Information zu Cyberrisiken

Risiko 1: Phishing

Das ist die Gefahr: Cyberkriminelle versenden gefälschte E-Mails oder Nachrichten (z. B. SMS), die vorgaukeln, von vertrauenswürdigen Quellen zu stammen. Das Ziel: Es sollen vom Empfänger sensible Informationen preisgegeben werden, etwa Anmeldeinformationen oder Passwörter. Meist will man die ergaunerten Informationen nutzen, um Schadsoftware zu platzieren oder eine Zahlung an die Kriminellen zu veranlassen.

Darauf sollten Sie achten: Oft gibt es eine unpassende oder unpersönliche Ansprache wie „Lieber Kunde“. Die Formulierungen sind unüblich und ggf. kommen auch Fehler bei Rechtschreibung und Satzbau vor. Es wird Druck aufgebaut, mit einem Übel gedroht und zu schnellem bzw. heimlichem Handeln aufgefordert. Auch wenn die E-Mails den Anschein erwecken, echt zu sein, stimmt oft etwas mit der Absender-E-Mail-Adresse nicht. Es werden häufig Buchstaben vertauscht, das Original imitiert oder Zahlen anstatt Buchstaben verwendet.

Risiko 2: Quishing (QR-Code-Phishing)

Das ist die Gefahr: QR-Codes werden manipuliert, etwa mit Aufklebern überklebt. Das Ziel: Die Nutzer bemerken die Fälschung nicht und landen auf einer gefälschten bzw. schadhafte Webseite. Dort geben sie sensible Anmeldeinformationen ein oder veranlassen direkt Zahlungen auf die Konten von Kriminellen.

Darauf sollten Sie achten: Bei QR-Codes sollten Sie immer Vorsicht walten lassen. Prüfen Sie etwa an Parkautomaten, ob es sich um einen Originalaufkleber handelt oder ob dieser überklebt wurde. Wird nach dem Erfassen der Link angezeigt, sollten Sie diesen genau unter die Lupe nehmen. Im Zweifel sollte die betreffende Webseite durch Eingabe der offiziellen Adresse aufgerufen werden, ggf. nach Suche über eine Suchmaschine.

Risiko 3: Whaling

Das ist die Gefahr: Dabei handelt es sich um speziell auf Führungskräfte ausgerichtete Angriffe von Kriminellen. Meist erfolgen diese Angriffe per E-Mail. Das Ziel: Man will direkt an die „dicken Fische“, um besonders wertvolle Informationen zu erhalten oder Zahlungen von größeren Summen zu veranlassen.

Darauf sollten Sie achten: Auch hier wird meist dringender Handlungsbedarf vorgetäuscht. Zudem nutzt man gerne das Hierarchiegefüge aus, indem etwa vorgegaukelt wird, dass die E-Mail von einer wichtigen Person aus der Einrichtung kommt und nur der Adressat ins Vertrauen gezogen wird. Achten Sie also besonders darauf, ob die Forderung zum Üblichen passt. Insbesondere sollten Sie hellhörig werden, wenn ungewöhnliche Vorgehensweisen eingefordert werden oder übliche Prozesse umgangen werden sollen. Solche Anfragen sollten Sie stets kritisch sehen, mit Vorgesetzten oder anderen Führungskräften besprechen oder mit demjenigen abklären, der die Forderung angeblich gestellt hat. Natürlich nutzen Sie zur Kontaktaufnahme nur die Kontaktdaten aus unserem internen Adressbuch. Suchen Sie die Kontaktdaten aktiv heraus.

Risiko 4: Spear-Phishing

Das ist die Gefahr: Hierbei handelt es sich um gezielte Phishing-Attacken, bei denen konkrete Informationen über den Empfänger genutzt werden, etwa zu Tätigkeit oder Aufgaben. Das Ziel: Es soll Vertrauen aufgebaut oder die Hilfsbereitschaft des Empfängers ausgenutzt werden.

Darauf sollten Sie achten: Solche E-Mails sind oft stark mit Informationen auf den Empfänger ausgerichtet. Es drängt sich oft die Frage auf: „Hä, warum schreibt der das?“ Achten Sie darauf, ob der Inhalt zum Üblichen passt. Erhalten Sie von einem Kollegen/einer Kollegin die Bitte, eine Datei zu öffnen, obwohl das noch nie der Fall war, sollte Sie das stutzig machen. Das erst recht, wenn die Kommunikationsform unüblich ist. Auch eine Bitte per SMS ist verdächtig, wenn bisher immer per E-Mail kommuniziert wurde. Machen Sie in solchen Fällen immer den Gegencheck, bevor Sie ggf. dem Geforderten nachkommen. Rufen Sie beispielsweise den angeblichen Absender an, natürlich unter der im Adressbuch enthaltenen Telefonnummer.

Risiko 5: Business E-Mail Compromise (BEC) und E-Mail-Account Compromise (EAC)

Das ist die Gefahr: Bei BEC kompromittieren die Kriminellen zunächst echte geschäftliche E-Mail-Kommunikation. So werden etwa echte E-Mails abgefangen und enthaltene Informationen bzw. Anhänge verändert bzw. ausgetauscht. Das Ziel: Der Adressat gibt sensible Informationen preis oder veranlasst Zahlungen. Beim EAC haben die Kriminellen die betreffenden E-Mail-Konten gekapert und verschicken echte E-Mails von den an sich echten Accounts. Inzwischen häufen sich jedoch auch die Fälle, in denen Kriminelle die Vorgehensweise auf Briefpost übertragen und echte geschäftliche Kommunikation durch gefälschte ersetzen. Dabei werden gestohlene Originalbriefe eingescannt. Der Inhalt (z. B. Beträge, Bankverbindung) wird am Computer manipuliert und wieder ausgedruckt. Die perfekte Täuschung, die allenfalls bei genauem Hinsehen und nur mit Mitdenken auffällt.

Darauf sollten Sie achten: Setzen Sie auf Ihre Erfahrung und Erwartung. Weicht etwas vom Üblichen ab, sollten Sie stets besondere Vorsicht walten lassen. Das ist gerade dann angebracht, wenn sich Kommunikationsmuster oder -wege ändern oder aus heiterem Himmel Zahlungsdaten aktualisiert werden sollen. Gerade wenn sich die Bankverbindung ändert bzw. nicht mehr zur bisherigen passt, ist eine Bestätigung durch den Geschäftspartner unerlässlich. Wählen Sie dafür die Ihnen bekannten Kontaktdaten und nutzen Sie keinesfalls diejenigen, die in der E-Mail oder auf dem Brief angegeben sind. Setzen Sie im Zweifel auch immer auf das Vieraugenprinzip bzw. holen Sie sich eine zweite Meinung ein, etwa von Kollegen.

Risiko 6: Social Engineering

Das ist die Gefahr: Die Kriminellen setzen auf manipulative Vorgehensweisen, um den Angesprochenen oder Adressaten zur Preisgabe von vertraulichen Informationen zu bewegen. Gern wird versucht, über angeblich gemeinsame Freunde oder Interessen eine Vertrauensbasis zu schaffen. Doch auch geschickt platzierte Komplimente oder ein Appell an die Hilfsbereitschaft sollen die Zurückhaltung überwinden.

Darauf sollten Sie achten: Gibt es ungewöhnliche Anfragen oder will man Sie näher kennenlernen, sollten Sie hellhörig werden. Gerade wenn man Sie über Ihren Job oder das Unternehmen ausfragt, sollten Sie nicht zu auskunftsfreudig sein. Nicht selten wird auch hier Druck aufgebaut, eine Notlage vorgetäuscht oder dringende Hilfe eingefordert. Geben Sie keine schätzenswerten Informationen heraus, auch wenn das aus Ihrer Sicht unproblematisch ist. Auch das sind Interna, die Fremde nichts angehen. Und vielleicht ist das nur der Einstieg, um Sie zu erpressen und wirklich Sensibles zu fordern.

Risiko 7: Ausnutzung von Schwachstellen

Das ist die Gefahr: Kriminelle setzen immer wieder darauf, dass ihre Opfer Software installieren oder nutzen, die Sicherheitslücken aufweist. Diese werden dann als Einfallstor genutzt, um etwa weitere Schadprogramme einzuschleusen, Daten abzugreifen oder mittels Ransomware zwecks Lösegelderpressung zu verschlüsseln.

Darauf sollten Sie achten: Nutzen Sie nur Software und entsprechende Quellen, die von der IT-Abteilung freigegeben sind. Brauchen Sie andere Lösungen, installieren Sie diese nicht auf eigene Faust, sondern stimmen das mit der IT-Abteilung ab. Halten Sie Ihre Geräte und Software immer auf dem aktuellen Stand. Bereitgestellte Aktualisierungen installieren Sie unverzüglich. Stellen Sie bei Computer & Co. ungewöhnliche Aktivitäten fest, reagiert dieser ungewöhnlich langsam oder können Sie nicht mehr auf Daten zugreifen, sprechen Sie sofort die Kollegen der IT-Abteilung an. Stellen Sie außerdem sicher, dass Ihre Daten bzw. solche in Ihrer Verantwortung regelmäßig gesichert werden. Ein Back-up kann entscheidend sein, um im Fall der Fälle weiterarbeiten zu können. Im Fall der Fälle haben Kriminelle ein Druckmittel weniger zur Verfügung.

Immens wichtig: Bleiben Sie wachsam!