von Wayne O. Evans

iSeries (AS/400) Sicherheitsüberprüfungen querbeet durch unterschiedlichste Industriesparten haben immer wieder die gleichen Sicherheitsgefahren ergeben. Im Folgenden werde ich die zehn häufigsten Gefahren beschreiben und Vorschläge unterbreiten, wie Sie Ihre Verwundbarkeit durch entsprechende Angriffe möglichst gering halten.

Bedrohung Nr. 1: Keine effektive Sicherheitsstrategie

Künstler Burgy Zapp

Viele Unternehmen verfügen über keine schriftlich ausgearbeitete Sicherheitsstrategie und auch jene, die eine haben, haben sie oft nur pro forma. Zu häufig kommt es noch vor, dass der Sicherheitsbeauftragte vom Management keine weiteren Vorgaben erhält, als „das System zu sichern“. Das Management würde nie einem Programmierer einfach den Auftrag erteilen, „ein Programm zu schreiben“, ohne ihm zugleich detaillierte Angaben über den gewünschten In- und Output des Programms zu liefern. Genauso wie ein Programmierer exakte Angaben zum Programm benötigt, benötigt der Sicherheitsbeauftragte eine ausformulierte Sicherheitsstrategie, um den Erwartungen des Managements gerecht zu werden. Um effektive Sicherheit der Computersysteme zu gewährleisten, müssen Anwender und Betriebssystem im Interesse des Datenschutzes zusammenwirken. Eine umfassende Sicherheitsstrategie berücksichtigt Mensch und Maschine und sollte insbesondere die folgenden drei Aspekte beinhalten: Eine **High Level Sicherheitspolitik** legt die Führungsprinzipien für das Unternehmen fest. Diese Betriebs-Prinzipien bilden die Basis für detailliertere Richtlinien und Standards. **Benutzerrichtlinien** definieren den menschlichen Bereich des Themas Sicherheit, indem sie die Anwender über akzeptables und erwartetes Verhalten informieren. Diese Richtlinien sollten mehr sein als nur eine Sammlung von Ge- und Verboten, sie sollten dem Anwender einen detaillierten Leitfaden für den Umgang mit dem Computer an die Hand

geben. Anwender sind viel eher bereit, sich an Sicherheitsstandards zu halten, wenn sie den Sinn ihrer Existenz einsehen. **System-Standards** definieren den maschinellen Bereich einer Sicherheitsstrategie. Sie legen im Einzelnen fest, wie sicherheitsrelevante Systemparameter gesetzt werden sollen, für Systemwerte, Benutzerprofile, Zugriffsrechte, alle an das interne Netz angeschlossene Geräte einschließlich Router und Drucker etc. Ein Leitfaden zur Sicherheit muss nicht von Grund auf neu geschaffen werden; Sie können natürlich Inhalte von anderen Bereichen übernehmen. Um die Erstellung von Sicherheitsrichtlinien zu erleichtern, habe ich vier Dokumente, die als Beispiel dienen können, auf meiner Website zur Verfügung gestellt (www.WOEvans.com). Der Download ist kostenlos, ich würde mich aber freuen, wenn Sie für die Information eine kleine Spende an einen Empfänger Ihrer Wahl machen würden.

Bedrohung Nr.2: Risiken beim Zugriff auf den PC

Wenn iSeries (AS/400)-Anwender ihre traditionellen Green Screen-Terminals gegen PCs vertauschen und Client Access installieren, um die Anwender mit ihren Servern zu verbinden, ergeben sich dadurch oft unvorhergesehene Sicherheitsrisiken. Auf ihrem PC können Anwender mit dem System in einer Weise interagieren, wie es von einem Terminal mit festgelegtem Funktionsumfang aus unmöglich ist. PC-Anwender können zum Beispiel ein Icon nutzen, um sich mittels Prompting von Bibliotheks-, Datei- und Member-Namen durch File Transfer-Operationen führen zu lassen. Versierte PC-Anwender könnten sich sogar die Verwendung der RMTCMD (Remote Command)-Funktion, als Teil von Client Access, zu Eigen machen. RMTCMD erlaubt es, CL-Befehle abzusetzen, und auf diese Weise die LMTCPB-Restriktionen im iSeries-Benutzerprofil zu umgehen, das die Verwendung eines Befehls von der Befehlszeile aus verhindert. Erfahrene PC-Anwender lernen schnell, mit FTP Dateien zu übertragen (GET und PUT). In einer FTP-Session können aber auch Befehle an OS/400 abgesetzt werden. Die beste Möglichkeit, PC-Operationen (wie File Transfers, Remote-Befehle etc.) zu überwachen, ist die Verwendung von Exit-Programmen. OS/400 bietet diese Möglichkeit, aber Sie müssen das Exit-Programm selbst schreiben und installieren, und es gehört schon eine gehörige Portion Zeit und Anstrengung dazu, um die entsprechende IBM Dokumentation zum Thema zu verstehen. Vielleicht denken Sie auch eher daran, ein entsprechendes Programm einer Fremdfirma zu installieren, als Ihre kostbare Zeit in die Einarbeitung in das Thema Exit-Programme zu investieren.

Bedrohung Nr. 3: Triviale Passwörter

Bei der Einrichtung eines neuen iSeries Benutzerprofils legt das CRTUSRPRF-Kommando (Create User Profile) standardmäßig den Namen des Benutzerprofils auch als Passwort fest. Allzuhäufig versäumt es der Sicherheitsbeauftragte, das Passwort für ungültig zu erklären, so dass die Anwender beim ersten Zugriff aufgefordert werden, ihre Passwörter zu ändern. Selbst wenn ein Passwort für ungültig erklärt wurde, versäumen es manche Anwender, die ein Passwort erbitten, dieses sofort zu bestätigen, so dass Passwort und Benutzerprofil wieder identisch bleiben. So ist es nicht verwunderlich, dass Hacker oft erfolgreich sind, wenn sie den Namen des Benutzerprofils als Passwort eingeben. Nicht nur einmal ist es mir in Banken und anderen Finanzorganisationen gelungen, erfolgreich in das System zu gelangen, indem ich leicht zu knackende Passwörter für Benutzerprofile verwendet habe, die von IBM ausgeliefert wurden, oder auch für Benutzerprofile, die bei der Installation erzeugt wurden wie z.B. TEST, PCUSER, FTP oder USER1. Oft sind Applikations-Programme von Fremdfirmen installiert mit wohlbekannten Profilen (z.B. JDEINSTAL, ALDONCMS, S2KOBJOWN) und passenden Passwörtern. Um Ihnen die Suche nach Benutzerprofilen mit passendem Passwort zu erleichtern, bietet OS/400 das Kommando ANZDFTPWD (Analyze Default Passwords) an. Auch um die Anwender davor zu schützen, leicht zu knackende Passwörter zu wählen, kann der OS/400 Sicherheitsverantwortliche mit dem Kommando CHGSYSVAL (Change System Value) Systemwerte festlegen. Ich schlage Ihnen folgende Passwort-Regelungen für alle

Systeme vor: – Mindestlänge des Passwortes: 6 Zeichen (länger ist besser) – Das Passwort sollte mindestens eine Ziffer enthalten – Die Anwender sollten ihre Passwörter alle 60 Tage ändern – Dasselbe Passwort darf frühestens wieder verwendet werden, nachdem zwischendurch mindestens 10 verschiedene andere Passwörter Anwendung fanden. – Das gleiche Zeichen sollte im Passwort nicht mehrfach hintereinander verwendet werden.