Die unterschätzten Cyberrisiken

KMU werden von Cyberkriminellen besonders gerne ins Visier genommen. Auch die Weber Hofer Partner AG musste erfahren, wie ihr Betrieb von einem Moment auf den anderen stillgelegt wurde.

Das Architekturbüro der Weber Hofer Partner AG in Zürich sieht genau so aus, wie man sich ein Architekturbüro vorstellt. Hohe, verwinkelte Decken mit unzähligen Fenstern lassen viel Licht in den ausgebauten Dachstock und öffnen den Raum, das Innendesign wirkt schlicht und zeitlos. In den klassischen Sideboards der Marke USM reihen sich die Ordner aneinander, auf den Bürotischen überdecken sich die Baupläne gegenseitig. Übersähe man die zahlreichen Desktops, könnte man meinen, hier werde noch ausschliesslich mit Stift und Papier gearbeitet. Dem sei aber nicht mehr so, ohne Computer laufe auch bei ihnen gar nichts mehr, entgegnet Josef Hofer, Gründer und Inhaber des Unternehmens. Spätestens seit einem Freitagmorgen im Frühjahr 2019 steht dies ausser Zweifel.

Trügerisches Sicherheitsgefühl

Als sich eine Mitarbeiterin an diesem Morgen als Erste an ihrem PC anmelden wollte, erhielt sie keinen Zugriff. Eigentlich nichts Ungewöhnliches, dies kam öfter mal vor. Entsprechend wandte sie sich an den IT-Support. Kurze Zeit später stand jedoch bereits fest: Das Architekturbüro war einem Cyberangriff zum Opfer gefallen. «Ich hätte nicht im Traum daran gedacht, einmal von einer solchen Attacke betroffen zu sein, wir sind doch völlig uninteressant», sagt Hofer bescheiden. Mit seiner Risikowahrnehmung steht der Architekt nicht allein da. «Viele Firmen wiegen sich in falscher Sicherheit. Sie gehen davon aus, dass sie nichts zu verstecken haben und so auch kein potenzielles Angriffsziel darstellen. Entsprechend wird bei der Cybersicherheit oft gespart», erläutert Tobias Ellenberger von der Oneconsult AG, einem auf Cyber Security spezialisierten Beratungsunternehmen. Dies spiele den Angreifern zusätzlich in die Karten. Sogenannte Phishing-Attacken, wie sie sehr häufig vorkommen, würden nämlich in der Regel grossflächig gestreut – ohne die möglichen Opfer zuerst konkret analysiert zu haben.

«Unterlagen, Archiv, Mailverkehr, alles war weg.»

Josef Hofer, Inhaber Weber Hofer Partner AG

Dies musste auch Hofer erfahren, obwohl er bereits viel in die digitale Sicherheit investiert hatte. Er verfügte über eine Firewall, und auch das Antivirusprogramm war stets auf dem neusten Stand. Backups wurden gewissenhaft und regelmässig erstellt, und sogar eine Cyberversicherung hatte er auf Anraten seines Versicherungsberaters abgeschlossen. Trotzdem konnte sich eine sogenannte Ransomware im Server der Firma einnisten und sich so Zugang zu den internen Daten verschaffen. In den meisten Fällen passiere dies, wenn Mitarbeitende infizierte Dokumente – beispielsweise aus Anhängen erhaltener E-Mails – anklicken. «Das Personal als grösste Risikoquelle zu betiteln, erachte ich aber als falsch. Vielmehr bietet sich durch dessen richtige Ausbildung und Sensibilisierung die grösste Chance zur →

Meine Firma

Das 1988 gegründete Architekturbüro nennt sich seit 2007 Weber Hofer Partner AG und beschäftigt heute vierzehn Mitarbeitende. Sowohl über die Kantons- als auch Landesgrenzen hinaus und sogar in Asien hat das Unternehmen bereits Grossprojekte realisiert.
→ www.weber-hofer.ch

Verhinderung solcher Ereignisse», ist Experte Ellenberger überzeugt.

Hello, dear friend!

Bereits kurz nach Aufnahme der Analysearbeiten durch die IT-Firma stand fest, dass die Eindringlinge bereits alle Daten verschlüsselt hatten. «Alles war weg, sowohl die Unterlagen zu unseren laufenden Projekten als auch das Archiv und die E-Mails», erzählt Hofer weiter. An einigen Projekten arbeiteten sie bereits seit über zehn Jahren. Sein Unternehmen verkaufe nicht ein Produkt, sondern primär Wissen. Umso prekärer der Datenverlust, da all dieses Wissen digital abgespeichert war. Während der Support versuchte, die verlorenen Daten wiederherzustellen, boten auch die Angreifer Hand – nach Zahlung einer Lösegeldsumme, versteht sich. Mit «Hello, dear friend!» begrüssten die Erpresser Hofer in einer Nachricht und forderten ihn auf, sich zum Aushandeln der Konditionen mit ihnen in Verbindung zu setzen. Er verzichtete darauf. «Bezahlen war nie eine Option, von diesen Betrügern hätten wir ja sowieso nichts bekommen», meint er bestimmt. Auch Tobias Ellenberger rät davon ab, sich im Falle eines Angriffs auf einen Deal einzulassen. Denn: «Es gibt keine Garantie, so wieder an seine Daten zu kommen. Lässt man sich erpressen, könnte dies zudem die Runde machen und weitere Angriffe nach sich ziehen.» Die Hacker seien nämlich gut vernetzt und gleich wie andere Unternehmen auch professionell organisiert. Umso wichtiger daher, sich der Folgen eines totalen Datenverlusts vorgängig bewusst zu werden und die entsprechenden Massnahmen zu treffen.

Mehrfache Belastung

Er sei mit einem «hellblauen Auge» davongekommen, stellt Josef Hofer heute fest. Nur einige Arbeitstage fiel der Betrieb aus, und alle Daten – ausser dem Mailverkehr der letzten Tage – konnten gerettet werden. Zudem übernahm seine Cyberversicherung einen Grossteil der Wiederherstellungskosten. So glimpflich kommen nicht alle davon, bestätigt Ellenberger: «Es gab auch schon Fälle, in denen Firmen gezwungen waren, sich auf Lösegeldforderungen einzulassen, weil sie den finanziellen Schaden infolge eines Datenverlusts sonst nicht hätten tragen können.» Ein weiterer – und laut dem Spezialisten oft zu Unrecht vergessener – Aspekt sind aber auch die psychischen Folgen einer Cyberattacke. «Für ein Team kann das extrem belastend sein. Das reicht von Schuldgefühlen bis hin zu Existenzängsten.» Am günstigsten und besten schütze man sich, «wenn man als Firma kontinuierlich seine Hausaufgaben macht und sich auf die gängigsten Szenarien vorbereitet», führt er weiter aus. Eine hundertprozentige Sicherheit, nicht doch einmal Opfer eines Angriffs zu werden, gebe es nicht. Durch die richtigen Massnahmen könne eine Firma aber nahe an diesen Wert herankommen.

Besser Vorsorgen als Nachsehen

Hofer hat bei der Polizei Strafanzeige gegen Unbekannt erstattet, dies war eine Auflage seiner Versicherung. Hoffnung, die Täter könnten dadurch überführt werden, habe er jedoch keine. Trotzdem sei es wichtig, Anzeige zu erstatten, hält Ellenberger dagegen und erklärt: «Mit jeder Anzeige erhält die Polizei mehr Hinweise auf die kriminellen Strukturen. Sie steht in engem Kontakt mit den internationalen Behörden – die Täter sitzen nämlich in der Regel im Ausland – und kann so zur Enthüllung der Hackerbanden beitragen.» Um nicht wieder in die Opferrolle zu geraten, hat Hofer mittlerweile aufgerüstet und speichert seine Backups nun auch auf einem zusätzlichen, vom eigenen Netzwerk getrennten Server. «Gratis gibt es nichts. Will man sich schützen, muss man investieren. Und wird man angegriffen, fährt man ganz sicher nicht günstiger», beteuert er aus Erfahrung.

Marcel Rubin

Meine Firma

Die Oneconsult AG ist Teil der 2003 gegründeten Oneconsult-Unternehmensgruppe mit Büros in Thalwil, Bern und München. Ihre Cyber-Security-Experten beraten Kunden zu internen und externen Bedrohungen aus dem Informationssicherheitsbereich.
→ www.oneconsult.com

«Die möglichen psychischen Folgen von Cyberkriminalität werden zu oft vergessen.»

Tobias Ellenberger, COO Oneconsult AG & Vice Chairman Oneconsult International AG