SCHRITT FÜR SCHRITT – KRISEN fit

Phishing: Einfallstor Nr. 1 für Schadsoftware – wie Unternehmen sich schützen können

E-Mails sind heute als Kommunikationsweg nicht mehr wegzudenken. Deshalb überrascht es kaum, dass auch IT-Kriminelle sie nutzen, um Schadsoftware in Unternehmensnetzwerke einzuschleusen und Daten zu stehlen. Neben technischen Maßnahmen kann die Sensibilisierung der Mitarbeiter in Verbindung mit regelmäßigen Schulungen für deutlich mehr Sicherheit sorgen.

„Die Angriffe per E-Mail werden immer raffinierter und für die Mitarbeiter wird es zunehmend schwerer, infizierte Mails zu erkennen“, sagt Caroline Eder, Vorsitzende des Arbeitskreises IT-Sicherheit der vbw und Geschäftsführerin des Bayerischen Verbandes für Sicherheit in der Wirtschaft e. V. (BVSW). „Auch die gefürchtete Ransomware, die Daten verschlüsselt, um anschließend Geld zu erpressen, kommt häufig per Mail ins Haus.“

Der Vereinigung der Bayerischen Wirtschaft unterstützt Bayerische Unternehmen und kooperiert im Bereich der IT-Sicherheit mit dem BVSW und den bayerischen Sicherheitsbehörden, wie dem Landeskriminalamt und dem Verfassungsschutz im Rahmen von Awareness- und Informationsveranstaltungen. „Phishing stellt mittlerweile eine ernstzunehmende wirtschaftliche Bedrohung dar“, so Caroline Eder, „Unternehmen müssen dafür sorgen, dass die Belegschaft ein Baustein in der IT-Sicherheitsstrategie wird.“

Typische Angriffsvektoren

Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sind verseuchte E-Mail-Anhänge der häufigste Verbreitungsweg für Schadprogramme. Die Angreifer sind durchaus kreativ, wenn es darum geht, die Aufmerksamkeit der Empfänger zu gewinnen. Mittlerweile gibt es verschiedene Arten von Phishing.

Spam-Mails beispielsweise sind ungezielte Attacken, bei denen die gleiche Mail an eine große Menge von E-Mail-Adressen versendet wird. Diese werden häufig im Darkweb zum Kauf angeboten, nachdem sie über ein Datenleck von einem Anbieter gestohlen wurden. Für eine höhere Erfolgsquote ihrer Spam-Mails setzen die Angreifer geschickt einen Bezug zum aktuellen Zeitgeschehen. So waren zu Beginn der Corona-Pandemie häufig Spam-Mails im Umlauf, die Atemmasken zum Verkauf anboten.

Derzeit sind zahlreiche Phishing-Attacken zu beobachten, die auf die Hilfsbereitschaft der Menschen setzen und angeblich Hinweise zu Spenden an die Ukraine geben.

Ähnlich wie bei den Phishing-Mails nutzen auch **Hoax-Mails** oft den Namen bekannter Institutionen, um Seriosität vorzutäuschen. Hoax-Mails verbreiten falsche Nachrichten, die verängstigen, oder das Gefühl vermitteln, etwas Wichtiges zu verpassen. Das Anliegen wird oft mit hoher Dringlichkeit vorgetragen, um den Empfänger dazu zu bewegen, möglichst ohne Rückfragen eine bestimmte Aktion durchzuführen. Dabei kann es sich beispielsweise um das Herunterladen einer Software handeln, mit der ein Fehler auf dem PC behoben werden soll. Statt der Fehlerbehebung lädt der Anwender jedoch ein Schadprogramm auf seinen Rechner.

Zielgerichteter und damit schwieriger zu enttarnen sind die sogenannten **Spear Phising Mails**. Als Absender wird oft eine Institution vorgetäuscht, die dem Empfänger gut bekannt ist, beispielsweise Paypal, ein Versanddienst oder die Bank des Empfängers. Bei Spear Phishing Mails wird ebenso Druck ausgeübt. So wird der Empfänger aufgefordert seine Kundendaten durch das Klicken auf einen Link zu bestätigen oder zu überarbeiten. Oft wird eine unrealistisch kurze Frist gesetzt, innerhalb der die Aktion durchgeführt werden muss. Tatsächlich ist die Trefferquote bei diesem Angriffsvektor deutlich höher als bei den beiden vorherigen.

Immer wieder versteckt sich Schadsoftware auch in **Bewerbungsmails**. Kriminelle versenden dabei Bewerbungen mit Bild und Lebenslauf im Anhang, die mit Malware infiziert sind. Da die Empfänger jeden Tag viele dieser Mails erhalten, können sie leichter in die Falle tappen.

Besonders schwer zu enttarnen sind **Social Engineering Attacken.** Diese werden oftmals nach vorangegangener Recherche auf ihre Empfänger maßgeschneidert, um sie zur Preisgabe sensibler Daten oder zur Überweisung eines bestimmten Betrags zu bewegen. Die notwendigen Informationen für ihre passgenaue E-Mail finden die Täter meist in den sozialen Netzwerken.

Ähnlich funktioniert der **CEO Fraud**. Hier identifizieren die Angreifer entscheidungsbefugte Personen im Unternehmen, beispielsweise über LinkedIn, Xing oder die Firmenwebseite. Anschließend versuchen sie, diese Mitarbeiter dazu zu bewegen, hohe Geldsummen zu überweisen, indem sie vorgeben, der Auftrag käme direkt vom Top-Management und müsse überdies streng geheim gehalten werden. Um den Betrug besonders glaubwürdig erscheinen zu lassen, setzen Kriminelle auch auf sogenannte Deepfakes. Dabei handelt es sich um gefälschte Audio- oder Videoaufnahmen, in denen Stimmen oder Gesichter manipuliert werden. „Zukünftig werden Deepfakes möglich sein, bei denen die imitierte Person sich kaum vom Original unterscheiden lässt“, so Caroline Eder. „Unternehmen müssen hier eine Strategie entwickeln, wie sie mit den Bedrohungen umgehen.“

Mitarbeiter sensibilisieren und trainieren

Schulungen, die über die aktuellen Betrugsmaschen aufklären, sind eine wichtige Grundlage, um die Mitarbeiter für die Gefahren zu sensibilisieren. In Trainings, bei denen ein Angriff nachgestellt wird, lässt sich das Erlernte anwenden. Darüber hinaus können Unternehmen immer wieder „Testangriffe“ an ihre Mitarbeiter versenden, um zu sehen, wo es eventuell noch Trainingsbedarf gibt. Das gilt es jedoch mit dem Betriebsrat abzustimmen. „Unternehmen müssen auch einen Weg finden, wie damit umgegangen wird, wenn ein Mitarbeiter tatsächlich auf eine infizierte Mail hereingefallen ist“, so Caroline Eder. „Eine offene und vertrauensvolle Unternehmenskultur kann hier Schaden verhindern, denn wenn der Mitarbeiter seinen Fauxpas aus Furcht vor Sanktionen verschweigt, kann sich die Schadsoftware unbemerkt weiter im Netzwerk verbreiten.“