Gebührenbetrug durch Missbrauch von Voicemailsystemen in TK Systemen

Das Umfeld:

Mit dem Leistungsmerkmal Fernkonfiguration (remote customization) haben Sie die Möglichkeit mit einem ankommenden Gespräch in das TK-System, über Ihren Persönlichen Assistenten eine Rufumleitung zu einem externen Ziel zu ermöglichen bzw. ein externes Ziel zu definieren.
Der ankommende Anrufer muss genau den Ablauf der Fernkonfiguration und des Persönlichen Assistenten kennen. (In diesem Fall führt das TK System den Anrufer nicht mit Sprachanweisungen durch die einzelnen Konfigurationsschritte).
Der Anrufer muss die interne Rufnummer und das geänderte und vom Nutzer festgelegte Passwort des entsprechenden Teilnehmerapparates kennen.
Das heißt, wenn der Persönliche Assistent bei einem Teilnehmer aktiviert ist, wird ein ankommendes Gespräch zu diesem konfigurierten fernen Ziel weitergeleitet

Der Missbrauch:

Unbekannte Täter nutzen die Voice-Mailboxen von Unternehmen dazu, Verbindungen zu ausländischen Diensteanbietern herzustellen mit dem Ziel, enorme Verbindungsentgelte zu Lasten des betroffenen Unternehmens auszulösen.
Unbefugte versuchen auf eine Mailbox zuzugreifen und über die Vertreterfunktion oder die Automatische Vermittlung der Mailbox teure Telefonate auf Kosten der Kunden zu führen.
Dieser Missbrauch ist möglich weil Kunden, die voreingestellte Codenummer der Mailboxen nicht geändert haben, obwohl in der Bedienungsanleitung und bei der Kundeneinweisung ausdrücklich darauf hingewiesen wird.

Benutzer Passwortregeln:

Die Autorisierungskontrolle für die Programmierung und Aktivierung von Rufumleitungen durch Dritte oder einer automatischen Weitervermittlung mit dem persönlichen Assistenten zu externen Zielen ist bei erlaubten Konfigurationen zur Nutzung dieser Leistungsmerkmale ein geändertes Teilnehmerpasswort.
In den meisten TK Systemen wird ein 4-stelliges numerisches Teilnehmerpasswort vergeben, welches 10.000 mögliche Kombinationen bietet.
(Dies sind genauso viele Kombinationen, wie bei einer Kreditkarte)
Dieses Teilnehmerpasswort stellt somit ein Sicherheitsmerkmal des TK-Systems dar.
Die Festlegung des Passwortes und die durch das verwendete Passwort erreichte Sicherheit obliegen somit der Verantwortung des Benutzers, bei erstmaliger Festlegung eines Teilnehmerpasswortes durch einen Systemadministrator oder Monteur der Verantwortung durch diesen Personenkreis.
Jeder anrufende konfigurierende Benutzer des Persönlichen Assistenten und jeder anrufende Benutzer des Leistungsmerkmals DISA Transit (remote Substitution) benötigt ein gültiges Passwort, welches den Anrufer auch als bevollmächtigten Nutzer autorisiert.
Wenn der Sprachspeicher eines Teilnehmers am TK System initialisiert wird, muss ein neues Nutzerpasswort festgelegt werden. Folgende Punkte sind Empfehlungen für eine erfolgreiche Passwort Festlegung:

- Einführen von Firmenregeln bezüglich regelmäßiger Aktualisierung aller Benutzer-Passwörter.
- Vermeiden einfacher Passwörter wie 1234, 9876, 1111, 0000, usw.
- Vermeiden weitläufig bekannter Passwörter wie 4711, 0815, usw.
- Vermeiden Sie für mehrere Teilnehmer verwendete einheitliche Passwörter
- Geben Sie das Passwort nicht an Dritte weiter
- Aktivieren Sie die Apparatesperre, wenn Sie längere Zeit abwesend sind (Urlaub, Wochenende, Nachtstunden,….)

Konsequenz:

Die Verantwortung für Schäden aus der Nichteinhaltung dieser Regel liegt beim Kunden.
Attacken dieser Art werden weltweit und Anlagenhersteller-übergreifend beobachtet.
Allein bei der Deutschen Telekom, gehen derzeit 20-30 Beschwerdefälle pro Woche zu Gebührenbetrug ein.
Helfen Sie mit, nicht die Opfer der nächsten Woche zu werden.
Bei Fragen oder Unklarheiten sprechen sie mit Ihrem technischen Betreuer.