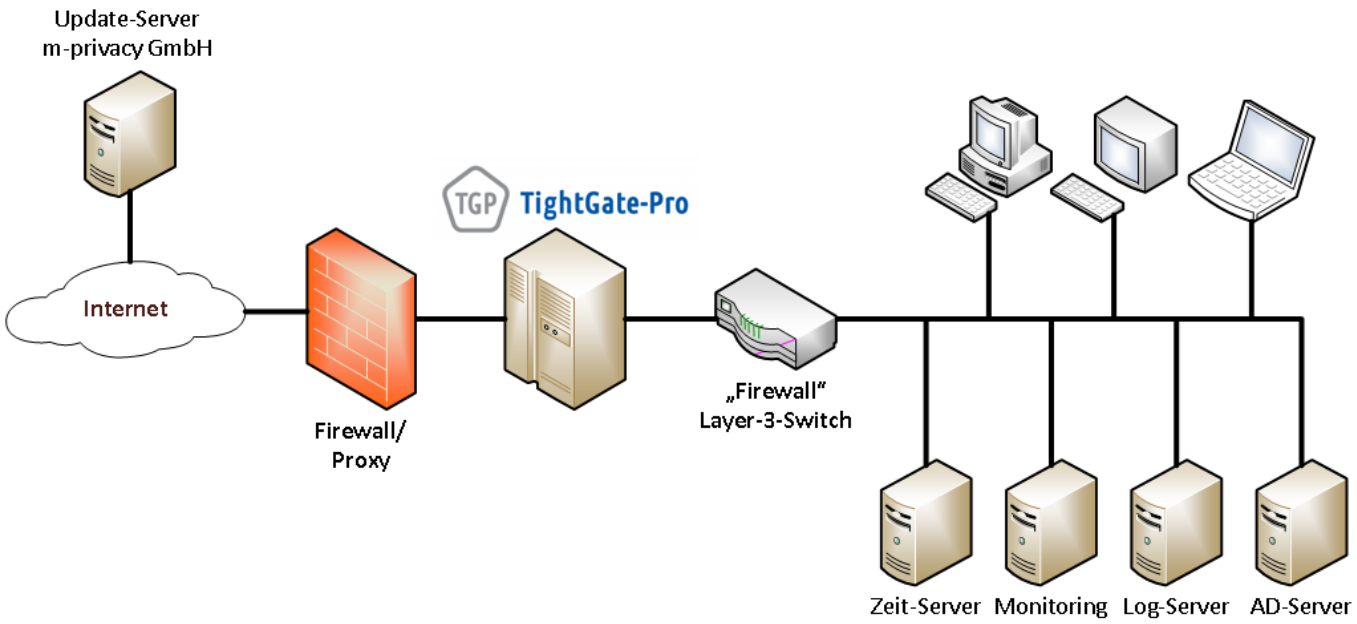
Einführung

Das dedizierte Remote-Controlled Browser System (ReCoBS) TightGate-Pro schützt präventiv vor Angriffen aus dem Internet und erweist sich damit regelmäßig als wirksamer als klassische Filtersysteme wie Malware-Scanner, Firewalls oder Intrusion Detection Systems (IDS). TightGate-Pro ist ein speziell entwickeltes ReCoBS-Schutzsystem, das als Appliance dem Unternehmens- oder Behördennetzwerk vorgeschaltet wird. Die Programme für den freien Internetzugriff (Internetbrowser) laufen nicht mehr auf dem Arbeitsplatzrechner, sondern zentral auf TightGate-Pro.

Der Zugriff auf das Internet erfolgt ausschließlich über TightGate-Pro. In das interne Netzwerk wird lediglich die Bildschirmausgabe des Browsers übertragen und auf den Arbeitsplatz-PCs angezeigt.

Gleichzeitig werden Maus- und Tastatureingaben der Benutzer zur Fernsteuerung des Browsers an TightGate-Pro gesendet. Für die Kommunikation zwischen Arbeitsplatzrechner und TightGate-Pro kommt ein auf Sicherheit optimiertes VNC-Protokoll zum Einsatz.

Netzwerkplanung



TightGate-Pro wird typischerweise direkt hinter der ersten Firewall in die Organisationsinfrastruktur eingebunden. Gegenüber dem internen Netz (LAN) wird TightGate-Pro durch einen Layer-3-Switch mit Paketfilterung abgeschottet. Dieser stellt sicher, dass ausschließlich definierte Verbindungsaufbauten von Arbeitsplatzrechnern (über TightGate-Viewer und ggf. TightGate-Schleuse) zu TightGate-Pro zugelassen werden. Ebenso verhindert der Layer-3-Switch regulär Verbindungen ausgehend von TightGate-Pro in Richtung internes Netzwerk. Ausnahmen sind nur zulässig, wenn TightGate-Pro Dienste nutzen muss, die ausschließlich im internen Netzwerk verfügbar sind (siehe Schaubild).

Alternativ kann TightGate-Pro in einer DMZ betrieben werden. Dabei ist jedoch zu berücksichtigen, dass der Netzwerkdurchsatz in Richtung internes Netz – insbesondere bei der Wiedergabe multimedialer Inhalte – stark ansteigt. Damit die Darstellung flüssig bleibt, muss die verfügbare Bandbreite ausreichend hoch sein. Die m-privacy GmbH empfiehlt daher dringend, die Absicherung in

Richtung LAN über einen dedizierten Layer-3-Switch zu realisieren, der für jeden TightGate-Pro-Server einen angemessenen Datendurchsatz gewährleistet.

Umfeldmaßnahmen

Der sichere Betrieb von TightGate-Pro und die damit erzielbare Schutzwirkung für Arbeitsplatzrechner und das umgebende Netzwerk werden auch durch das IT-Umfeld des TightGate-Pro-Servers sowie der Klientenrechner beeinflusst.

Absicherung der Arbeitsplatzrechner (Klientenrechner)

Arbeitsplatzrechner, von denen aus über TightGate-Pro auf das Internet zugegriffen wird, dürfen keine weiteren Zugänge zum Internet besitzen. Ihre Netzwerkverbindungen sind mittels entsprechender Paketfilter oder Firewalls vollständig vom Internet abzuschotten. Sofern eine Gefährdungsanalyse dies erforderlich macht, ist im internen Netzwerk sowie auf den Klientenrechnern ein geeigneter Malware-Schutz einzurichten.

Benutzer sollen Klientenrechner ausschließlich mit eingeschränkten Rechten nutzen. Die Systemadministration muss sicherstellen, dass der TightGate-Viewer nicht mit administrativen Berechtigungen gestartet werden kann, um eine dauerhafte oder unberechtigte Änderung von Konfigurationseinstellungen zu verhindern.

Die Nutzung von TightGate-Pro ist ausschließlich mit dem TightGate-Viewer möglich. Andere VNC-Viewer können entweder aufgrund fehlender Funktionalitäten (z. B. Verschlüsselungsverfahren) keine Verbindung aufbauen oder genügen den sicherheitsrelevanten Anforderungen nicht. Die Systemadministration hat sicherzustellen, dass Installation und Betrieb alternativer VNC-Viewer auf den Arbeitsplatzrechnern unterbunden sind.

Warnung

TightGate-Pro bietet systembedingt keinen Schutz vor Angriffen, die über andere freigegebene Netzwerkkanäle auf Klientenrechner oder das interne Netzwerk wirken. Grundlegende Schutzmaßnahmen für die Betriebsumgebung von TightGate-Pro sind daher durch die Systemadministration zu gewährleisten.

Eigensicherheit von TightGate-Pro

TightGate-Pro verfügt über umfassende Mechanismen zur eigenen Absicherung für einen stabilen und sicheren Dauerbetrieb.

Serverbetriebssystem und Kommunikationsprotokoll

Das Betriebssystem enthält ausschließlich die für den Betrieb notwendigen Komponenten. Eine konsequente Kapselung aller Programme und Prozesse verhindert die unkontrollierte Ausführung nicht autorisierter Software sowie Manipulationen installierter Komponenten. Ein funktionsspezifisches

Kommunikationsprotokoll zwischen TightGate-Pro und TightGate-Viewer verhindert zuverlässig unkontrollierte Zugriffe in das interne Netzwerk und aus diesem heraus.

Abschottung von Benutzerkonten

Alle Benutzerkonten sowie die von VNC-Benutzern initiierten Sitzungen sind vollständig voneinander isoliert. Ein gegenseitiger Zugriff oder eine Beeinflussung ist ausgeschlossen. VNC-Benutzer verfügen ausschließlich über Berechtigungen ihrer jeweiligen Benutzerrolle und besitzen keine administrativen Rechte.

Sichere Startbedingungen

Jede Benutzersitzung auf TightGate-Pro beginnt in einem definierten, sicheren Ausgangszustand. Zentrale Sicherheitsoptionen sind serverseitig fest vorgegeben und werden zu Beginn jeder Session automatisch neu gesetzt. Vom Benutzer vorgenommene Änderungen wirken sich daher nicht dauerhaft aus und eröffnen keine Sicherheitslücken.

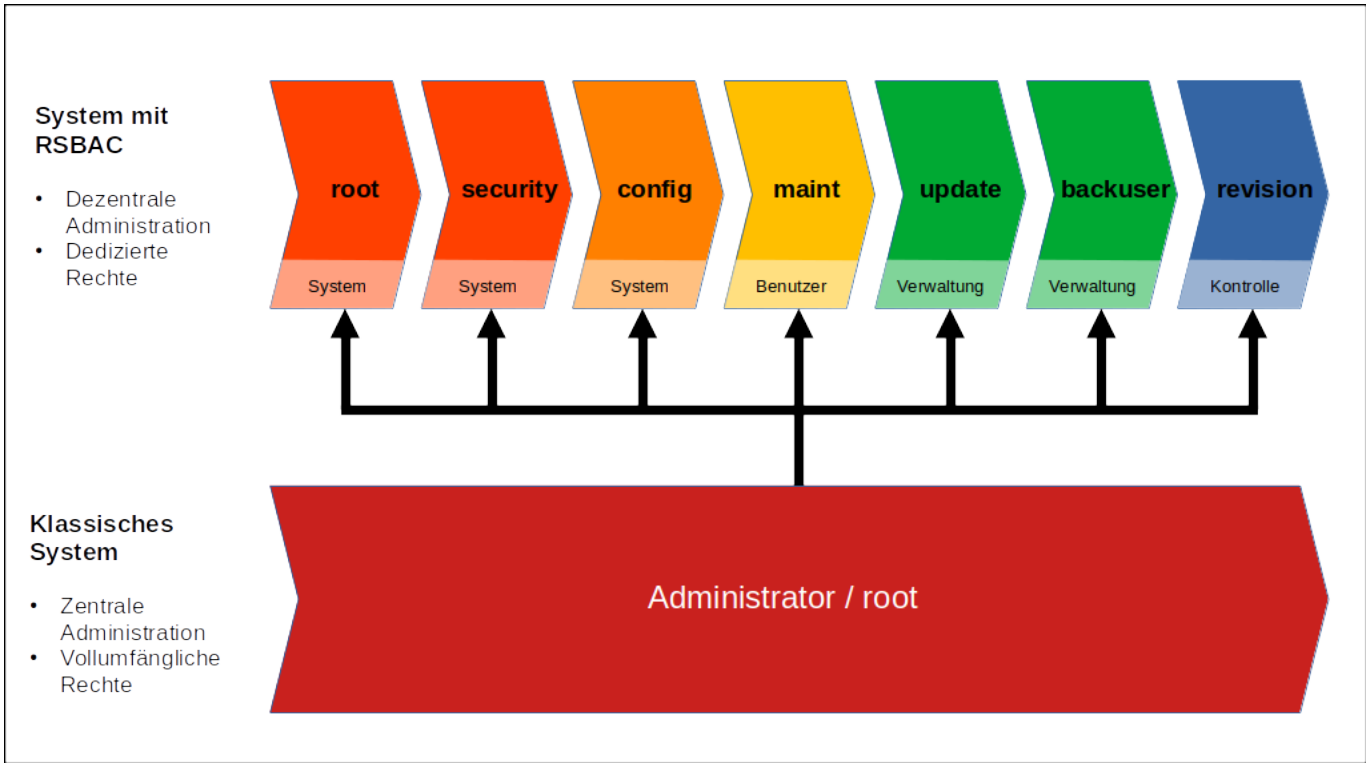
Nach dem Ende einer Internetsitzung verbleiben keinerlei aktive Inhalte auf TightGate-Pro. Sämtliche im Benutzerkontext gestarteten Programme und Anwendungen werden bei der Abmeldung automatisch beendet.

Eine gegenseitige Beeinflussung von Anwendungen – insbesondere im Hinblick auf den eingesetzten Internetbrowser – ist durch die vollständige Kapselung aller Softwarekomponenten in strikt getrennten Berechtigungssphären zuverlässig ausgeschlossen.

Mehrdimensionale Systemhärtung und Fehlerresistenz

Die Kombination verschiedener Härtungs- und Kapselungsmaßnahmen sowie das spezialisierte Kommunikationsprotokoll führen zu hoher sicherheitstechnischer Robustheit – selbst unter der Annahme, dass einzelne Softwarekomponenten Unzulänglichkeiten in Logik oder Implementierung aufweisen könnten.

Das Administrationskonzept von TightGate-Pro



TightGate-Pro hat werksseitig fest vordefinierte Administratorenrollen, die den herkömmlichen Administrator (root) ersetzen. Keine dieser Administratorenrollen verfügt über umfassende Zugriffsrechte auf das Gesamtsystem (Superuser-Privilegien). Die Vorteile dieses dezentralen Administrationskonzepts ist einerseits der Schutz des Systems und der Benutzerdaten vor einer funktional unangemessen Allmacht[1)]. Anderseits wird durch die Abbildung einzelner Administrationsvorgänge auf mehrere Rollen eine Delegation der Aufgaben möglich. Die konkreten Berechtigungen der jeweiligen Rollen sind im Anhang zu diesem Administrationshandbuch tabellarisch zusammengefasst.

Systembezogene Administration

Für System- und Sicherheitsadministration steht das Konto ***config*** zur Verfügung. Es verwaltet Netzwerkeinstellungen und systemweite Vorgaben, etwa für Benutzerkonten. Kein Zugriff besteht auf Benutzerverzeichnisse oder Benutzereinstellungen, sodass ein Großteil der Wartungsaufgaben datenschutzkonform delegiert werden kann.

Personenbezogener Bereich

Das Konto ***maint*** ist für die Benutzerverwaltung zuständig. Es können Benutzer angelegt, Zugangsberechtigungen angepasst und Passwörter geändert werden. Zudem kann ***maint*** einzelne Dienste neu starten und bei Bedarf einen Fernwartungszugang freischalten. Ein Einblick in Benutzerverzeichnisse oder -daten ist dieser Rolle jedoch nicht möglich.

Wartungsbereich

Für Wartungsaufgaben existieren die Rollen ***backuser*** und ***update***. Beide verfügen über stark eingeschränkte Rechte. ***backuser*** ist ausschließlich für Erstellung und Verwaltung von Backups zuständig, während ***update*** Aufgaben der Systempflege übernimmt. Beide Rollen besitzen weder Zugriff auf Netzwerkeinstellungen noch auf Benutzerverzeichnisse.

Sicherheitsbereich

Die zentrale Systemsicherheit wird durch den Zugriffsrechteschutz RSBAC gewährleistet. Die zugehörige Konfiguration ist bei Auslieferung vollständig eingerichtet und darf in der Regel nicht verändert werden. Zur Anpassung der RSBAC-Sicherheitsparameter stehen die Administratoren ***root*** und ***security*** zur Verfügung.

[1)]

Die herkömmliche Konzentration aller Administrationsaufgaben und Systemrechte in einem zentralen Account gefährdet diesen in besonderem Maße im Bezug auf Eindringversuche. Unbefugte, die Zugang zu einem solchen Benutzerkonto erlangen, erhalten Zugriff auf das gesamte System.