13.03.2026

Vorsicht vor HTML-Phishing

Aktuell kursiert eine besonders tückische Form von Phishing – das HTML-Phishing. Im Unterschied zu klassischen Phishing-Angriffen befindet sich die gefälschte Login-Seite hierbei direkt in einem HTML-Anhang.

So funktioniert HTML-Phishing

Anders als üblich bei einem Phishing-Angriff enthalten die E-Mails eine HTML-Datei im Anhang. Öffnet man diese Datei, wird im Browser eine professionell gestaltete und sehr glaubwürdig wirkende Webseite angezeigt. Die Nutzerinnen und Nutzer werden aufgefordert, auf dieser ihre Zugangsdaten einzugeben. In Wirklichkeit werden die Daten aber direkt an die Täter übermittelt. Zusätzlich können solche HTML-Dateien Skripte enthalten, die weiteren Schaden auf dem Gerät verursachen.

HTML-Phishing ist besonders gefährlich, weil die Webseite lokal geöffnet wird und in der Browserzeile keine typische Webadresse angezeigt wird. Viele Sicherheitsfilter erkennen HTML-Anhänge nur schwer und das professionelle Erscheinungsbild erhöht die Glaubwürdigkeit der Nachricht erheblich.

So schützen Sie sich

Seien Sie bei unerwarteten HTML-Anhängen in E-Mails grundsätzlich skeptisch. Zugangsdaten sollten nur auf bekannten, sicheren Webseiten eingegeben werden. Im Zweifel empfiehlt es sich, die Echtheit einer Nachricht über offizielle Kontaktwege zu überprüfen.

HTML-Phishing ist eine Weiterentwicklung klassischer Phishing-Angriffe, die durch die Kombination aus visueller Authentizität und psychologischem Druck besonders tückisch ist. Aufmerksamkeit, Vorsicht und konsequentes Handeln sind die wichtigsten Mittel, um solche Angriffe zu unterbinden.

Weitere Informationen, auch zu anderen Phishing-Varianten, finden Sie hier (https://www.ebas.ch/phishing) .