20.06.2024

Reply-Chain Phishing

So gut wie jeder kennt Antwortketten in E-Mails. Eine E-Mail wird an eine oder mehrere Personen gesendet und verschiedene Personen antworten darauf. Sie erwarten nicht, dass sich in dieser laufenden E-Mail-Konversation eine Phishing-E-Mail verbirgt. Die meisten Menschen erwarten eine Phishing-E-Mail als neue Nachricht, nicht als Teil einer laufenden Antwortkette.

Bei einem Reply-Chain Phishing Angriff verwenden Kriminelle zuvor gestohlene legitime E-Mail-Adresse, um eine E-Mail-Antwort mit einem bösartigen Link oder QR-Code zu senden. Diese E-Mail-Adresse gehört zu den Beteiligten einer E-Mail-Konversation. Somit kann der Hacker von einer E-Mail-Adresse aus mailen, welche die anderen Empfänger kennen und der sie vertrauen. Ausserdem haben die Kriminellen den Vorteil, dass sie die Kette der Antworten mitlesen können. So können sie eine äusserst passende Antwort verfassen. Diese Punkte unterstützen die Glaubwürdigkeit der Antwort. Infolgedessen glaubt der Empfänger, dass die Antwort von einem vertrauenswürdigen Absender stammt, und die Zielperson ist eher geneigt, auf den Link zu klicken oder den Anhang zu öffnen, welchen die Kriminellen über das gestohlene E-Mail-Konto einschleusen.

Folgende Massnahmen können das Risiko für einen Reply-Chain Phishing Angriff verringern:

- Verwenden Sie starke Passwörter und speichern Sie diese an einem sicheren Ort, z.B. in einem Password-Manager, ab. Damit machen Sie es Kriminellen schwerer, an ihr E-Mail-Konto zu gelangen.
- Verwenden Sie einen Link, der per E-Mail oder Kurznachricht zugeschickt oder per QR-Code eingescannt wurde, nur mit grosser Vorsicht.
- Geben Sie nie ihre Zugangsdaten für Ihre Geräte, E-Mail-Konten etc. bekannt.

Weiterführende Informationen zu Phishing finden Sie hier (https://www.ebas.ch/phishing/) .