Artikel von Media NRW
ARP-Spoofing-Angriffe auf Voice-over-IP

http://www.media.nrw.de/kurznachrichten/artikel.php?id=3937

Voice over IP abhörsicher

[19.09.2005]

Hagener Unternehmen stellt Sicherheitssoftware vor

ISL | Voice over IP (VoIP) ist wegen der günstigen Kosten und verschiedenen Zusatznutzen ein beliebter Telekommunikationdienst. Allerdings können VoIP-Gespräche leicht von Unbefugten belauscht werden. Eine Sicherheitslösung, die sich speziell an mittelständische Unternehmen und Konzerne mit mehreren Standorten und hoher Kundennähe richtet, hat die ISL Internet Sicherheitslösungen GmbH aus Hagen entwickelt.

Die VoIP-Technologie werde gerne von Unternehmen eingesetzt, die keine zwei internen Netze unterhalten wollen, teilte ISL mit. Bei herkömmlichen analogen und ISDN-Telefonleitungen sei es für Unbefugte gar nicht so einfach, Gespräche mitzuhören, denn

sie müssten einen tatsächlichen physikalischen Zugriff auf die Leitungen haben, um sie abhören zu können. Software, die im Internet verfügbar sei, ermögliche Angriffe auf Netzbereiche, in denen alle Endgeräte eines Bereiches, eines Gebäudes oder in eines ganzen Unternehmens angeschlossen sind. Bei solchen "Man-in-the-middle-Attacken" kann der Ohrenzeuge vertrauliche Gespräche sogar auf seinen Computer laden und eine CD damit brennen. Bei einer "Man-in-the-Middle-Attacke" fälscht ein Angreifer die IP-Adressdaten in den Adressverzeichnissen anderer Teilnehmer-Telefone, um Informationen an sein eigenes IP-Telefon umzuleiten. "Jeder, der VoIP einsetzt, ist kinderleicht angreifbar", teilte ISL-Geschäftsführer Dr.-Ing. Andreas Rieke mit.

Besonders gefährdet seien Unternehmen mit mehreren Standorten. Verzweigte Produktionen und immer engere Kundenbeziehungen würden dafür sorgen, dass die Kommunikation immer umfangreicher, intensiver und vertraulicher werde. Mit der ISL-Software sollen Mithör-Attacken von vornherein nicht mehr möglich sein, teilten die Entwickler mit. Grundlage ist der ARP-Guard eine ISL-Entwicklung für den Datenschutz bei Computern, die auch für VoIP eingesetzt werden kann. Das Gerät mit integrierter Software wird im internen Netz des Unternehmens aufgestellt. Erkennt es einen Angriff, schaltet es den Port des Angreifers einfach ab. Man kann den lokalisierten Angreifer natürlich auch auf frischer Tat ertappen.

"Vor allem für mittelständische Unternehmen mit beispielsweise 100 VoIP-Telefonen kann diese Investition im unteren vierstelligen Bereich eine Überlegung Wert sein, vor allem, wenn sowieso eine neue TK-Anlage angeschafft werden soll", so Andreas Rieke. Intensiv in der Praxis getestet wurde das Gerät vom Universitätsrechenzentrum der FernUniversität in Hagen.