CYBER SAMURAI

KENNEN SIE SPOOFING?

UND WISSEN SIE, WIE SIE SICH DAVOR SCHÜTZEN KÖNNEN?

IN DER IT-SICHERHEIT STEHT SPOOFING FÜR DAS VERSCHLEIERN DER EIGENEN IDENTITÄT ODER DAS VORTÄUSCHEN EINER FREMDEN IDENTITÄT, UM SICH ZUGANG ZU VERTRAULICHEN INFORMATIONEN UND FREMDEN SYSTEMEN ZU VERSCHAFFEN ODER GELD ZU ERBEUTEN. KRIMINELLE NUTZEN DIE IDENTITÄT VON VERTRAUTEN PERSONEN ODER BEKANNTEN ORGANISATIONEN, UM SICH DAS VERTRAUEN DER OPFER ZU ERSCHLEICHEN.

BEISPIELE VON SPOOFING

E-MAIL-SPOOFING

Beim E-Mail-Spoofing verwendet der Kriminelle eine E-Mail-Adresse, die der Zielperson vertraut ist. Die E-Mail kann z.B. vermeintlich von einem Kollegen, Familienmitglied oder einer bekannten Organisation stammen und zu einer Handlung auffordern. Manche Spoofing-E-Mails enthalten Anhänge, in den Viren oder Trojaner versteckt sind. Durch das Vortäuschen einer bekannten Identität erhöht sich die Wahrscheinlichkeit, dass der Empfänger die Handlung ausführt, weil er dem vermeintlichen Absender vertraut.

CALLER-ID-SPOOFING

Beim Caller-ID-Spoofing nehmen die Täter telefonisch Kontakt mit ihrem Opfer auf. Sie rufen unter einer unauffälligen Rufnummer an, z.B. mit einer lokalen Vorwahlnummer, der Rufnummer einer Behörde oder Autoritätsstelle wie der Polizei. Im Gespräch versuchen sie ihre Opfer dann zur Herausgabe von vertraulichen Daten oder zum Tätigen einer Überweisung zu bewegen. Dank neuester KI-Technologie können auch Stimmen vertrauter Personen imitiert werden. Eine besonders heimtückische Methode.

BEISPIEL FÜR EINE SPOOFING-ATTACKE

Ein Beispiel für E-Mail-Spoofing ist der sogenannte Chef-Betrug. Dabei gibt sich der Täter als Vorgesetzter aus:
Ein Mitarbeitender in der Finanzabteilung erhält von seinem Vorgesetzten eine E-Mail, in der er von ihm aufgefordert wird, 500.000 Euro an einen Geschäftspartner im Ausland zu überweisen. Da der Vorgesetzte sich gerade auf Geschäftsreise befinde, habe er selbst keinen Zugriff auf die Geschäftskonten. Laut der E-Mail müsse sofort gehandelt werden, denn der Deal mit dem Geschäftspartner drohe zu platzen, wenn das Geld nicht umgehend überwiesen werde. Telefonisch erreichbar sei der Vorgesetzte in den nächsten Stunden nicht, da er gerade an Bord des Flugzeugs gegangen sei. Der pflichtbewusste Mitarbeitende kommt der Aufforderung des Chefs nach, da sich für ihn alles plausibel anhört und er nicht für einen geplatzten Deal verantwortlich sein möchte. Er überweist das Geld an die angegebene Kontonummer. Die Falle schnappt zu.

SO SCHÜTZEN SIE SICH VOR SPOOFING

Je nach Art des Angriffs gibt es verschiedene Möglichkeiten, um Spoofing zu entlarven. Achten Sie bei einer Kontaktaufnahme auf Ihr Bauchgefühl. Sobald Ihnen etwas seltsam vorkommt, ist Vorsicht besser als Nachsicht.

- ✓ Prüfen Sie stets die E-Mail-Adresse des Absenders. Wenn Sie sich unsicher sind, klicken Sie nicht auf beigefügte Links und öffnen Sie keine Anhänge.
- ✓ Bleiben Sie auch bei telefonischen Anfragen achtsam, vor allem wenn es um zeitkritische Handlungsaufforderungen geht.
- ✓ Nehmen Sie über einen anderen Kanal Kontakt zu der bekannten Person auf und versichern Sie sich, dass die Anfrage echt ist, bevor Sie einer Handlungsaufforderung nachkommen.
- ✓ Lassen Sie sich nicht unter Druck setzen und bewahren Sie Ruhe.

Bleiben Sie wachsam! Weitere Informationen finden Sie unter
https://cyber-samurai.net
oder schreiben Sie uns an info@cyber-samurai.net.

Das Team von Cyber Samurai wünscht Ihnen frohe Weihnachten und einen guten Rutsch ins Neue Jahr.

CYBER SAMURAI

CYBER SAMURAI GMBH
BRAHMSSTRASSE 9
85591 VATTERSTETTEN