GEWIEFTE ANGLER

PHISHING IN DER CHEFETAGE

Immer häufiger und immer weiter werfen Hacker ihre digitalen Angelruten aus – stets auf der Jagd nach Unternehmensdaten. Dabei mittlerweile bei weitem die begehrteste Beute: Die dicken Fische in den Chefetagen. Denn wenn jemand Zugriff und Berechtigungen auf sensitive Unternehmensdaten hat, dann in der Regel die Geschäftsführung.

Cyber-Angriffe auf Unternehmen nehmen seit Jahren exponentiell zu – das ist nichts Neues. Doch die Dimensionen, die sie angenommen haben, erreichen mittlerweile ungeahnte Ausmaße. Von kleinen Firmen über mittelständische Betriebe, Krankenhäuser und Banken bis hin zu Großkonzernen – Kriminelle Hacker machen vor niemandem Halt. Auch und besonders nicht vor den Chefetagen. Dabei geht es auch immer öfter um Erpressung im Zusammenhang mit der Verschlüsselung von Unternehmensrechnern und -servern, welche nur gegen Zahlung beträchtlicher Summen wieder entsperrt werden – so der Hacker will.

Deutschland besonders betroffen

Eine Schlagzeile jagt die nächste, ob der Angriff auf das Klinikum Fürth, die Deutsche Bahn oder das Unternehmen Telefónica – auch in Deutschland sind namhafte Betriebe und Konzerne betroffen. Die Folge: Enorme Ausfälle und damit verbundene, teils existenzbedrohende Kosten für die Unternehmen. Besonders auffällig: Im internationalen Vergleich gehört Deutschland laut einer Analyse des Spezialversicherers Hiscox zu den Ländern mit der durchschnittlich höchsten Schadenssumme pro Firma. Die Zahl der Angriffe hat sich laut dem britischen Versicherer seit 2020 international nahezu verdoppelt – Tendenz weiter steigend. Auch das Bundeskriminalamt bestätigt die Zahlen: 2021 erreichte Deutschland den traurigen Rekord von rund 146.000 erfassten Straftaten im Cyber-Umfeld.

Doch wie ist es möglich, dass Hacker in diesem Ausmaß und scheinbar mühelos Zugriff auf deutsche Unternehmensdaten erlangen? Und was haben die persönlichen Zugriffsrechte von Geschäftsführern damit zu tun?

Mehr Angriffsfläche, lukrative Lösegelder

Die organisierte Cyber-Kriminalität stellt generell ein lukratives Betätigungsfeld für ambitionierte Hacker dar. Neben hohen Gewinnchancen und der einfachen Verfügbarkeit in Crypto-Währungen ist das Risiko, gefasst zu werden, gering. Dabei macht die Kombination aus fehlender Manpower aufgrund des Fachkräftemangels und dem Vorherrschen eklatanter Schwachstellen in den IT-Sicherheitsstrukturen vor allem deutsche Unternehmen zum gefundenen Fressen auf dem internationalen Hacker-Bankett. Laut Sicherheitsexperten der IT-Branche haben zudem die wachsende Digitalisierung und die erhöhte Home-Office-Tätigkeit die Tatgelegenheiten vervielfacht. Auch die generell vergrößerte Angriffsfläche durch immer mehr User mit IT-Berechtigungen und eine höhere Anzahl an verwendeten Endgeräten trägt maßgeblich zum gestiegenen Risiko bei. Dabei nicht zu vergessen: Die zum Teil umfangreichen Zugriffsrechte von Geschäftsführern und Geschäftsführerinnen.

ES GIBT HEUTE KEINE IT SECURITY TECHNOLOGIE, DIE NICHT DURCH SOCIAL ENGINEERING ÜBERWUNDEN WERDEN KANN. GERADE WENN ES UM ZIELE WIE DEN GESCHÄFTSFÜHRER GEHT, IST DESHALB BESONDERE VORSICHT GEBOTEN.

Yunus Karakaya, IT-Security-Experte, Consulting4IT, www.consulting4it.de

Selten genug erhalten Arbeitnehmer und Arbeitnehmerinnen konkrete Anweisungen und Verhaltensregeln, wie sie im Büro oder zuhause dafür sorgen können, dass ihre Netzwerkumgebung und ihre Geräte nicht zum Einfallstor für listige Hacker werden. Doch nicht nur sie – auch die Chefetage ist nicht vor Phishing und gewieften Angriffen moderner Hacker gefeit.

Mitarbeiter im Visier

Um ihre Ziele zu erreichen, setzen Cyber-Kriminelle deshalb gezielt auf den Schwachpunkt Mensch. Denn sie haben längst erkannt, wie sie erfolgreich die sprichwörtliche Angel auswerfen können, um über Einzelpersonen Zugang zu Unternehmensnetzwerken zu bekommen. Der Köder: Extrem gut getarnte Phishing-Mails. Dabei ziehen Hacker das ganze Register psychologischer Tricks, damit die Zielperson den Köder schluckt. Sie arbeiten mit ausgefeilten, persönlichen Formulierungen, Zeitdruck, Angst, Nutzung von Autoritätsmacht oder Existenzsorgen, beispielsweise in Form von auffordernden Mails der an-

geblichen Buchhaltung. Ein argloser Klick auf die vermeintliche Lohnunterlage und schon ist es passiert. Die Datei ist geöffnet, die Malware entfaltet ihr zerstörerisches Werk.

Die Geschäftsführung als Sicherheitsrisiko

Besonders heikel: Die Accounts der Geschäftsführung. Denn leider werden diese bei Sicherheitsthemen oft nicht berücksichtigt. Häufig hört man ausschließlich vom Sicherheitsrisiko Mitarbeiter – dabei fällt aktuell auch immer wieder der Begriff „Zero Trust". Aber sind es wirklich ausschließlich die Mitarbeiter, die aufgrund fehlender Sicherheitsvorkehrungen und unzureichender Schulungen zum Einfallstor für Hacker werden? Sicher, jeglicher Zugang kann auf schädlichste Weise genutzt werden. Doch Cyber-Kriminelle peilen mittlerweile immer öfter die Person an, bei der sie umfangreiche Berechtigungen vermuten: Die Geschäftsführung des Zielunternehmens. Meistens landen sie damit einen Volltreffer.

Denn als Chef muss man ja nicht nur einen riesigen Schreibtisch, sondern auch Zugriff auf jede Datei und jedes Laufwerk haben – eine brandgefährliche Einstellung. Denn schafft es ein Hacker, den Account eines Geschäftsführers zu hacken, hat er häufig das gesamte Unternehmen in der Hand und kann sämtliche Daten nach Belieben abgreifen oder verschlüsseln. Das Ende vom Lied: Eine unternehmerische Katastrophe, die durchaus mit einer Firmenpleite einhergehen kann.

Den Hackern ein Schnippchen schlagen

Aber ist es denn tatsächlich nötig, dass die Person an der Spitze Vollzugriff auf alle Unternehmensdaten hat? Ist es nicht eigentlich deren Aufgabe, strategisch zu arbeiten und das operative Geschäft, welches gewisser Berechtigungen viel eher bedarf, anderen Mitarbeitern zu überlassen? Hand aufs Herz: Ein Geschäftsführer sollte doch eigentlich – auch im Sinne seiner Vorbildfunktion – ausschließlich Zugriffsrechte für die Daten erhalten, die er tatsächlich für seine tägliche Arbeit benötigt. So wie jeder andere Mitarbeiter auch.

AUCH DER CHEF ODER DIE CHEFIN SIND NICHT VOR PHISHING UND GEWIEFTEN ANGRIFFEN MODERNER HACKER GEFEIT.

Linda Schmittner, Autorin, Consulting4IT, www.consulting4it.de

Den großen Boss zu markieren - Das ist ohnehin nicht mehr „State of the art". Aber im Zusammenhang mit der wachsenden Bedrohung durch Phishing und Ransomware verzichtet ein kluger Geschäftsführer generell auf einen Datenvollzugriff.

Natürlich handelt es sich dabei nur um eine von vielen Maßnahmen. Die Sensibilisierung und Schulung von Mitarbeitern, das regelmäßige Updaten von Unternehmenssoftware und das Erstellen von Backups sowie eines Recovery-Plans gehören nach wie vor zum Pflichtprogramm für jedes Unternehmen. Zusätzlich sollte jedoch unbedingt auf die Schwachstelle in der Chefetage geachtet werden. Denn ein Chef ist auch nur ein Mensch. Und als ein solcher kann er ausspioniert und ausgetrickst werden. Nimmt man also dem Geschäftsführer die Rechte, schlägt man den Hackern ein Schnippchen - Und der vermeintlich dicke Fisch wird zum echten Flopp.

Linda Schmittner, Yunus Karakaya