Mainframe

Im Mainframeumfeld des ARZ werden Großrechner aus der IBM z Systems Serie zusammen mit dem Betriebssystem IBM z/OS eingesetzt. Im Gegensatz zu verschiedenen anderen Betriebssystemen, laufen unter z/OS standardmäßig keine Dienste, die einen externen Login ermöglichen. Stattdessen müssen diese vielmehr explizit installiert, konfiguriert und aktiviert werden, wobei bei deren Konfiguration im ARZ der Sicherheit besondere Aufmerksamkeit geschenkt wird.

Eine zweite Säule des Konzepts zur Betriebssystemhärtung am Mainframe im ARZ ist die Verwendung des externen Security Managers CA TopSecret. Dieser Security Manager regelt über die SAF-Schnittstelle von IBM z/OS die Kontrolle des Zugriffs auf den Mainframe und die verschiedenen darauf beheimateten Ressourcen. Bei der Vergabe der Zugriffsberechtigungen auf die unterschiedlichen Ressourcen wird dabei nach dem Prinzip "so viel wie nötig, so wenig wie möglich" vorgegangen und den einzelnen Benutzern ein möglichst passgenaues, rollenbasiertes Zugangsprofil mit nur all jenen Berechtigungen zugeteilt, die zwingend erforderlich sind, um den jeweiligen Tätigkeiten im Rahmen der individuellen Zuständigkeit (der Rolle) nachgehen zu können. Generische Zugriffsberechtigungen werden zum einen nur dort eingesetzt, wo dies aus organisatorischen Gründen mehr oder weniger notwendig ist und zum anderen nur innerhalb enger Grenzen vergeben (z.B. Steuerung des Zugriffs auf Datasets anhand eines Namenspräfixes).

Serverdienste (Started Tasks), die für den korrekten Betrieb in vielen Fällen höhere Privilegien als Standardbenutzer benötigen, werden ausschließlich mit logischen Anwendungsusern betrieben. Für diese Benutzeraccounts wird der interaktive Login unterbunden, sodass diese nur auf Umwegen (z.B. durch Ausnutzen von Softwarebugs) missbräuchlich verwendet werden können. Jedoch findet das bereits erwähnte Konzept "so viel wie nötig, so wenig wie möglich" auch bei diesen logischen Applikationsusern Anwendung. In eine ähnliche Kerbe schlägt auch das Bestreben, jeder Applikation ihren eigenen anwendungsspezifischen logischen User zuzuweisen und so eine schleichende, vielleicht implizite "Berechtigungsakkumulation" und damit die Schaffung von hochpotenten Benutzerkonten zu verhindern.

Mainframe

Mainframe computers of the IBM z Systems series in combination with the IBM z/OS operating system are used in the ARZ mainframe environment. In contrast to various other operating systems, no services run by default on z/OS, which permit an external login. Instead, these must be explicitly installed, configured and activated, in the course of which particular attention must paid to security in their configuration at the ARZ.

A second pillar of the concept for the operating system hardening on the mainframe at ARZ is the use of an external Security Manager CA TopSecret. Via the SAF interface of IBM z/OS, this Security Manager manages the control over the access to the mainframe and the different resources stored on it. The principle of "least privilege" is applied in the assignment of rights to access the various resources and the individual users are assigned the most personalised, role-based access profile possible with merely all those rights that are necessarily required to be able to perform the respective tasks within the scope of personal responsibility (the role). Generic access rights are for one thing used only where this is more or less necessary for organisational reasons and, if so, only within narrow limits (e.g. management of the access to datasets by means of a name prefix).

Server services (started tasks) that need higher privileges than standard users for the correct operation in many cases are operated exclusively with logical application users. For these user accounts, the interactive login is prevented so that misuse is possible only indirectly (e.g. by taking advantage of software bugs). However, the mentioned "least-privilege principle" is also applied to these logical application users. The intention of attributing a designated application-specific logical user to each application aims at a similar end and at thereby preventing a creeping, perhaps implicit "rights accumulation" and consequently the creation of highly potent user accounts.