Niedersächsisches Ministerium
für Inneres und Sport

Wirtschaftsschutz - *Info*

Hannover im Oktober 2013

Sehr geehrte Damen und Herren,

schlecht gewartete Telefonanlagen stellen zunehmend ein Sicherheitsrisiko dar.

Der Wirtschaftsschutz Niedersachsen weist seit längerem auch auf die Gefahren durch Telefonanlagenmanipulationen hin. Verstärkte Rückmeldungen aus den Unternehmen veranlassen uns, Ihnen einen aktuellen Fall zum Themenfeld Telefonanlagen-Hacking durch Manipulation der TK-Anlagensoftware näher zu bringen, der dem niedersächsischen Wirtschaftsschutz gemeldet wurde.

Es zeigt sich hier, wie wichtig es ist, nicht nur die reine Firmen-IT im Fokus der Sicherheitsbestrebungen zu haben.

Für Rückfragen zu diesem Thema stehen wir jederzeit gerne zur Verfügung, wobei das Angebot des Wirtschaftsschutzes zu individuellen und vertraulichen Gesprächen unberührt bleibt.

Ihr Wirtschaftsschutz-Team

Niedersächsisches Ministerium für Inneres und Sport
Referat 55 - Wirtschaftsschutz

Postfach 4420
30044 Hannover
Tel.: 0511 / 6709-247 oder -248
Email: wirtschaftsschutz@verfassungsschutz.niedersachsen.de

Falldarstellung

Ein mittelständisches Unternehmen aus dem produzierenden Gewerbe betreibt eine größere Telefonanlage mit 200 Nebenstellen. An allen Nebenstellen ist die Komfortfunktion Voicemail (Anrufbeantworter) aktiviert. Nach einem langen Wochenende, während dessen der Betrieb ruhte, entstanden unerwartet Telefonkosten in Höhe von mehr als 10.000 €. Unbekannte Täter hatten die Telefonanlage des Unternehmens offensichtlich übernommen und für ihre kriminellen Zwecke missbraucht, indem sie Auslandstelefonate über die Unternehmens-TK vermittelten. Trotz dieser belegten Tatsache ist das Unternehmen zur Zahlung der entstandenen Kosten an den Telekommunikationsanbieter verpflichtet.

In dieser Situation wurde der Wirtschaftsschutz, neben der polizeilichen Bearbeitung des Sachverhaltes, um Hilfe und Unterstützung gebeten.

Folgende Hintergründe sollten Sie kennen:

Die Hacker gehen in der Regel nach der gleichen Methode vor: Sie suchen nach Unternehmen, deren Telefonanlage sogenannte integrierte Voicemail-Funktionen besitzen, also einen Anrufbeantworter für jeden Anschluss. Da viele Besitzer solcher Anlagen die Standard-PIN der Anrufbeantworter nicht ändern, diese PINs gleichzeitig aber im Netz kursieren, sind sie wie eine offene Tür. Über das Gerät haben die Hacker Zugriff auf das Telefonsystem, können die PIN ändern, Anrufweiterleitungen einrichten und danach aus der Ferne über diese Anlage telefonieren. Zumindest bis das Unternehmen die nächste Telefonrechnung bekommt und den Betrug entdeckt.

Diese Angriffsmethode ist verstärkt seit 2011 im gesamten Bundesgebiet zu beobachten und wird nach wie vor erfolgreich eingesetzt.

Um sich vor Hacker-Angriffen auf TK-Anlagen und den damit verbundenen Schäden zu schützen, sollten folgende Maßnahmen erfolgen:

1. Update der Anlagensoftware auf die neuste Version des Herstellers. (insbesondere Zugangssperre nach Fehlversuch)

2. Ändern des Standard-Passwortes aller Mailboxen – Dies muss vom Anwender selbst vorgenommen werden. Keine einfachen Zahlenkombinationen wie z.B. 0000, 1111, 1234 oder die Durchwahlnummer des Anschlusses verwenden.

3. Ratsam ist ebenfalls die Standardansagen der Mailboxen zu ändern, da die Betrüger anhand der Ansage auf TK-Anlagen Typen- und Versionsrückschlüsse ziehen können, um so per Bedienungsanleitung die Standardpasswörter auszuprobieren.

4. Alternativ abschalten der Mailbox.

5. Deaktivieren der Rufumleitung extern.

6. Anpassung der Rufnummernsperre für das Ausland.

7. Bei einem Fernwartungszugang überprüfen und ändern sie ggf. ebenfalls die Zugangsdaten.

Beachten Sie das ein Mehr an Komfortfunktionen immer ein Weniger an Sicherheit ist.