„Warum eine Firewall für das System i? Es ist doch absolut sicher!“

VON WOLGANG SCHITTKO

Diese Fallstudie zeigt, dass trotz der sehr hohen System i-Security ein großes Sicherheitsrisiko besteht. Bei einer Auditierung der IT-Sicherheit eines internationalen Großkonzerns wurde die INCONSA GmbH als Dienstleister und Ansprechpartner für alle Bereiche der installierten System i Plattformen hinzugezogen. Die Auditoren gingen äußerst detaillierten Fragen nach und legten großen Wert auch auf die einzelnen internen Zugriffsmöglichkeiten.

Eine Firewall auf dem System i?

Im herkömmlichen Sinne ist eine Firewall eine Schutzmaßnahme vor fremden und unberechtigten Verbindungsversuchen aus dem öffentlichen Internet ins lokale Netzwerk.

Jedes Unternehmen wird diese Firewall implementiert haben, aber warum nun eine separate Firewall für das System i? Bei einem Audit eines meiner Kunden im Konzernverbund sind zahlreiche Mängel aufgefallen, die ein hohes Unternehmensrisiko innerhalb aller IT-Lösungen auf System i Plattformen darstellen.

Zwar sind durch die sehr ausgereiften Sicherheitsmechanismen des OS/400 die Lücken schwer zu erkennen, aber in der Auditierung wurde klar, dass durch bewussten oder auch unbewussten, berechtigten oder unberechtigten Datenzugriff interner Mitarbeiter ein hohes Risikopotential besteht.

„IT Dienstleistungen dürfen nicht zufrieden stellen, Sie müssen begeistern.“

Dipl.-Inf. Wolfgang Schittko, Gründer und Geschäftsführer der INCONSA GmbH

Risiko: IT-Kenntnisse der User

Man kann nicht mehr davon ausgehen, dass „heutige“ User keine IT-Kenntnisse haben. Gerade jüngere Mitarbeiter im Unternehmen bringen schon einen sehr großen Erfahrungsschatz im IT-Bereich mit. Sei es vor privatem oder aus beruflichem Hintergrund. So wird zum Beispiel die Konfiguration einer „Fritzbox“ oder eines Heimnetzwerkes mit IP-, FTP, Routing und auch NAS-Raid-Systemen heutzutage nicht mehr von Technikern durchgeführt, sondern in Eigenregie. Dieses Knowhow der User birgt auch Gefahren für die Unternehmens-IT.

Die Sicherheitsrisiken

Hier ein paar Beispiele der Risiken, die im besagten Audit angesprochen wurden und auch in vielen anderen Unternehmen auftreten:

– Zahlreiche User arbeiteten selbständig mit Query. Somit ist es schnell geschehen, dass per Query die Daten im gesamten ERP-System geändert werden. ERP-Dateien können durch inkorrekte Querys gelöscht oder inkonsistent werden. Ein selektiver Zugriff auf User/Lib/File-Ebene konnte nicht garantiert werden.
– Jeder User hatte die Möglichkeit des FTPs. Mit einem einfachen FTP im DOS-Fenster können ebenfalls Daten verändert werden.
– Excel via ODBC oder auch der „Remote Command“ (RMTCMD) war für die User frei zugänglich.
– Schwerwiegend war auch die Tatsache, dass die detaillierte Protokollierung der Zugriffe außerhalb der „normalen Anwendungen“ am Server nicht möglich war.

Es konnten daher nicht alle sicherheitsrelevanten Zugriffe auf das System aufgelistet werden.

Die vollständige Sicherheit

Die sicherste Lösung aller aufgezeigten Probleme ist eine Firewall, die die Autorisierung von System-Zugriffen über die im Betriebssystem definierten Schnittstellen nutzt. Diese sogenannten „Exit Points“ können dann einzeln so parametrisiert werden, dass jede sicherheitsrelevante Zugriffsregel abgebildet werden kann.

„Exit Points“ existieren z.B. für die oben genannten Systemdienste wie FTP, Telnet, SQL, DB, IFS, etc. und jeder erlaubte und unerlaubte Zugriff wird protokolliert. Hinzu kommen die Regeln die auf IP, User, Verb und Objekt definiert werden können.

Erstellung des Regelwerks aus der Protokollierung

Die Konfiguration einer System i Firewall kann einfach und zeitsparend von dieser Protokollanzeige vorgenommen werden, indem von dem Protokolleintrag, (sei es ein erlaubter oder ein unerlaubter Zugriff) automatisch in die dafür zuständigen „Exit Point“-Konfiguration gesprungen wird.

Handelt es sich um einen noch nicht abgesicherten Zugriff so wird durch spezielle Algorithmen eine Regel vorgeschlagen, die nach den Bedürfnissen angepasst werden kann.

Falls es sich um einen schon abgesicherten Zugriff handelt, so wird die für diesen Protokolleintrag zuständige Regel angezeigt und kann geändert werden.

Dadurch hat man die Möglichkeit im Dialog und in Realtime sofort die Sicherheitslücken zu schließen.

Einfache und effiziente Verwaltung der Firewall

Um die Verwaltung der System i Firewall einfach zu gestalten, können User Gruppen, Applikationen oder auch Lokationen jeweils zusammengefasst werden.

Dadurch werden zum Beispiel die Berechtigungen von IT-Mitarbeitern, „Superusern“ und „Usern“ bequem verwaltet.

Auf File-, Library-, Data queue-, Printerfile- und Programmebene kann ebenfalls alles unkompliziert gruppiert und definiert werden.

Einige Wochen später wurde in der Nachaudit bestätigt, dass durch die Installation einer System i Firewall alle sicherheitsrelevanten Mängel behoben wurden.

Die IT-Abwehrkette von Organisationen ist immer nur so stark wie ihr schwächstes Glied – und dieses Glied sind häufig die Mitarbeiter. Die aktuelle Industrienationen-Studie des Ponemon Institutes sagt aus, dass immerhin 30 % der Datenschutzverletzungen auf den sogenannten Human Factor zurückzuführen sind. Diese Zahl erfasst nachlässige Mitarbeiter sowie Geschäftspartner. Bei einer Aufteilung nach Quelle der Schadenskosten wird zwischen kriminellen Angriffen, Systemfehlern und menschlichen Fehlern unterschieden. Hierbei liegen die kriminellen Angriffe zwar deutlich in Führung, doch die menschlichen Fehler kosten fast genauso viel wie Systemfehle r. ♦