INFORMATIONEN

informationen

Sicherheit für außen liegende Nebenstellen

Außen liegende Nebenstellen erfreuen sich immer größerer Beliebtheit – leider auch bei Hackern. Diese Gefahren müssen besonders bei Nebenstellen berücksichtigt werden, die nicht mittels VPN-Tunnel an das ITK-System angebunden sind.
Sie werden meist über dynamische DNS-Dienste und Portfreigaben in den Routern direkt mit dem ITK-System verbunden.

Einigen Hackern ist es bereits gelungen, sich in die Systeme verschiedener Hersteller einzuloggen und kostenpflichtige Gespräche, meist ins entfernte Ausland, zu führen.

Nehmen Sie die folgenden Hinweise nicht auf die „leichte Schulter". Fremdzugriffe auf ITK-Systeme häufen sich und die dabei entstehenden Kosten bewegen sich sehr schnell in einen 4- bis 5-stelligen Euro-Bereich. Bemerken werden Sie es aber erst mit der nächsten Abrechnung des Telefonanbieters.

Wie gehen die „Bösewichte" vor?

Zunächst versuchen sie, über Server automatisiert, die URL oder IP-Adresse des Anschlusses zu ermitteln. Hier gibt es sogar Dienstleister im Internet, bei denen man einfach nach bestimmten Begriffen suchen lassen kann und die passenden öffentlichen IP-Adressen von unbedarften Kunden als Liste erhält. Nun scannen sie die IP-Adressen nach den Standard-SIP-Ports (z. B. 5060). Ist der Scan aus deren Sicht erfolgreich, werden verschiedene Benutzernamen und Passwörter solange probiert, bis die richtigen Kombinationen gefunden sind. Danach wird z. B. eine Servicenummer in Übersee angerufen. Ist der Anruf erfolgreich, wird dieser Zugang für weitere, sehr kostspielige Telefonate genutzt.

Wie können Sie sich schützen?

Grundsätzlich sind beim Einsatz außen liegender, über VoIP angebundener Nebenstellen VPN-Tunnel vorzuziehen. Sie bieten ausreichend Sicherheit.

Wichtig: Jedes Öffnen eines Ports auf dem NAT-Router stellt eine Gefahr dar. Daher sind zusätzliche Maßnahmen zu Ihrem Schutz unumgänglich.

1. **Auswahl der Benutzernamen und PINs (Passwörter)**

   Verwenden Sie niemals Standard-PINs aus dem Auslieferzustand. Vermeiden Sie Geburtstage bzw. Datumsangaben als PINs. Sie vereinfachen es dem Angreifer die Richtige zu finden. Auch einfach zu ratende PINs wie 111111 oder 123456 sollten niemals verwendet werden.

   Möchten Sie auch das Webinterface des ITK-Systems aus dem Internet erreichen (via http oder besser https), dann sollten Sie auch den Benutzernamen des Administrators (admin) ändern.

   Vergeben Sie für jeden Benutzer eine separate PIN!

2. **Einrichten von Amtberechtigungen und Sperrwerke**

   Richten Sie für die außen liegenden Nebenstellen eine reduzierte Amtberechtigung und ein Sperrwerk ein. Die Amtberechtigung kann auf den Telefontarif des eigenen Anschlusses abgestimmt sein (z. B. nur nationale Gespräche). Zu Tageszeiten, in denen in der Regel nicht telefoniert wird, z. B. nachts bzw. außerhalb der Geschäftszeiten, kann die Amtberechtigung auf ein Minimum reduziert werden.

   Das Sperrwerk sollte zusätzlich die Vorwahlen von Mehrwertdiensten und ggf. Mobilfunknetzen beinhalten (z. B. 0900, 0180, 0137).

3. **Nicht die Ports 5060 (SIP) und 80 (http) freischalten**

   Wählen Sie andere Ports für die Freischaltung zum ITK-System. Wichtig ist, dass der Port 5060 vom Router in Richtung ITK-System (intern) verwendet wird. Vom Gateway in Richtung Internet (extern) kann ein anderer Port definiert sein.

   Für den Zugriff auf die Weboberfläche kann der Port im ITK-System geändert werden.

4. **Umgang mit Daten zum Anschluss**

   Geben Sie niemals Benutzernamen, PINs und die öffentliche IP-Adresse des ITK-Systems bekannt. Damit sind nicht nur Postings in Foren und Communities gemeint, sondern auch Service-Logs von Routern oder Wireshark-Traces.

5. **Kontrolle**

   Prüfen Sie regelmäßig die Gesprächsdatenerfassung Ihres ITK-Systems und ggf. die LOGs Ihres NAT-Routers auf Unstimmigkeiten.

Wenn Sie alle genannten Punkte beachten, ist Ihre Anlage besser vor Hackerangriffen geschützt.

97241 03 Stand 03/2013

Auerswald GmbH & Co. KG • Vor den Grashöfen 1 • 38162 Cremlingen
Tel. (0 53 06) 92 00-700 • Fax (0 53 06) 92 00-760 • www.auerswald.de