeitern hat man einmal die Woche per Video gesagt, „was Sache ist“.

Der Erpresser habe nach drei, vier Tagen aufgegeben: „Am Schluss war er weniger höflich und hat uns gedroht, wir kommen auf die Nichtzahlerliste im Darknet“, sagt Attensam: „Das war für uns eine Erlösung, weil das für andere Hacker heißt, wir sind eine hartnäckige Firma, die nicht zahlt.“