



Smishing – Kurznachricht mit Langzeitschaden

2. März 2021 | Beatrice Kübli

Da die digitale Kommunikation immer mehr via Smartphone und Messenger-Dienste stattfindet, versuchen Betrüger*innen nun, ihre Opfer über Kurznachrichten (SMS, Whatsapp etc.) in die Falle zu locken. Smishing heisst das neue Vorgehen, eine Wortmischung aus SMS und Phishing.

Das Smishing-Vorgehen

Sie erhalten per SMS oder über einen anderen Kurznachrichtendienst eine Information, die eine Reaktion erfordert. Häufig bleibt scheinbar nur wenig Zeit, um zu reagieren, oder man muss mit unangenehmen Konsequenzen rechnen, wenn man nichts tut. Die Inhalte der Nachrichten sind glaubwürdig, zum Beispiel:

- eine Sendungsankündigung der Post,
- ein Paket, das wegen fehlendem Porto blockiert ist,
- ein von einem Kontakt versehentlich verschickter Code,
- eine verpasste Mitteilung,
- ein Wettbewerb mit tollen Preisen.

Der/die Empfänger*in wird aufgefordert, auf einen Link zu klicken, eine SMS an eine bestimmte Nummer zu schicken oder auf eine SMS zu antworten.

Die Konsequenzen eines Smishing-Angriffs

Kommt man der Aufforderung nach, kann dies unterschiedliche Aktionen auslösen:

- ein Abo wird abgeschlossen, z.B. wenn man mit «Ja» auf eine SMS reagieren soll.
- Zahlungsdaten werden missbraucht, z.B. wenn man seine Apple-ID eingeben muss, um eine scheinbar dringende App zu laden, oder wenn ein Link auf eine gefälschte Zahlungsseite führt.

- Ein Account wird gehackt, z. B. wenn man einen Code an einen vermeintlichen Kollegen weiterleitet. In Wahrheit handelt es sich hierbei um den Bestätigungscode, dass ein Account (z. B. WhatsApp) zurückgesetzt werden soll. Die Betrüger*innen setzen ein neues Passwort und übernehmen die Kontrolle.
- Schadsoftware wird installiert, z. B. indem man auf einen Link klickt.

Vertrauen und fehlende Kontrolle werden ausgenutzt

Die Betrügerinnen und Betrüger profitieren davon, dass man einer SMS eher vertraut als einer E-Mail und sie auch eher beantwortet. Viele sind sich der Gefahr von Links in E-Mails bewusst und agieren hier entsprechend vorsichtig. Eine SMS hingegen wird als persönlich und vertrauenswürdig wahrgenommen. Zudem dürfen SMS bisher nicht auf den Inhalt geprüft werden. Während E-Mail-Anbieter und Mailprogramme Phishing-E-Mails ausfiltern, fehlt den Fernmeldediensteanbietern dazu die gesetzliche Grundlage. Eine Analyse der Inhalte würde gegen das Fernmeldegeheimnis verstossen. Hinzu kommt, dass die wenigsten auf ihrem Smartphone einen Virenschutz oder eine Antispamsoftware installiert haben. Das ist insbesondere bei Android-Geräten wichtig. iPhones sind durch das geschlossene Apple-System besser geschützt.

Wie schütze ich mich vor Smishing?

- **Fragen Sie bei zweifelhaften Nachrichten** auf anderen, offiziellen Kanälen nach! Rufen Sie die Post, Ihren Kollegen etc. an oder schreiben Sie eine E-Mail an eine offizielle Adresse! Verwenden Sie dazu aber NICHT die Angaben aus der SMS!
- **Öffnen Sie keine Dokumente** bzw. klicken Sie auf keine Links, wenn Sie dem Absender nicht zu 100% vertrauen können!
- **Achten Sie auf Unstimmigkeiten!** Würde ein/e Bekannte/r Sie so anschreiben? Entspricht die Aufforderung dem üblichen Vorgehen? Es ist beispielsweise nicht normal, dass für eine Gewinnübergabe eine Bezahlung geleistet werden muss.
- **Googeln Sie die Anfrage**, um zu sehen, ob andere sie bereits als Betrug identifiziert haben.
- **Löschen Sie die Nachricht!**
- **Installieren Sie einen Virenschutz** auf Ihrem Android-Smartphone und eine Antispamsoftware!
- **Machen Sie regelmässig Updates** der Software auf Ihrem Smartphone!

Die Schweizerische Kriminalprävention (SKP) ist eine interkantonale Fachstelle im Bereich Prävention von Kriminalität und Kriminalitätsfurcht. Sie wird von der Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) getragen. Zu den wichtigsten Aufgaben der Schweizerischen Kriminalprävention gehören die Stärkung der interkantonalen Polizeizusammenarbeit im Bereich Kriminalprävention und die Aufklärung der Bevölkerung über kriminelle Phänomene, Präventionsmöglichkeiten und Hilfsangebote.