Perseus Schadenbeispiel

Smishing-Angriff auf Cloud-Anbieter

Was ist passiert?

Der US-basierte Cloud-Kommunikationsdienstleister Twilio wurde Opfer eines SMS-Phishing-Angriffs. Die Textnachrichten, die die Mitarbeitenden erhielten, stammten vermeintlich aus der IT-Abteilung des Unternehmens und enthielten diverse dringende Handlungsaufforderungen. Über die SMS wurde die Belegschaft dazu aufgefordert, auf einen Link zu klicken, der sie auf eine gefälschte Anmeldeseite des Unternehmens führte. Die Angreifer konnten sich so mit den gestohlenen Login-Daten Zugriff auf interne Server verschaffen, wodurch sie eine bestimmte Anzahl an sensiblen Kundeninformationen abgreifen konnten. Twilio leitete direkt nach Bekanntwerden der Cyberattacke Maßnahmen ein, um die Täter aus den Systemen auszuschließen und Schadensbegrenzung zu betreiben.

Das wurde richtig gemacht!

- Das Incident-Response Management, um Schäden so gering wie möglich zu halten.
- Die Kooperation mit externen forensischen Dienstleistern, Strafverfolgungsbehörden und weiteren betroffenen Unternehmen, da die interne Expertise derartigen Ereignissen nicht gewachsen ist.
- Eine Schritt-für-Schritt-Analyse der Geschehnisse, um Ursache und Schwachstelle zu identifizieren und zu schließen.
- Die transparente Unternehmenskommunikation mit der Öffentlichkeit über die eigene Webiste, um das Vertrauen wiederherzustellen und den Raum für Spekulation so gering wie möglich zu halten.
- Die umgehende Inkenntnissetzung der betroffenen Kunden sowie die entsprechenden Handlungsempfehlungen, um die entstanden Schäden auf Kundenseite zu minimieren und eine vertrauensvolle Beziehung aufrechtzuerhalten.

Das hätte besser sein können!

Investitionen in den Faktor Mensch

- Präventive Maßnahmen
- Mitarbeitersensibilisierungen
- Phishing-Training
- Gefahrenwarnungen zu neuen Angriffsmethoden

Valentin Savulescu

Team Lead Incident Response Management

Das sagt der Experte!

In dem vorliegenden Beispiel konnte der Cyberangriff nur erfolgreich sein, weil menschliches Fehlverhalten es den kriminellen Hackern ermöglichte, bestehende Sicherheitsvorhekehrungen zu umgehen und somit Zugang zu internen Systemen zu erhalten. Hätten die Mitarbeitenden ausfühliche Schulungen zum Umgang mit Phishing erhalten, diese internalisiert und sich entsprechend verhalten, hätte die Cyberattacke abgewehrt werden können. Es ist unabdingbar, dass bewusstseinsbildende Maßnahmen ein Teil der Cyberabwehr eines jeden Unternehmens sind, denn der Mensch steht in der Cybersicherheitsstrategie an erster Stelle.

Wir sind für Sie rund um die Uhr da - auch im Verdachtsfall. ☎ **+49 30 233 2730 95**