Rollenberechtigungen

Die per RSBAC erstellten Rollen beinhalten eine Reihe von Rechten, welche die Zugriffe der ausgeführten Programme auf andere Ressourcen (wie Dateien, Netzwerk-Ports und Devices) beschränken oder ermöglichen. Hintergrund: In einem Linux-Betriebssystem mit RSBAC-Erweiterung können neben dem konventionellen Zugriffsrechtemodell noch weitere Modelle geladen und die Rechte miteinander kombiniert werden. Dabei versteht man unter Rechten auch Beschränkungen. Bei TightGate-Pro ist insbesondere das Role Compatibility Model (RC-Modell) zu nennen. Das RC-Modell erlaubt eine wesentlich feinere Rechtevergabe als das Standard-Zugriffsrechtemodell unter Linux.

Jede Rolle hat einen eigenen Satz an Rechten, unabhängig von allen anderen Rollen. Ruft ein Benutzer zum Beispiel den Webbrowser auf, der mit den Rechten der Rolle Webbrowser startet, so hat der Webbrowser die RC-Rechte für genau die Aktionen, die mit dem Webbrowser ausgeführt werden sollen. Zusätzlich bleiben die Rechtebeschränkungen aus den anderen Sicherheitsmodellen erhalten, der Browser eines Benutzers kann den Browser eines anderen nicht gefährden.

Hinweis: Bislang war zumeist von einem Administrator die Rede, wenn ein systemseitig angelegter Benutzeraccount mit den Berechtigungen einer bestimmten Rolle gemeint war. Im Folgenden werden Rollen in Großbuchstaben geschrieben, während Administratorkonten in Kleinbuchstaben referenziert werden. Eine Rolle beschreibt einen Berechtigungskontext, den ein Benutzer- bzw. Administratorenkonto, aber auch ein Programm innehaben kann. Für zentrale Rollen gibt es in TightGate-Pro jeweils nur ein einziges Administratorenkonto, das ebenso benannt ist wie die Rolle selbst.

Auch Programme werden einem Rollenkontext gestartet. Dies dient der Kapselung dieser Programme und verhindert sicherheitstechnisch relevante "Übergriffe" untereinander oder auf das zugrunde liegende Betriebssystem.

- Für die Rolle ***OFFICE***, welche ebenso wie ***MUA*** (Mail User Agent, Rolle zur Verwendung der E-Mail-Applikation auf TightGate-Pro) und ***WEBBROWSER*** erst durch den Start des jeweiligen Programms aktiviert wird, gelten besondere Regeln.
- Die Benutzerkonten regulärer VNC-Benutzer werden in der Rolle ***BENUTZER*** verwaltet. Es ist nicht möglich, als angemeldeter Benutzer im Rollenkontext eines Administrators zu arbeiten. Im Fall einer Direktanmeldung in einer Administratorenrolle wird immer das jeweilige Administratorenkonto aktiv, auch wenn sich ein regulärer Benutzer anmeldet. Eine Übertragung von Administratorrechten auf reguläre Benutzer ist im Gegensatz zu klassischen Betriebssystemen grundsätzlich nicht möglich.
- Ein Spezialfall der Benutzerrolle ist die Rolle ***TRANSFER***. In diesem Rollenkontext arbeiten ausschließlich die sogenannten ***transfer***-Benutzer, die der systemübergreifenden Bedienung der gesicherten Dateischleuse vorbehalten sind. ***transfer***-Benutzer sind auf alle transfer-Verzeichnisse sämtlicher regulärer Benutzer schreib- und leseberechtigt.
- Die Rolle ***CONFIG*** ist für den speziellen Administratoraccount ***config*** vorgesehen, welcher die Aufgabe hat, die spezifischen (Netzwerk-)Anpassungen für TightGate-Pro an das lokale Netz vorzunehmen. Die Rolle ***MAINT*** wird vom lokalen Administrator ***maint*** zur Nutzerverwaltung verwendet und ermöglicht das Anlegen und Löschen von Benutzern sowie die Vergabe von (initialen) Passwörtern.
- Die Rolle ***SECURITY*** bestimmt die Möglichkeiten des Sicherheitsbeauftragten. Diese Rolle kann das gesamte RSBAC-Regelwerk bearbeiten. Es können neue Rollen definiert und Rechte bestehender Rollen geändert werden. Wegen des großen Kompetenzumfangs ist die Rolle ***SECURITY*** in der Voreinstellung nur von der lokalen Konsole aus zugänglich. Ein SSH-Remote-

Zugang für ***SECURITY*** kann nur durch den Administrator ***maint*** für einen begrenzten Zeitraum aktiviert werden.

- Die Rolle ***ROOT*** entspricht im wesentlichen dem klassischen Systemverwalter für Systemdienste. Als ***ROOT*** können installierte Systemdienste gestartet und angehalten werden, es können Tests mit Systemwerkzeugen durchgeführt und eingeschränkt Systemdienste konfiguriert werden. Gegenüber dem universell berechtigten root-Account eines konventionellen Linux-Systems unterliegt die Rolle ***ROOT*** besonderen Beschränkungen. So kann ***ROOT*** insbesondere nicht auf die Verzeichnisse der Benutzer zugreifen, keine Programme mit RSBAC-Rechten ausstatten und generell keine RSBAC-Rechte ändern - wohl aber die RSBAC-Rechte einsehen.
- Die Rolle ***UPDATE*** dient der unkomplizierten Aktualisierung von TightGate-Pro. ***UPDATE*** vereinigt die Möglichkeiten des Netzwerkzugriffs (z.B. mittels SSH) und des Updates von Programm-Paketen mittels eines Paketmanagers.
- Die Rolle ***REVISION*** / Datenschutzbeauftragter (DSB). Die Rolle des Revisors und des Datenschutzbeauftragten finden sich praktisch in jeder Firma und Behörde gleichermaßen. Auch wenn diese Rollen in der Praxis oft durch verschiedene Personen wahrgenommen werden, so haben sie doch etwas gemeinsam: Sie haben das Recht (und die Pflicht), inhaltlich kontrollierend (d.h. lesend) auf System- und Benutzerdaten zuzugreifen, ohne Veränderungen vornehmen zu können.
- In der Standard-Konfiguration von TightGate-Pro ist die Rolle ***REVISION*** mit den Kontrollrechten eines Datenschutzbeauftragten ausgestattet. Ein Hilfsmenü ("Kopier-Tool") erleichtert es dabei dem Anwender, Kopien der Benutzerverzeichnisse zu erstellen und auf ihnen zu arbeiten. Die Rolle ***REVISION*** verhält sich ansonsten ähnlich wie die Rolle ***BENUTZER***, inklusive der Nutzung der Browser-, Office- und Mail-Rollen, jedoch ohne Netzwerkzugriff.
- Die Rolle ***VNC-SERVER*** steht stellvertretend für eine einem Systemdienst zugeordnete Rolle. Die Definition der nötigen RSBAC-Rechte in der Rolle ***VNC-SERVER*** und die Zuweisung dieser Rolle schränkt die Rechte des darunter laufenden Dienstes auf eben diesen definierten Bereich ein. Ein möglicher Programmfehler, eine Backdoor oder ein gezielt auf den Daemon abgestimmter Exploit können nur in diesem eng gesteckten Rahmen wirksam werden. Schon der Versuch, etwas anderes zu tun, führt zu einer Warnmeldung an die Systemadministration.
- Die Rolle ***BACKUP*** beinhaltet den Berechtigungskontext für den Administrator ***backuser***, welcher für alle Belange der zentralen Datensicherung und -rücksicherung auf TightGate-Pro zuständig ist.
- Die ***ROOT***-Wartungsrolle ist eine Erweiterung der normalen ***ROOT***-Rolle zuzüglich der Berechtigung, Prozesse sehen und signalisieren zu dürfen. Da die ***ROOT***-Wartungsrolle eine Ausweitung der Rechte für root darstellt, wurden besondere Vorsichtsmaßnahmen getroffen, um diese vor Missbrauch zu schützen. So ist die Erweiterung nur über ein Vieraugenprinzip zu erlangen. Dabei muss die Rolle ***SECURITY*** die Rolle ***ROOT-Wartung*** freischalten, bevor sie vom Administrator ***root*** verwendet werden kann.

Funktion Berechtigung	**Rollenbezeichnung**									
	BENUTZER	**CONFIG**	**MAINT**	**UPDATE**	**BACKUP**	**REVISION**	**TRANSFER**	**SECURITY**	**ROOT**	**ROOT-WARTUNG**
Auf Menüfunktionalität beschränktes Ändern von Netzwerkeinstellungen	-	+	-	-	-	-	-	-	-	-
Neustart des Systems	-	+	+	+	-	-	-	-	+	+
Individuelles Ändern von Konfigurationsdateien	-	-	-	-	-	-	-	-	-	+ eingeschränkt
Vergabe von Rollenberechtigungen	-	-	-	-	-	-	-	+	-	-
Shell-Zugriff	+	-	-	-	-	+	-	+	+	+
Grafische Oberfläche	+	-	-	-	-	+	-	-	-	-
Auf Menüfunktionalität beschränkte Benutzerverwaltung	-	-	+	-	-	-	-	-	-	-
Neustart einzelner Dienste	-	+	+	+	-	-	-	-	+	+

Funktion Berechtigung	**Rollenbezeichnung**									
Zeitbeschränkte Zulassung von Administratoranmeldungen per SSH	-	-	+	-	-	-	-	+(*)	-	-
Zulassung von Anmeldungen per SSH über Netzwerk von außerhalb des vorgesehenen Klientennetzwerks	-	+	-	-	-	-	-	-	+(*)	+(*)
Öffnen des Fernwartungszugangs für die m-privacy GmbH	-	-	+	-	-	-	-	-	-	-
Über Menüfunktionalität beschränkte Aktualisierung der installierten Programmpakete	-	-	-	+	-	-	-	-	-	-
Zugriff auf /home-Verzeichnisse	+ nur eigenes Verzeichnis	-	-	-	-	+ nur lesend	-	+ nur lesend	-	+
Sichern und Zurückspielen der RSBAC-Konfiguration	-	-	-	+ Restore	-	-	-	+	-	-
RSBAC-Konfiguration ändern	-	-	-	-	-	-	-	+	-	-
Voller Zugriff mittels Interpreter auf Abbilder gewählter Benutzerverzeichnisse	-	-	-	-	-	+	-	-	-	-
Nur-Lesezugriff auf Systemprotokolle (Logs)	-	-	-	-	-	+	-	+	+	+
Schreibzugriff auf Systemprotokolle	-	-	-	-	-	-	-	-	-	-
Netzwerkzugriff	+	-	-	eingeschränkt	eingeschränkt	-	-	eingeschränkt	eingeschränkt	eingeschränkt
Nur-Lesezugriff auf Benutzerdaten	-	-	-	-	-	+	-	+	-	-
Editieren der Konfiguration von ungeschützten Systemdiensten	-	-	-	-	-	-	-	-	-	+
Nutzung von Test-Tools (z. B. netstat)	-	-	-	-	-	-	-	-	+	+
Aufruf von "rsbac_menu"	-	-	-	-	-	-	-	+	+ (nur lesend)	+ (nur lesend)

Legende:

(*) Option ist nur manuell über die Konsole einstellbar, nicht über eine Menüoption.