E-Mail-Bedrohungen: Diese drei sind am schwierigsten zu erkennen

Unternehmen sollten sich bezüglich Strategie zur Gewährleistung der E-Mail-Sicherheit fragen: Sind die Mitarbeiter in der Lage, zwischen einer seriösen E-Mail und einer Bedrohung der E-Mail-Sicherheit zu unterscheiden?

Nicht jedes Unternehmen hat jedoch die Mittel, massiv in den Aufbau einer Sicherheitsarchitektur zu investieren. So unterschiedlich die technischen Voraussetzungen sein mögen, gibt es doch einen gemeinsamen Nenner im Hinblick auf die IT-Security-Strategie: die Endanwender. Barracuda hat 13 Arten von E-Mail-Bedrohungen gelistet. Die folgenden drei sind am schwierigsten zu identifizieren:

Business E-Mail Compromise

Auch als CEO-Fraud, Whaling und Überweisungsbetrug bekannt. Betrüger geben sich in einer E-Mail als Vorgesetzter, Geschäftspartner oder eine andere vertrauenswürdige Person aus. In der Regel legen die Kriminellen es hierbei darauf an, das Opfer entweder zur Überweisung von Geld oder zur Herausgabe von Anmeldedaten oder anderen vertraulichen Informationen zu bewegen. Diese E-Mails sind so gestaltet, als kämen sie von einem persönlichen E-Mail-Konto und enthielten eine dringende Anfrage. Sie wollen beim Empfänger erreichen, dass dieser denkt, der Absender habe es eilig und brauche Hilfe. Der Hinweis, dass die Nachricht von einem mobilen Gerät kommt, macht es wahrscheinlicher, dass der Empfänger Tippfehler oder abnormale Formatierungen übersieht. Oftmals kennen Einzelpersonen die legitimen persönlichen E-Mail-Adressen ihrer Mitarbeiter oder Vorgesetzten nicht. Scheint der Name in der Kopfzeile und der Signatur korrekt, stellen sie deren Identität nicht infrage.

Conversation Hijacking

Beim Conversation Hijacking klinken sich Cyberkriminelle in bestehende Geschäftskonversationen ein oder initiieren neue Konversationen auf Grundlage von ausgespähten Informationen. Conversation Hijacking ist häufig Teil einer E-Mail-Kontenübernahme: Hierbei überwachen Kriminelle das kompromittierte Konto, um Unternehmensvorgänge, Geschäftsaktivitäten, Zahlungsverfahren und andere Details auszuspionieren. Die gekaperten Konten selbst nutzen Angreifer jedoch eher selten für Conversation Hijacking, da der Kontobesitzer die betrügerische Kommunikation leichter bemerken würde. Zudem bleiben Konten in der Regel nicht für einen langen Zeitraum kompromittiert. Conversation Hijacking kann jedoch wochenlange, kontinuierliche Kommunikation zwischen Angreifer und Opfer in Anspruch nehmen. Deshalb nutzen Angreifer hierfür die E-Mail-Domain-Imitation, die es ermöglicht, Angriffe fortzusetzen, selbst wenn die zuvor entführten Konten gesichert und bereinigt wurden.

Brand Impersonation

Bei den meisten Marken-Imitationsangriffen verwenden Kriminelle E-Mails, um sich als vertrauenswürdige Instanz auszugeben, etwa als bekanntes Unternehmen oder eine häufig verwendete geschäftliche Anwendung. In der Regel versuchen die Betrüger, dass Empfänger ihre Anmeldedaten preisgeben oder auf bösartige Links klicken. Die Angreifer verwenden häufig Domain-Spoofing-Techniken oder ähnlich aussehende Domains, um ihre Identitätswechselversuche so überzeugend wie möglich zu gestalten. Benutzer haben sich daran gewöhnt, legitime E-Mails von Anwendungen zu erhalten, die sie auffordern, ihre Anmeldedaten erneut einzugeben. Anfragen von Microsoft 365, Amazon und Apple, in denen die Benutzer aufgefordert werden, ihre Identität zu bestätigen, ihre Kennwörter zurückzusetzen oder neuen Servicebedingungen zuzustimmen, sind in vielen Posteingängen alltäglich. Viele klicken daher unbedarft auf Links, die sie letztendlich zu Phishing-Seiten führen. Cyberkriminelle bauen darauf, dass ihre Benutzer den Köder schlucken. Mit Schulungen zur Stärkung des Risikobewusstseins erlernen Mitarbeitende, potenzielle Sicherheitsrisiken zu erkennen und auf sie zu reagieren. ■

Barracuda Networks AG, CH-8060 Zürich
dachsales@barracuda.com, de.barracuda.com