Hacker-Angriff auf Telefonanlage

Mit der Umstellung auf die modernere Technologie All-IP wird das Telefon immer öfter zum Tatort. Hacker nutzen dabei zahlreiche Angriffsmuster und richten Schäden in Milliardenhöhe an. Sie dringen in die Telefonanlage ein und verursachen durch Anrufe weltweit oder an kostenpflichtige Rufnummern Schäden, die häufig erst bei der nächsten Telefonrechnung bemerkt werden.

Der konkrete Fall aus 2020

Unser Kunde, eine Niederlassung eines mittelständischen Logistikunternehmens in Europa, ist wiederrum Kunde eines Telefonserviceanbieters, wobei jede Niederlassung eine separate monatliche Telefonrechnung erhält. Die interne Revision bemerkte, dass der in Rechnung gestellte Eurobetrag einer monatlichen Telefonrechnung einer in Deutschland gelegenen Niederlassung statt der üblichen 1.900 Euro netto im Monatswechsel auf 19.500 Euro anstieg. Aufgrund der bestehenden Einzugsermächtigung wurde dieser Betrag durch den Telefonserviceanbieter abgebucht. Bei der Überprüfung der Einzelgesprächsaufstellung fiel auf, dass als Zielland für die geführten Telefonate der afrikanische Kontinent dokumentiert war. Allerdings bestanden mit dem afrikanischen Kontinent keine direkten Geschäftsbeziehungen. Die IT-Abteilung unseres Kunden startete interne Recherchen und überprüfte die Hardware der gesamten Telefonanlage des Konzerns innerhalb der europäischen Niederlassungen. Bei dieser Untersuchung wurden einige technische Ungereimtheiten festgestellt.

Für den Kunden verursachte der Kontrollverlust über seine eigene Telefon-Infrastruktur massive Kosten. Zu den monetären Schäden kommen natürlich noch die internen Aufwände wie Erkennung, Aufklärung und Lösung.

Das Unternehmen verfügt nach vollständiger Realisierung eines afm Risikoplans über eine spezielle Cyberversicherung, die auch forensische Dienstleistung mit einschließt. Der Kunde hat diese Versicherung erst gegen nicht unerheblichen internen Widerstand aus dessen IT-Abteilung und Geschäftsleitung abgeschlossen.

Zurück zum Schadenfall: In kürzester Zeit konnten wir Kontakt zwischen dem Softwarehersteller und den Experten einem der führenden Beratungshäuser für Security und IT-Management (Partner der Cyberversicherung) herstellen. Die Recherchen ergaben eine Sicherheitslücke auf einem der im Einsatz befindlichen Router. Die Funktion, Updates automatisch herunterzuladen, war offensichtlich bei einigen Routern nicht aktiviert gewesen. Es blieb offen, ob es sich bei der Ursache um menschliches Versagen handelte. Bedingt durch diese Sicherheitslücken konnten sich interessierte Hacker der Telefonanlage des Kunden bemächtigen und über einen Monat lang unbemerkt von dessen Telefonanlage auf Kosten des Unternehmens weltweit Telefonate führen.

Wer für die Installation der sogenannten Patches verantwortlich gewesen sei, konnte letzten Endes durch das Logistikunternehmen und den Hersteller dieser Router nicht eindeutig geklärt werden. Jedoch konnten die Sicherheitslücken schnell durch das Aufspielen der Patches in den Routern geschlossen werden und die automatische Downloadfunktion für Updates wurde wieder dauerhaft aktiviert.

Die bestehende Cyberversicherung übernahm die Kosten für die forensische Dienstleistung, die zur Schließung des Risikos geführt hat. Auch die entstandenen erhöhten Telefonkosten, welche die Folge einer durch eine IT-Sicherheitsverletzungsbedingten Kaperung einer Telefonanlage entstanden sind, wurden für unseren Kunden ersetzt. Die zum Abschlusszeitpunkt bestehenden Vorbehalte einzelner Instanzen des Kunden gegen den Nutzen einer Cyberversicherung sind nachhaltig überwunden.