„Hackerangriffe nehmen massiv zu“

Kleine und mittelständische Firmen stehen genauso wie Konzerne im Fadenkreuz von IT-Verbrechern. Ein Experte gibt Tipps, wie Unternehmen sich schützen können

Meldungen von Hackerangriffen und Cybererpressungen häufen sich. Erst vor wenigen Wochen waren mehrere Firmen in der Oberpfalz betroffen. Egal ob kleine Firma, Mittelständler oder Großkonzern – mittlerweile stehen alle im Fokus der Hacker, sagt Bernhard Altschäffel. Der 43-jährige Berater für IT-Sicherheit aus Aiterhofen (Kreis Straubing-Bogen) ist seit über 20 Jahren im Informationstechnologiebereich tätig. Er erklärt, wo es sicherheitstechnisch in den Firmen oft noch hapert.

Sicherheitsexperte Bernhard Altschäffel ist seit über 20 Jahren in der IT tätig. Foto: Photography Sascha Iwanow

Herr Altschäffel, wie groß ist das Problem von Hackerangriffen auf Firmen?

Bernhard Altschäffel: Es gibt eine aktuelle Bitkom-Studie. Daran nahmen rund 1100 Firmen aus ganz Deutschland teil, die zehn Mitarbeiter oder mehr beschäftigen. Die Studie zeigt deutlich, dass das Problem größer wird. 88 Prozent der Befragten gaben an, 2020/2021 von Datenklau, -spionage oder -sabotage betroffen gewesen zu sein.

Welche Schadenssummen entstehen dabei?

Altschäffel: Für den Zeitraum 2018/2019 belief sich die Schadenssumme der Bitkom-Studie zufolge auf 103 Milliarden Euro. 2020/2021 waren es bereits 220 Milliarden Euro. Diese Summen beziffern aber nur den Schaden, der den Unternehmen entsteht, wenn sie durch einen Cyberangriff lahmgelegt werden. Wenn sie also nicht mehr produzieren oder keine Ware verkaufen können. Schäden aus Datenspionagefällen fließen nicht in diese Bilanz mit ein.

Für die Freigabe der gestohlenen Daten verlangen diese Hackergruppen üblicherweise Lösegeld. Um welche Summen geht es da?

Altschäffel: Anzahl und Höhe der Lösegeldforderungen haben weltweit deutlich zugenommen. Meist machen die Forderungen mehrere Prozent des Jahresumsatzes aus. Bei diesen Hackern darf man sich keine Illusionen machen. Das sind keine verschrobenen Einzelgänger, sondern professionelle Hackergruppen, die sich im Darknet organisieren und diese Erpressungen als von A bis Z durchstrukturiertes Geschäft betreiben. Deshalb gehört die Handhabung einer solchen Lösegeldforderung unbedingt in offizielle, professionelle Hände. Hackerangriffe mit Datendiebstahl müssen Unternehmen an die entsprechenden Behörden melden. Betroffene Unternehmen sollten grundsätzlich kein Lösegeld zahlen.

> „Bei diesen Hackern darf man sich keine Illusionen machen“

Bevorzugen die kriminellen Hacker eine bestimmte Firmengröße?

Altschäffel: Als die Digitalisierung bei kleinen und mittelständischen Firmen noch nicht so fortgeschritten war wie heute, standen vor allem große Unternehmen im Fokus. Mittlerweile darf sich keine Firma mehr dem Irrglauben hingeben, dass die Angriffe weit weg sind. Alle stehen nun im Fadenkreuz. Hacker wissen, wie verwundbar gerade kleine und mittlere Firmen sind. Heutzutage sind auch kleine Firmen als Zulieferer oder Dienstleister mit großen Unternehmen vernetzt. Hacker nutzen diese Hintertür aus.

Wie lange legen Hackergruppen Firmen erfahrungsgemäß lahm?

Altschäffel: Das hängt sehr stark davon ab, wie umfänglich so eine Attacke ausfällt. Bis Daten wiederhergestellt sind, kann es eine bis vier Wochen dauern. Schaffen es die Hacker, die Daten bis hin zum Backup – also zur Sicherungskopie – zu verschlüsseln, müssen in einer Firma erst wieder alle IT-Systeme neu aufgebaut werden. So ein Angriff ist, wie wenn ein Haus abbrennt und man wieder von vorne anfangen muss.

Gibt es Warnhinweise, auf die man achten kann, wenn ein Angriff bevorsteht?

Altschäffel: Wenn etwa einzelne Mitarbeiter plötzlich nicht mehr auf das Firmensystem oder Daten zugreifen können. Falls Mitarbeiter per E-Mail oder SMS aufgefordert werden, ihre Zugangsdaten einzugeben, sollte man Rücksprache mit der IT-Abteilung halten. Ein anderes Szenario: Kollegen melden, dass sie seltsame Mails im Namen eines anderen Kollegen bekommen, der davon aber nichts weiß. Das könnte darauf hindeuten, dass die E-Mail-Adresse gehackt wurde. Wichtig ist: Wenn Mitarbeitern etwas seltsam vorkommt, müssen sie wissen, an wen sie sich wenden können, um die Sache abzuklären. In jeder Firma sollte es hierfür eine Meldekette geben.

Im Zusammenhang mit Datensicherung ist immer wieder von der 3-2-1-Regel die Rede. Was versteht man darunter?

Altschäffel: Die Einhaltung dieser Regel ist die Mindestanforderung in puncto Datensicherung. Sie besagt, dass ein Unternehmen seine Daten mindestens dreifach sichern muss. Zwei Datenträger müssen dafür genutzt werden. Alle Sicherungskopien auf einer Festplatte oder einen Server zu legen, hilft nichts. Einer dieser Datenträger sollte physisch von den anderen getrennt sein – also an einem anderen Ort und auch nicht ins selbe Netzwerk eingebunden. Sofern die Regel in den Firmen überhaupt Standard ist, ist dann leider der Irrglaube weit verbreitet, dass es damit gut ist. Diese Regel macht aber nur Sinn, wenn auch regelmäßig überprüft wird, ob die Wiederherstellung des Backups funktioniert. Deshalb rate ich zur erweiterten Form der 3-2-1-Regel.

> „Einfallstor für Angriffe sind die Mitarbeiter – und das passiert so leicht“

Wie lautet die?

Altschäffel: Das ist die 3-2-1-1-0-Regel. Die zweite 1 steht für die externe Sicherungskopie, die den Status „unveränderbar“ haben muss. Die 0 steht für die stetige automatische Überprüfung, ob das Backup funktioniert.

Was ist für ein Unternehmen als Vorbereitung noch unabdingbar?

Altschäffel: Einen IT-Sicherheitscheck von einem Spezialisten durchführen lassen. Sich auf den Ernstfall mit Not- und Krisenplänen vorbereiten. Wichtig dabei: Diese Pläne einmal im Jahr testen. Hierzu gehören auch das Vorhandensein und das regelmäßige Testen von Datensicherungskonzepten und Wiederanlaufpläne. Das sind Pläne, in denen festgelegt ist, in welcher Reihenfolge die Systeme wieder hochgefahren werden müssen, damit das Unternehmen nach einer Lahmlegung wieder möglichst schnell ins Tagesgeschäft zurückkehren kann.

Was gehört noch dazu?

Altschäffel: Die Firmen müssen sich technisch wappnen. Das heißt, bei der Hard- und Software wie etwa Antivirusprogramm, Authentifizierungsprogramm und Firewall auf dem neuesten Stand sein. Eine Cyberversicherung abschließen, aber nicht ohne eine Prüfung im Vorfeld, damit man keine bösen Überraschungen erlebt. Rund wird das alles aber erst, wenn auch an die Sicherheitslücke Mensch gedacht wird. Die Mitarbeiter müssen geschult werden, etwa im Erkennen von Phishingmails, dem sicheren Umgang mit Passwörtern sowie Firmendaten. Einfallstor für Angriffe sind die Mitarbeiter – und das passiert so leicht.

Können Sie das anhand eines Beispiels veranschaulichen?

Altschäffel: Nehmen wir an, ein Mitarbeiter eines Autozulieferers erhält eine gefälschte E-Mail, in der er darauf hingewiesen wird, dass sich eine geschäftliche Paketlieferung verzögert. Zur Bestätigung soll er auf einen Link im Anhang klicken. Wie es der Zufall will, erwartet der Mitarbeiter vielleicht wirklich eine Lieferung. Mit dem Klicken auf den Link hat er aber einem Trojaner Tür und Tor geöffnet. Der nistet sich nun ins System ein. Das bleibt vielleicht zunächst sogar unbemerkt, da Trojaner nicht unbedingt immer sofort aktiv werden, sondern erst nach zwei oder drei Jahren aus dem Schläfermodus erwachen. Verschärft wird die Situation, wenn dieser Mitarbeiter in dem Unternehmen eine verantwortungsvolle Position einnimmt, in der er auch die Zugriffsrechte auf sensible Daten hat.

Die Corona-Pandemie hat der Digitalisierung zu einem Schub verholfen – Stichwort Homeoffice. Inwiefern hat sich das auf die Cybersicherheit von Firmen ausgewirkt?

Altschäffel: Das war ein Stresstest für die IT-Sicherheit. Vor der Pandemie haben neun von zehn Arbeitnehmern nicht regelmäßig im Homeoffice gearbeitet. Als die Pandemie es nötig machte, dass die Menschen von zu Hause aus arbeiten, mussten diese Strukturen schnell aufgebaut werden. Vielen Homeoffice-Arbeitern musste erst einmal bewusst werden, dass sie auch daheim verantwortungsvoll mit Daten umgehen müssen. Wenn sich zum Beispiel Mutter oder Vater mit dem Kind dasselbe Notebook für Homeoffice und Homeschooling teilen, ist das natürlich ein Sicherheitsrisiko. Die Homeoffice-Situation war ein Brandbeschleuniger für Hackerangriffe.

> „Homeoffice war ein Brandbeschleuniger für Hackerangriffe“

Es befindet sich gerade ein Projekt des Bundesamts für Sicherheit in der Informationstechnik im Aufbau. Was verbirgt sich dahinter?

Altschäffel: Das Projekt heißt Cybersicherheitsnetzwerk und ist ein Zusammenschluss von IT-Sicherheitsexperten, die ihre Expertise bei Sicherheitsvorfällen zur Verfügung stellen. Ziel ist eine flächendeckende, dezentrale Struktur, die kleinen und mittelständischen Unternehmen sowie Privatpersonen effizient und kostenfreundlich zur Verfügung stehen sowie präventiv beraten soll.

Was kommt in puncto Hackerangriffe auf die Unternehmen in Zukunft noch zu?

Altschäffel: Die Sicherheitsvorfälle werden massiv zunehmen. Aber auch die Methoden und Technologien, die Angriffe verhindern, werden sich weiterentwickeln. Hundertprozentige Sicherheit ist jedoch eine Illusion. Wichtig ist: In Unternehmen muss Cybersicherheit Chefsache sein, denn sie ist kein reines IT-Thema. Die Geschäftsführung muss sich intensiv mit dem Thema auseinandersetzen und darf es nicht nur delegieren.

Interview: Valerie Tielich