

Der nachfolgende Artikel stand in der Computerwoche online

Der nachfolgende Artikel stand in der Computerwoche Online und ist zu finden unter <http://www.computerwoche.de/index.cfm?pageid=254&artid=27388>

Von CW-Redakteurin Sabine Ranft

Fällt die Festung Mainframe?

Auch die Dinosaurier des Computerzeitalters sind nicht unverwundbar: Vor allem die Kombination mit der modernen IP-Technologie weicht die traditionell hohe Sicherheit von Mainframe-Umgebungen auf. Hier müssen die betroffenen Firmen ihre Schutzmaßnahmen überdenken.

Dem Mainframe eilt der Ruf einer uneinnehmbaren Festung voraus - und das nicht ganz unberechtigt: In der Tat verfügen die Boliden über ausgefeilte Sicherheitsmechanismen. Deren Herzstück bildet die Datenbank Resource Access Control Facility (RACF) im Betriebssystem OS/390, in der User-IDs, Passwörter und Rechte für den Zugriff auf Ressourcen hinterlegt sind.

Die Ausfallsicherheit der Ungetüme ist legendär. So lassen sie sich beispielsweise zu Clustern zusammenschließen und können viele Prozessoren nutzen. Traditionell über SNA vernetzt und weitgehend von der Außenwelt isoliert, galten sie zudem als ziemlich einbruchssicher. Geldautomaten etwa hängen nicht in öffentlichen Netzen.

Missbrauch von Berechtigungen

Die größte Gefahr geht also nicht von externen Angreifern aus, sondern von den eigenen Mitarbeitern. Risiken birgt hier vor allem der Missbrauch von Berechtigungen. "Was regelmäßig vorkommt, ist, dass Mitarbeiter Daten klauen und zum Beispiel für Erpressung verwenden", bestätigt Klaus Brandstätter, Geschäftsführer der Bereiche Technik und Entwicklung bei der Firma HOB in Cadolzburg. HOB stellt Host- und Connectivity-Software her. Berichtet wird von einem konkreten Fall, in dem ein gechasster Bankmitarbeiter eine Liste von Kunden gestohlen hatte, die Konten in Luxemburg besaßen. Die Erpressung ging jedoch gründlich schief, weil der Ex-Arbeitgeber umgehend Anzeige erstattete. Externe dagegen, die die internen Abläufe nicht kennen, kommen nur schwer an die Boliden heran.

Eine Hürde für potenzielle Eindringlinge dürfte das immer weiter abnehmende Wissen über die alte Welt der Systems Network Architecture (SNA) sein. Bezeichnenderweise stammt dieser Begriff vom Mainframe-Riesen IBM; heute bringen nur noch wenige Spezialisten das für einen Angriff notwendige Know-how mit. Doch deshalb allein sollten sich Unternehmen nicht in Sicherheit wiegen. Peter Hager, Geschäftsführer bei der Netzwerksicherheitsfirma Net'Q GmbH in München, warnt: "Wer sich gut auskennt, kann leicht Schaden anrichten." Eine wunder Punkt, auf den der SNA-Spezialist seinen Finger legt, betrifft die Verwechslung von Ressourcen. Dabei wird dem Host eine neue Ressource als eine bereits bekannte untergeschoben. Diese Möglichkeit beruht auf der Eigenschaft von SNA, dass alle Ressourcen vordefiniert werden. Fällt eine Ressource aus, lässt sich anderswo eine gleichartige nachdefinieren ("Spoofing") und bekommt auch Zugriff. Führt jemand Böses im Schilde, kann er das leicht ausnutzen.

Doch in vielen Firmen regiert der Leichtsinn. Sie schenken den vereinzelt Mahnrufen keinen Glauben. Die Investitionen in die Sicherheit von Hosts tröpfeln nur noch spärlich, weil es anderswo - etwa bei den Linux- und Unix-Maschinen - noch mehr hapert. Aus Sicht der Anwender mag das nachvollziehbar sein. Doch William Malik, Vice President und Research Area Director Application Integration und Information Security bei Gartner, sieht darin ein Alarmsignal für eine Vernachlässigung der Großrechnersicherheit. Anlass zur Besorgnis ist in seinen Augen die Tatsache, dass die Häufigkeit von Generalinspektionen (Sicherheits-Audits) in Mainframe-Umgebungen sinkt und diese oft nur noch pro forma vorgenommen werden.

Einführung von TCP/IP-Connectivity

Weitere Lücken reißt die Einführung von TCP/IP-Connectivity in die (bis dato weitgehend heile) Großrechnerwelt. Selbst eine rein interne Migration auf IP schafft Sicherheitsprobleme, die kein SNA-Administrator kennt. Ein Vorzug des Protokolls verwandelt sich nämlich leicht in ein Manko: Wer TCP/IP einsetzt, strebt in der Regel Standardlösungen an, die einfach zu administrieren und zu benutzen sind. "Aber immer, wenn etwas einfacher zu benutzen ist, ist es für einen Angreifer auch einfacher, Schaden anzurichten", nennt Brandstätter die Kehrseite der Medaille. Ein Beispiel: Bei SNA muss man diverse Parameter kennen, um eine Verbindung zum Host aufzubauen. Diese Parameter werden am Host spiegelbildlich vorgehalten. Stimmen die Werte nicht überein, wird der Zugriff verweigert. "Unter TCP/IP dagegen kann das jeder", weiß Brandstätter. Selbst von einem PC aus lasse sich eine Emulation auf dem Host starten.

Als weitere Schwachstelle entpuppt sich das File Transfer Protocol (FTP), das vor allem intern exzessiv genutzt wird und viel Verkehr auf den Mainframes erzeugt. "Die FTP-Server laufen durchweg unsicher", bemängelt Hager. Unter OS/390 könnten Benutzer sämtliche FTP-Kommandos verwenden, sogar Jobs ließen sich starten. Doch damit nicht genug: Seinen Angaben zufolge gibt es bei Mainframes kein Attribut, das sagt, diese Datei darf zwar gelesen, aber nicht kopiert werden. "Das ist ungefähr so, als ob Sie in einen Supermarkt gehen und alles, was Sie sehen, auch mit nach Hause nehmen können, ohne zu bezahlen", vergleicht Hager. "Und vor allen Dingen wird alles transparent. Wenn zum Beispiel eine Bank FTP-Zugriff erlaubt - und die Banken tun das heute fast alle - dann kann ein Kunde die Datenstrukturen und Dateinamen vom anderen sehen. Das kann schon Begehrlichkeiten wecken."

Als Schutz empfiehlt Pricewaterhouse-Coopers, den Zugang zu einzelnen FTP-Kommandos pro Benutzer zu erlauben beziehungsweise zu sperren. Eine Einschränkung gewisser Kommandos auf bestimmte Datenmengen kann ebenfalls sinnvoll sein. Nicht zuletzt sollte die IP-Adresse eines Benutzers überprüft werden. Um diese Anforderungen zu erfüllen, ist in der Regel ein Zusatzprodukt nötig.

Verbindungen vom Host nach außen

Am empfindlichsten sind naturgemäß die Verbindungen vom Host nach außerhalb. Dies schlug in der Pannenstatistik aber noch nicht stark zu Buche, weil die Anbindung von Mainframes an das Internet noch vergleichsweise selten ist. Es kommt jedoch - zum Beispiel in Banken und Versicherungen - durchaus vor, dass der Host Daten und Anwendungen beherbergt, deren Ergebnisse im Internet präsentiert werden. Worauf man bei der Sicherung dieser Verbindung achten muss, verrät Christopher Mathes, Sicherheitsbeauftragter von IZB Soft in München. (Das Informatikzentrum Bayern (IZB) erbringt IT-Dienstleistungen für die bayerischen Sparkassen.) Einen Schutz durch konventionelle Instrumente wie Firewall und Intrusion Detection hält der Experte für unerlässlich. Zusätzlich sollte auf dem Host eine logische Trennung erfolgen, so dass man nicht mit IP direkt an die Kundendaten herankommt. Eine stärkere Authentisierung flankiert diese Maßnahmen, denn auch in Großrechnerumgebungen sind zu schwache Passworte eine Gefahr.

Ein Beispiel dafür liefert der "Domino-Go"-Web-Server. Wie Insider Malik von der Gartner Group erläutert, enthält dieser Server ein Muster-Shellsript namens "getmvs.sh", mit dessen Hilfe ein Web-Benutzer Zugang zum OS/390-Host (früher: MVS) erlangen kann. Dieser Benutzer durchläuft lediglich dieselbe Authentisierung mit User-ID und Passwort wie ein interner Nutzer. Das Protokoll TCP/IP macht es aber möglich, den Inhalt von Paketen mitzulesen, die zwischen Web-Browser und OS/390 hin- und hergeschickt werden. Diese Schwachstelle beruht nicht auf einer Sicherheitslücke im Host oder einem Missbrauch des Internet. Sie entsteht durch die Kombination der Mainframe- mit der IP-Welt, und jede der beiden Welten für sich genommen hätte die Lücke nicht. Malik empfiehlt daher, dieses Script vom Domino-Go-Web-Server zu entfernen. Kunden, die Web-Zugang zum Host benötigen, sollten lieber Virtual-Private-Network-(VPN-) oder Secure-Sockets-Layer-(SSL-)geschützte Verbindungen verwenden. Beides beinhaltet eine Verschlüsselung der übertragenen Informationen.

Doch nicht nur die Technik hat ihre Tücken. Oft wird auch der Mensch zur Achillesferse. Ein Problem kann beispielsweise der Arbeitsaufwand sein, um alle Löcher im System zu stopfen. Um Policies einzurichten,

User und Rechte zu pflegen, sind in der Regel mehrere gut ausgebildete Systemadministratoren nötig - etwa zwei bis drei für ein großes Rechenzentrum. Nicht immer wird das beherzigt: "Wir haben Kunden, da wissen die Administratoren fast nicht, was sie tun. Andere kennen sich gut aus und führen auch Sicherheitstests durch", attestiert Brandstätter den Anwenderfirmen.

Ein guter Administrator sollte bei allem, was er tut, auf mögliche Sicherheitsrisiken achten. Arno Foschepoth, Geschäftsführer der Bereiche Technik und Entwicklung bei der SBF Gruppe aus Osnabrück, die Großrechner-Support anbietet, rät außerdem, einer einzelnen Person nicht zu viel Macht zu geben. Bei vielen Entscheidungen ist ein Vier-Augen-Prinzip sinnvoll sowie die strikte Trennung zwischen Anwendungsentwicklung, Produktion und Qualitätssicherung. Mit anderen Worten: Bei der Übergabe produktionsreifer Anwendungen müssen die Zugriffsrechte der Entwickler zurückgesetzt und die in der Produktion neu aufgebaut werden.

Angriffe auf Mainframes selten

Angriffe auf Mainframes hat es schon gegeben, allerdings nicht besonders häufig. Die Seltenheit der Vorfälle bedeutet jedoch nicht notwendigerweise, dass es unmöglich wäre, Großrechner zu knacken. Hager behauptet sogar: "Wenn ich meine Energie darauf ansetzen würde, könnte ich in Deutschland 90 Prozent der Systeme mit einem ganz normalen Laptop lahm legen - es sei denn, ich käme vorher ins Gefängnis." Schnelle Netze und intelligente Workstations, wie sie für IP-Netze charakteristisch sind, erleichtern solche Attacken. Mit ihrer Hilfe kann der Angriff bedeutend schneller ablaufen.

Erfolgreiche Angriffe auf Großrechner setzen nach Angaben von Malik meist das Erraten oder Ausspionieren eines Passworts voraus oder nutzen falsche Konfigurationen aus. Viren infizieren diese Maschinen nicht, aber es gab schon per Mail verschickte Trojanische Pferde wie "Christma.exe", das Ende der 80er Jahre in VM-Umgebungen zuschlug.

Schutz über Callback-Funktionen

Auch Foschepoth hat bereits von Angriffen auf Mainframes "gehört, aber sie nicht in taktischer Auswirkung erlebt". Es habe über öffentliche Netze Wählangriffe auf Vorrechner der Boliden gegeben - zum Beispiel vom Chaos Computer Club, der einfach eine Reihe von Telefonnummern durchprobiert hat. Dabei erwischten die Hacker dann teilweise auch Einwählpunkte für den Fernzugriff auf Mainframes. Diese Attacken blieben allerdings meist erfolglos, weil die Zugänge über Callback-Funktionen geschützt sind. Das bedeutet: Wenn jemand anruft und sich als autorisierter Benutzer anmeldet, dann wird die Verbindung abgebaut und der registrierte Benutzer zurückgerufen. Auf diese Weise kann man zwar möglicherweise Kontakt mit einem Großrechner aufnehmen, aber nicht darauf arbeiten. "Es existieren natürlich Firmen ohne Callback", schränkt Foschepoth ein, "aber das ist mehr als leichtsinnig."

Sicherheitstipps

Wer Mainframes sicher in IP-Netze einbinden will, tut gut daran, sich ausgiebig mit den Sicherheitsmechanismen von Unix vertraut zu machen. Viele Konzepte im Großrechnerbereich sind von Unix entliehen.

Auch die bereits mit offenen Systemen gewonnenen Erfahrungen sollten berücksichtigt werden.

Es empfiehlt sich, mehrere IP-Stacks an einem Mainframe zu verwenden. So lassen sich beispielsweise Benutzer, die von außen auf den Host zugreifen, auf einen anderen IP-Stack lenken als interne. Bemerkte man nun einen Angriff, kann man den betroffenen Stack deaktivieren und wieder hochfahren, ohne die interne Kommunikation über den anderen Stack zu beeinträchtigen.

Jede Software lässt sich so reglementieren, dass sie nur bestimmte Teile des Großrechners benutzen kann. Das begrenzt die Auswirkungen möglicher Denial-of-Service-Attacken.

FTP überträgt im Standardzustand Passwörter im Klartext. Daher sollte man extern möglichst nur Anonymous FTP verwenden. Für die Software und die Geräte, die von außen Zugriff haben, ist zudem eine Verschlüsselung sinnvoll, ebenso für die im Großrechner gespeicherten Passwörter und User-IDs.

Werden Standardpasswörter nicht geändert, ist das System offen. Schließlich kennen viele Systemprogrammierer diese Einstellungen. Zum Beispiel ist bei VM das Standardpasswort für Master User deren Name.

Quellen: Behrooz Moayeri (Comconsult) und Klaus Brandstätter (HOB)

Sicherheitsmechanismen der Betriebssysteme

Virtual Machine (VM): hat ein Directory mit User-IDs und Passwörtern. Ein User kann sich nur an einem Terminal einloggen (Single Logon). Zugriffe sind nur auf die Ressourcen erlaubt, die dem Benutzer zugeordnet sind. Nach dem dritten falschen Logon-Versuch wird das Terminal gesperrt.

Virtual Storage Extended (VSE): beinhaltet die Schutzfunktion im Transaktionsmonitor Cics. Der Security Manager kennt User-IDs und Passwörter. Ein Nutzer darf nur bestimmte Transaktionen ausführen und Ressourcen nutzen. Single Logon.

OS/390: enthält die Sicherheitsdatenbank Resource Access Control Facility (RACF), in der User-IDs, Passwörter und Rechte für den Zugriff auf Ressourcen hinterlegt sind. Nach dem dritten Fehlversuch beim Logon wird der Benutzer blockiert.

BS2000: Die Sicherheit des Siemens-Systems ist etwa vergleichbar mit der von OS/390, da viele Funktionen von dem IBM-System übernommen worden sind und teilweise identische Hardware zum Einsatz kommt. Identischer Befehlssatz. Unterschiede: Connectivity, Datenbanksysteme. Bewertung der Tools

Das mächtigste Sicherheits-Tool ist die Datenbank RACF. Im Laufe der Zeit wurde in OS/390 alles implementiert, was man irgendwann einmal brauchen konnte. Zum Beispiel können fast alle Wartungsarbeiten während des Betriebs erledigt werden. Das System verfügt zudem über eine hohe Fehlertoleranz: Ist ein Plattenstecker herausgezogen, verabschiedet es sich nicht gleich, sondern bringt eine entsprechende Fehlermeldung.

Hinsichtlich der Sicherheit von VM und VSE gibt es einige kleinere Schönheitsfehler. Bei VSE beispielsweise ist der TCP/IP-Stack kein IBM-Produkt, sondern stammt von der Firma Connectivity Systems aus den Vereinigten Staaten. Laut Ronald Hammer, Projektleiter für die Systembetreuung von VM, VSE und OS/390 bei Infoconcept in Karlsruhe, sind hierbei einige Sicherheitsmechanismen lockerer als üblich, zum Beispiel beim File-Transfer: "Wenn ich im FTP-Bereich die Verwendung des gesamten File-Systems zulasse, kann jeder, der meine IP-Adresse benutzen kann, alle Files lesen und schlimmstenfalls zerstören." Daher ist eine eigene Exit-Routine nötig, die die bisherigen Sicherheitsmechanismen beim Login einbezieht.

Auch VM hat einen Nachteil: "Wenn sich jemand mit dem Betriebssystem auskennt und eine User-ID samt Passwort hat, kommt er auch ans Directory heran und weiß von jedem Benutzer ID und Passwort", gibt Hammer zu Bedenken. Allerdings kann sich ein Systemprogrammierer schützen, indem er das Verzeichnis nur für sich selbst sichtbar macht. VM und VSE lassen sich mit Erweiterungen von Drittherstellern auf das gleiche Niveau wie OS/390 mit RACF aufrüsten. Bekanntester Hersteller ist Computer Associates mit "ACF2" und "Topsecret". Ein Vorteil der Mainframe-Betriebssysteme: Programme, die vor 35 Jahren geschrieben wurden, laufen auf den modernsten Maschinen immer noch. Müssten sie ständig an Neuerungen angepasst werden, wäre auch dies ein nicht unbeträchtliches Sicherheitsrisiko.

Quellen: Ronald Hammer (Infoconcept) und Arno Foschepoth (SBF Gruppe)