CSBW
CYBER
SICHERHEITS
AGENTUR
BADEN-WÜRTTEMBERG

Betrug durch Spoofing

Derzeit häufen sich Angriffe, bei denen Kriminelle gefälschte E-Mail-Adressen und Telefonnummern einsetzen. Indem sie sich als eine Ihnen bekannte oder seriöse Person ausgeben und vertraute oder leicht veränderte Daten nutzen, wollen sie an sensible Informationen gelangen.

SPOOFING
bezeichnet die **Manipulation** oder **Verschleierung der Identität** des Angreifenden.

Dabei setzen die Angreifenden auf das sogenannte **Social Engineering** und nutzen z. B. das Vertrauen oder die Angst von Menschen aus.

Beim **Spoofing via Telefon (Call-ID-Spoofing)** täuschen die Angreifenden mithilfe bestimmter Techniken einen Anruf von einer bestehenden und dem Opfer meist bekannten Telefonnummer vor. Hierdurch ist der Betrug zunächst nur schwer zu erkennen. Die Legitimität eines Anrufs kann mit geringem Aufwand geprüft werden: Bei einem Rückruf der angezeigten Telefonnummer wird die eigentliche Nummer erreicht, da die eigentliche Verbindung nicht kompromittiert ist.[1]

Beim **Spoofing via E-Mail** erfolgt der Angriff über **gefälschte Absende-E-Mail-Adressen**, die den echten E-Mail-Adressen zum Verwechseln ähnlich sehen. So täuschen sie ebenfalls eine andere Person oder Institution als Absender vor.

Allgemeine Handlungsempfehlungen:[1]

- Geben Sie zweifelhaften Aufforderungen nach sensiblen und persönlichen Daten weder per E-Mail noch per Anruf nach.
- Beenden Sie im Verdachtsfall schnellstmöglich die Kommunikation.
- Sollten Sie unsicher sein, rufen Sie über eine Ihnen bekannte oder offizielle Nummer zurück.
- Melden Sie im beruflichen Kontext eine verdächtige Situation immer Ihrem zuständigen Informationssicherheitsbeauftragten (ISB).

Betrug durch Spoofing

Administrative Handlungsempfehlungen, um E-Mail-Spoofing zu verhindern:

Verwenden Sie eine **E-Mail-Authentifizierung**, um Spoofing Ihrer eigenen E-Mail-Adressen zu verhindern. Eine E-Mail-Authentifizierung prüft, ob E-Mails von einem legitimen Absender stammen.[2]

- Hierzu wird die Nutzung des sog. **Sender Policy Framework (SPF)** empfohlen. Mit dieser Methode können empfangende Mailserver automatisiert überprüfen, ob der absendende Mailserver autorisiert ist, im Namen einer Domain (@xy.de) E-Mails zu versenden. Hier findet eine Überprüfung der **Absender-Adresse (Feld Von:)** statt.

- Ergänzend zum SPF empfiehlt sich die Verwendung von **DomainKeys Identified Mail (DKIM)**. Diese technischen Prüfkriterien betrachten neben der Von-Adresse auch den Absender und den Inhalt der E-Mails auf Integrität und stellen sicher, dass die Inhalte der E-Mails nicht manipuliert sind. E-Mails, die den Authentifizierungsrichtlinien nicht entsprechen, können als Spam markiert werden.

- Durch die Erstellung von **Domain-based Message Authentication, Reporting and Conformance (DMARC)**-Regeln wird festgelegt, wie Empfänger-Adressen mit den Ergebnissen der DKIM- und SPF-Prüfungen umgehen sollen.

Weitere Informationen zur Einrichtung von SPF und DKIM erhalten Sie in ausführlichen Anleitungen im Internet oder bei Ihrem Domainanbieter.

Generell können technische Maßnahmen ein gesundes Maß an Misstrauen nicht ersetzen.

Quellen:

[1] BSI - Betrug durch gefälschte Telefonnummern und E-Mail-Adressen (bund.de)

[2] https://learn.microsoft.com/de-de/microsoft-365/security/office-365-security/email-authentication-about?view=o365-worldwide

CSBW CYBER SICHERHEITS AGENTUR BADEN-WÜRTTEMBERG

Weitere Factsheets und Informationen unter:
www.cybersicherheit-bw.de

CSBW Prävention
Kontakt: schulungen@cybersicherheit.bwl.de

Stand: 11.2023