Zeitschrift: LANline Heft: 015 Jahrgang: 2002 Seite: 55

Security-Scanner im Einsatz

Schwachstellenanalyse in konvergenten Netzen

In der Presse häufen sich Meldungen über Viren, Würmer und Angriffe auf Web-Server. Doch viele andere Bereiche wie etwa moderne Telekommunikationseinrichtungen sind ebenfalls gefährdet, und oft widmet man deren Sicherheit zu wenig Aufmerksamkeit. Nachfolgend werden einige typische Schwachstellen aufgezeigt und Möglichkeiten zur Schwachstellenanalyse am Beispiel von so genannten Security-Scannern vorgestellt. Neben einer Interpretation der möglichen Ergebnisse stellt der Autor auch die Grenzen dieser Verfahren dar.

Zurzeit ist der Begriff “Voice over IP” in aller Munde, und viele Hersteller propagieren die Vorteile dieser Technologie. Es erscheint vorteilhaft, klassische Sprachdienste und IT-Kommunikation über ein gemeinsames Medium zu verwenden, doch meistens wird auf den Punkt Sicherheit zu wenig eingegangen. Selbst dann, wenn Web-Server, Mail-Server, Firewall-Systeme und Clients von Angriffen bedroht sind, kann man sich in der Regel auf sein Telefon verlassen. Sollte das Versenden einer E-Mail nicht möglich sein, hat der Anwender immer noch die Option, mit den Kommunikationspartnern per Telefon in Verbindung zu treten. Doch wie sieht es aus, wenn Sprachdaten nur noch per IP verschickt werden, wie schützt man sich vor einem Denial-of-Service-Angriff auf die VoIP-Telefone? Um Sicherheit als Gesamtprozess zu verstehen, muss sich der Administrator zunächst darüber im Klaren sein, dass auch die klassische Telekommunikation Sicherheitsprobleme aufweist.

Sicherheitslücken bei Telekommunikationseinrichtungen

Sicherheitsmaßnahmen, die bei IT-Systemen inzwischen Standard sind wie etwa die automatisierte Überprüfung auf Schwachstellen und die Härtung der Betriebssysteme werden oft bei “klassischen” Telekommunikationseinrichtungen vernachlässigt oder vergessen. Wenn bei einer Telefonanlage das werksseitig eingestellte Kennwort nicht verändert wurde oder sogar die Möglichkeit der Fernwartung noch aktiv ist, stehen einem Angreifer Tür und Tor offen. Fast problemlos kann er – in der Regel unbemerkt – die Anlage entsprechend seinen Wünschen umkonfigurieren, sei es um Anrufe/Daten abzuhören, Faxmitteilungen umzuleiten oder sogar Aufschaltberechtigungen und Raumüberwachungsfunktionen zu nutzen.

Telekommunikationseinrichtungen müssen auch, ähnlich wie Server oder aktive Netzkomponenten, gegen physischen Zugriff gesichert werden. Ist der Zugang zur Anlage geschützt oder hat praktisch jeder Zugriff darauf, der daran vorbeigeht? Heutzutage ist es kein Problem, in kürzester Zeit mit einem Laptop und einem seriellen Kabel die Konfiguration einer beliebigen TK-Anlage zu laden, zu verändern und wieder zu speichern. Auch hier sollte ein entsprechender Schutz durch Kennwörter und eine räumliche Zugangskontrolle gewährleistet sein. Es empfiehlt sich die Unterbringung in einem abschließbaren Server-Raum, der auch die Kriterien zur Klimatisierung und zum Brandschutz erfüllt.

Sicherheitsprobleme bei VoIP

Beim Einsatz von VoIP-Lösungen wird eine gemeinsame Infrastruktur und ein gemeinsames Protokoll (IP) benutzt, sodass mit neuen Angriffsmethoden zu rechnen ist. Dabei muss nicht nur an den Schutz des eigenen Netzwerks vor Angreifern aus dem Internet (Firewall) gedacht werden, auch weitere Lösungen zum Schutz vor internen Angreifern sind notwendig. Verglichen mit dem “Anzapfen” einer Telefonleitung stehen für das Abhören von VoIP viele Standard-Tools zur Verfügung. Mit so genannten “Sniffern” ist man in der Lage, Rechner in Netzsegmenten zu belauschen und deren Daten zu sammeln. Es ist zwar bekannt, dass dies in Switch-basierten Netzen nicht so einfach ist, aber dass dies unmöglich wäre, ist ein Mythos. Sind keine weiteren Sicherheitsmaßnahmen im LAN getroffen worden – und das ist die Regel – so kann sich ein Client beispielsweise durch das Versenden bestimmter Pakete als Switch ausgeben. Selbst eine VLAN-Isolierung hilft meistens an dieser Stelle nicht, da das Endgerät über einen gefälschten Trunk-Port an allen VLANs partizipiert. Dass dies noch einfacher geht, etwa wenn der Administrator die Geräte mit Telnet verwaltet (Klartextpasswörter) oder der SNMP-Zugriff nicht geändert wurde, soll nicht weiter ausgeführt werden. In dem Moment, in dem ein Angreifer die Switches administrieren kann, dürften Überlegungen zu einer ausgereiften VLAN-Struktur überflüssig werden.

Verschlüsselung von Verbindungen

Abhilfe kann die Verschlüsselung von Verbindungen schaffen. Dies wird oft zur Kostenreduzierung bei externen Netzen verwendet (VPN), und diese Verfahren sind inzwischen relativ gut standardisiert und einsetzbar. Durch

diese Techniken lassen sich auch interne Verbindungen schützen. So ist beispielsweise unter Windows 2000 die Einrichtung von internen VPN-Verbindungen recht elegant gelöst. Der Administrator kann vorgegeben, dass bestimmter Verkehr, beispielsweise Zugriffe der Entwicklungsabteilung auf den zentralen Backup-Server, nur verschlüsselt über das Netz erfolgen darf. Prinzipiell lässt sich diese Technik auch bei VoIP-Verbindungen einsetzen, ob aber die VoIP-Hersteller eine solche Funktion unterstützen, ist im Einzelfall zu prüfen. Es sollte des Weiteren beachtet werden, dass für diese Verschlüsselung Rechenleistung erforderlich ist. Ein Client mit aktiven Anwendungen, Hintergrund-Virenscanner und installierter VoIP-Software muss auch für die Verschlüsselung über ausreichende Leistungsreserven verfügen. Eine Verbesserung könnte sich durch die Verwendung des AES (Advanced Encryption Standard) ergeben. Der Hauptgrund für die AES-Initiative des NIST (National Institute of Standards and Technology – Standardisierungsinstanz im Bereich der US-amerikanischen Behörden) ist nicht unbedingt in der (Un-)Sicherheit der derzeit verwendeten Algorithmen zu sehen. Eine Studie von Lenstra und Verheul [1] und eigene Untersuchungen haben ergeben, dass aus kryptologischer Sicht 3DES mit einer effektiven Schlüssellänge von 112 Bit bis mindestens 2020 als sicher betrachtet werden kann. Weitaus wichtiger ist, dass sich der Gewinner der Ausschreibung, der Algorithmus “Rijndael” [2], mit deutlich niedrigerem Ressourcenbedarf implementieren lässt. Dies ist zum einen für PDAs interessant und wäre in Bereichen mit erhöhtem Sicherheitsbedarf auch für IP-Telefone denkbar. Verschiedene Hersteller von VoIP-Lösungen geben auch Empfehlungen zur Implementierung einer sicheren VoIP-Lösung ab. So stellt etwa Cisco in diversen Whitepapers im Rahmen eines “Safe-Framework” Lösungen dazu vor. Das Unternehmen empfiehlt, für VoIP-Komponenten ein eigenes VLAN zu verwenden, das dann über einen Layer-3-Switch/Router kontrolliert mit dem Netzwerk verbunden wird.

Schwachstellenanalyse – Penetrationstests

In letzter Zeit führen die Systemverantwortlichen – motiviert durch die täglichen Meldungen über neue Schwachstellen von Betriebssystemen und Anwendungen – immer öfter so genannte Penetrationstests durch. Kommerzielle Tools wie etwa ISS Internet Scanner, NAI Cybercop, Cisco Secure Scanner und viele Linux-Tools wie beispielsweise Satan, Nessus und Cops ermöglichen das automatische Aufspüren von vorhandenen Schwachstellen. In den Programmen sind Module enthalten, die je nach Einstellung Informationen ausspähen, Schwachstellen aufdecken oder sogar Angriffe simulieren. Der Vorteil dieser Verfahren liegt darin, dass der Administrator zügig Informationen darüber erhält, welche Schwachstellen in Firewall-Systemen, Web-Servern, Servern, Clients und sogar in aktiven Komponenten wie etwa Routern vorhanden sind. Neben einer detaillierten Beschreibung der Schwachstelle werden in der Regel Maßnahmen zur Behebung vorgeschlagen wie die Installation von bestimmten Service-Packs und Hotfixes. Auch kann der Administrator feststellen, welche Dienste zur Verfügung stehen. Oft sind viele Dienste standardmäßig aktiv, obwohl sie für den laufenden Betrieb gar nicht erforderlich sind. In diesen Fällen empfiehlt es sich, diese Dienste zu deaktivieren oder besser komplett zu deinstallieren.

Im Zusammenhang mit der Durchführung eines Penetrationstests sollte man sich darüber im Klaren sein, dass in der Regel nur ein Ausschnitt eines Netzes getestet wird. Eine Überprüfung des gesamten Netzwerks inklusive aller Clients dürfte in der Regel zu teuer (Lizenzkosten) und zu zeitintensiv sein. Man wählt daher meist Bereiche wie beispielsweise die Umgebung der Firewall-Systeme oder Server-Farmen aus. Die Funktion etwa der Firewall lässt sich über das Internet, aber auch vom internen Netz aus und von einzelnen DMZs (Demilitarisierte Zone) heraus testen. Es empfiehlt sich, Zeit für die Planung zu reservieren, um sämtliche Angriffsvariationen durchzuspielen. In der Grafik ist eine mögliche Vorgehensweise dargestellt. In einem ersten Scan-Vorgang werden vom Internet aus mögliche Schwachstellen der Firewall und der Systeme in der DMZ gesucht. In einem zweiten Test erfolgt die Überprüfung der Firewall und der DMZ vom internen Netz aus, da auch eine Gefährdung durch eigene Mitarbeiter – fahrlässig oder vorsätzlich – möglich ist. Im dritten Teil testet der Systemverantwortliche von einer DMZ aus die Firewall und Zugangsmöglichkeiten zum LAN. Dadurch kann der Fall simuliert werden, dass es einem Angreifer gelungen ist, ein System in der DMZ zu kompromittieren. Die Ergebnisse zeigen, welche weiteren Schäden möglich oder verhindert werden. Um den Prüflauf zu vervollständigen – und dies erfordert oft den meisten Aufwand – überprüft der Administrator die internen Systeme (Clients, Server) auf Schwachstellen. In der Regel geschieht dies nur exemplarisch. Der Systemverwalter überträgt die Ergebnisse anschließend auf identische Systeme.

Grenzen von Penetrationstests

Was durch solch einen Test aber nicht überprüft wird – und auch nicht überprüft werden kann – sind organisatorische Schwachstellen. Erhält der Administrator beispielsweise das Resultat “Web-Server XY weist keine Schwachstellen auf”, so kann dies sein, weil der Verantwortliche letzte Woche Zeit hatte und alle notwendigen Patches installiert wurden. Es ist aber auch möglich, dass ein Prozess definiert ist, der regelmäßige Updates vorsieht und somit die Aktualisierung nicht dem Zufall überlässt. Man erhält also nur ein Ergebnis für einen ganz bestimmten Zeitpunkt. Daraus lässt sich nicht schließen, dass die Ergebnisse auch für andere Zeiten gültig sind. Bei Überprüfungen – speziell über das Internet – werden weitere wichtige Sicherheitsmechanismen nicht gecheckt. Die Ergebnisse zeigen nicht auf, ob etwa der Server in einem abgeschlossenen Server-Raum untergebracht ist, die Kabelführungen geschützt sind, wer Zugang zu den Systemen hat, ob eine USV für Stromausfälle vorsorgt und ob dem Brandschutz ausreichend Aufmerksamkeit gewidmet wurde.

Diese weiteren möglichen Schwachstellen lassen sich nur durch eine Vor-Ort Begehung, Besprechungen mit den

Verantwortlichen und einer Durchsicht der Sicherheitskonzeption erreichen. Daher empfiehlt es sich in der Regel, einen Penetrationstest immer mit einer Sicherheitsanalyse der organisatorischen und physischen Maßnahmen zu kombinieren. Da nur nach bekannten Schwachstellen gesucht wird und die Angriffe von deutlich niedrigerem Niveau als bei einem professionellen Hacker sind, sollte man sich nicht in den Irrglauben führen lassen, dass ein System sicher ist, sobald der Security-Scanner keine Schwachstelle findet. Professionelle Hacker zeichnen sich durch ein hohes Know-how und eine systematische Vorgehensweise aus, oft ergänzt durch Kreativität und Voraussicht. Eine gefundene Lücke wird daher in der Regel nicht öffentlich kundgetan, denn erst wenn die Schwachstelle publik geworden ist, reagieren die Hersteller. Bis dahin kann man aber die Sicherheitslücke ausnutzen, und auch Security-Scanner zeigen diese nicht auf.

Fazit

Wie so oft steht bei der Einführung von neuen Systemen die Kommunikation und die Erweiterung von Anwendungen im Vordergrund. Über die Sicherheit wird dann erst nachrangig nachgedacht oder schlimmer, erst falls ein Sicherheitsbruch bemerkt wurde. Obwohl einige Hersteller, wie etwa Cisco mit ihrem “Safe-Framework” und weiteren Designüberlegungen, Hinweise zur Implementierung von sicheren konvergenten Netzen geben, ist davon auszugehen, dass die Realisierung in der Praxis einiges an Aufwand bedeutet. Konvergente Netze lassen sich sowohl auf IP-Telefonie- als auch auf klassischer IT-Systemebene durch so genannte “Security-Scanner” überprüfen. Bekannte Schwachstellen können aufgedeckt und behoben werden, allerdings sollte der Systemverantwortliche eine solche Maßnahme unbedingt durch eine Analyse der organisatorischen und physischen Sicherungsmechanismen ergänzen. Die Ergebnisse eines Penetrationstests alleine sagen nur etwas über den Stand der Sicherheit zu einem bestimmten Zeitpunkt aus.

(Dipl.-Ing. Stefan Gora/mw)

Literatur:

[1] Lenstra, Verheul: Selecting Crypto-graphic Key Sizes in Commercial Applications, PriceWaterhouseCoopers CCE Quartely Journal Issue 03, 1999

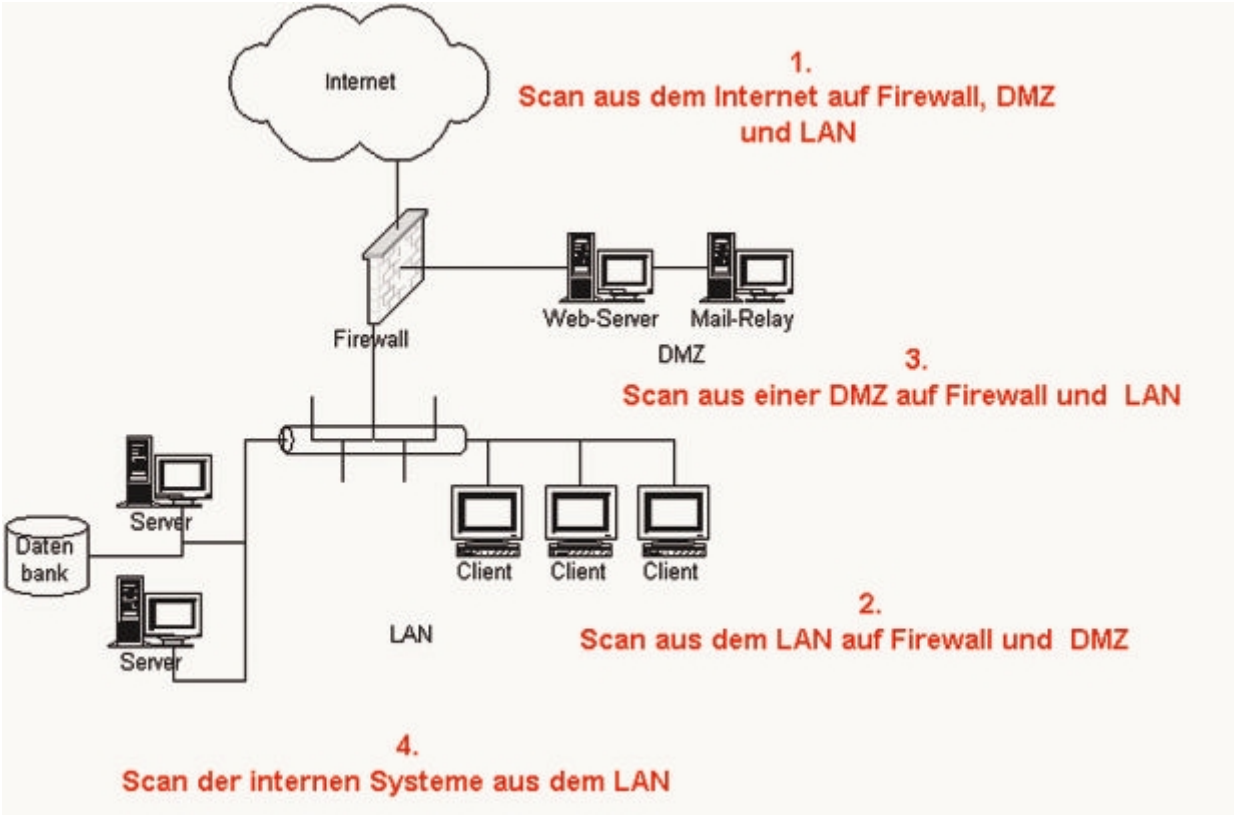
[2] Daemen, Rijmen: Rijndael, the advanced encryption standard, Dr. Dobb’s Journal Vol.~26 No.~3, 2001

http://www.esat.kuleuven.ac.be/~rijmen/rijndael/

Info: Secorvo Security Consulting

Tel.: 0721/6105-500

Web: www.secorvo.de



Überprüfungsmöglichkeiten

voriger Artikel | nächster Artikel | Trefferliste | neue Suche

 Fragen und Anregungen