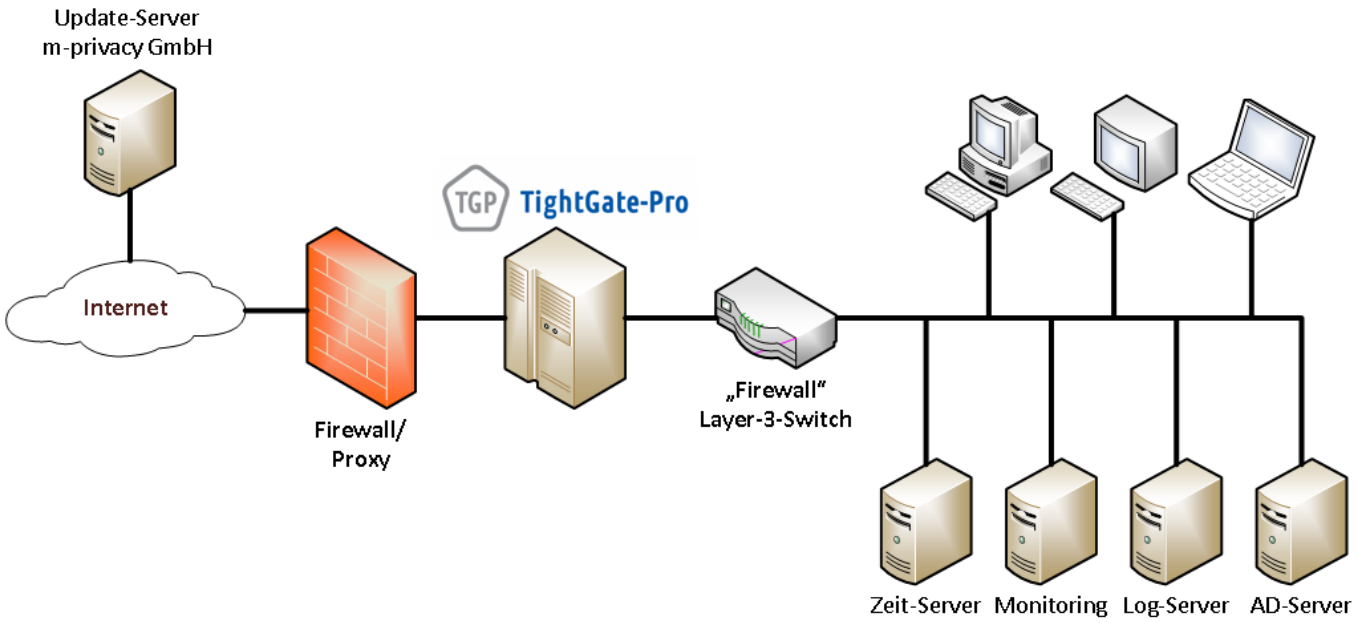
Einführung

Das dedizierte Remote-Controlled Browser System (ReCoBS) TightGate-Pro schützt präventiv vor Angriffen aus dem Internet. Damit erweist es sich regelmäßig wirksamer als jedes filternde System wie Malware-Scanner, Firewalls oder Intrusion Detection Systems (IDS). Bei TightGate-Pro handelt sich um ein dediziertes ReCoBS-Schutzsystem, das als Appliance dem Unternehmens- oder Behördennetzwerk vorgeschaltet wird. Die Programme für den freien Internetzugriff (Internetbrowser) werden nicht mehr auf dem Arbeitsplatz-PC, sondern auf TightGate-Pro ausgeführt.

Die Zugriffe in das Internet erfolgen ausschließlich von TightGate-Pro aus. Lediglich die Bildschirmausgabe des Browsers wird in das interne Netzwerk übertragen und auf den Arbeitsplatz-PCs angezeigt.

Zugleich werden Maus- und Tastaturinformationen zur Fernsteuerung des Browsers von den Arbeitsplatz-PCs an TightGate-Pro übermittelt. Zur Kommunikation zwischen Arbeitsplatz-PC und TightGate-Pro dient ein auf Sicherheit optimiertes VNC-Protokoll.

Netzwerkplanung



TightGate-Pro wird regelmäßig unmittelbar hinter der ersten Firewall in die Organisationsinfrastruktur integriert. Zum internen Netz (LAN) hin wird TightGate-Pro mit einem Layer-3-Switch (mit Paketfilterung) abgeschottet, welcher sicherstellt, dass nur definierte Verbindungsaufbauten vom Arbeitsplatz-PC (per TightGate-Viewer und ggf. TightGate-Schleuse) zu TightGate-Pro möglich sind. Der Layer-3-Switch soll ebenfalls verhindern, dass es Verbindungsaufbauten von TightGate-Pro in Richtung internes Netz (LAN) gibt. Ausnahmen von dieser Regel gelten nur, sofern TightGate-Pro Dienste verwenden soll, die nur im internen Netzwerk (LAN) bereitgestellt werden (Siehe Schaubild).

TightGate-Pro kann auch direkt in einem DMZ-Bereich aufgestellt werden, jedoch ist zu beachten, dass der Netzwerkdurchsatz bei TightGate-Pro in Richtung internes Netzwerk (LAN) gerade bei der Betrachtung von Multimedia-Inhalten stark erhöht ist. Um sicherzustellen, dass die Wiedergabe von

TightGate-Pro flüssig läuft, muss der Datendurchsatz in Richtung LAN ausreichend sein. Daher wird seitens der m-privacy GmbH dringend empfohlen, die Absicherung in Richtung LAN über einen dedizierten Layer-3-Switch zu leiten, welcher für jeden eingesetzten TightGate-Pro Server einen angemessenen Netzwerkdurchsatz gewährleistet.

Umfeldmaßnahmen

Der sichere Betrieb von TightGate-Pro und die damit erzielbare Schutzwirkung auf Arbeitsplatzrechner und das sie umgebende Netzwerk können durch das IT-Umfeld von TightGate-Pro Server sowie der Klientenrechner (Arbeitsplatzstationen) beeinflusst werden.

Absicherung der Arbeitsplatzrechner (Klientenrechner)

Arbeitsplatzrechner (Klientenrechner), von denen aus über TightGate-Pro auf das Internet zugegriffen werden soll, dürfen keine anderweitige Verbindung zum Internet haben. Die Netzwerkverbindung der Klientenrechner ist über entsprechend konfigurierte Paketfilter bzw. Firewalls vom Internet abzuschotten. Erforderlichenfalls ist für adäquaten Malware-Schutz im internen Netzwerk sowie auf den Klientenrechnern zu sorgen, falls eine Gefährdungsanalyse einen entsprechenden Bedarf erkennen lässt.

Es ist darauf zu achten, dass Benutzer die Klientenrechner nur mit eingeschränkten Benutzerrechten verwenden. Seitens der Systemadministration muss sichergestellt sein, dass der TightGate-Viewer durch den Benutzer nicht mit administrativen Rechten gestartet wird, um eine dauerhafte Verankerung unbeabsichtigter oder unberechtigter Änderungen von Konfigurationseinstellungen am TightGate-Viewer zu unterbinden.

Die Nutzung von TightGate-Pro ist nur mit TightGate-Viewer zu bewerkstelligen. Andere VNC-Viewer können sich entweder aufgrund fehlender Funktionalität (z. B. Verschlüsselungsverfahren) nicht mit TightGate-Pro verbinden oder erfüllen nicht die Anforderungen im Hinblick auf bestimmte Sicherheitsvorkehrungen beziehungsweise Verfahrensvorgaben. Durch die Systemadministration ist sicherzustellen, dass die Installation und der Betrieb alternativer VNC-Viewer auf den Arbeitsplatzrechnern nicht möglich ist.

Warnung

TightGate-Pro bietet systembedingt keinen Schutz vor Angriffen, die über anderweitig freigegebene Netzwerkkanäle auf die Klientenrechner oder das interne Netzwerk einwirken. Grundlegende Maßnahmen zum Schutz der Betriebsumgebung von TightGate-Pro sind durch die Systemadministration zu ergreifen.

Eigensicherheit von TightGate-Pro

TightGate-Pro verfügt über weitreichende Mechanismen zum Eigenschutz im Hinblick stabilen und sicheren Dauerbetrieb.

Serverbetriebssystem und Kommunikationsprotokoll

Das Betriebssystem von TightGate-Pro verfügt ausschließlich über solche Programmkomponenten, die für dessen Betrieb unabdingbar sind. Eine umfassende Kapselung sämtlicher Programme und Prozesse beugt einer unkontrollierten Ausführung nicht autorisierter Software sowie eine Manipulation installierter Programmkomponenten auf TightGate-Pro wirksam vor. Ein funktionsspezifisches Kommunikationsprotokoll zwischen TightGate-Pro und TightGate-Viewer verhindert zuverlässig den unkontrollierten Zugriff in das interne Netzwerk und aus diesem heraus.

Abschottung von Benutzerkonten

Sämtliche Benutzerkonten und die durch angemeldete Benutzer (VNC-Benutzer) initiierten Benutzersitzungen sind auf TightGate-Pro vollständig voneinander abgeschottet. Es besteht keine Möglichkeit eines wechselseitigen Zugriffs oder einer Beeinflussung. VNC-Benutzer sind nicht mit administrativen Berechtigungen ausgestattet, die über die Benutzerrolle hinausgehende Handlungsoptionen eröffnen.

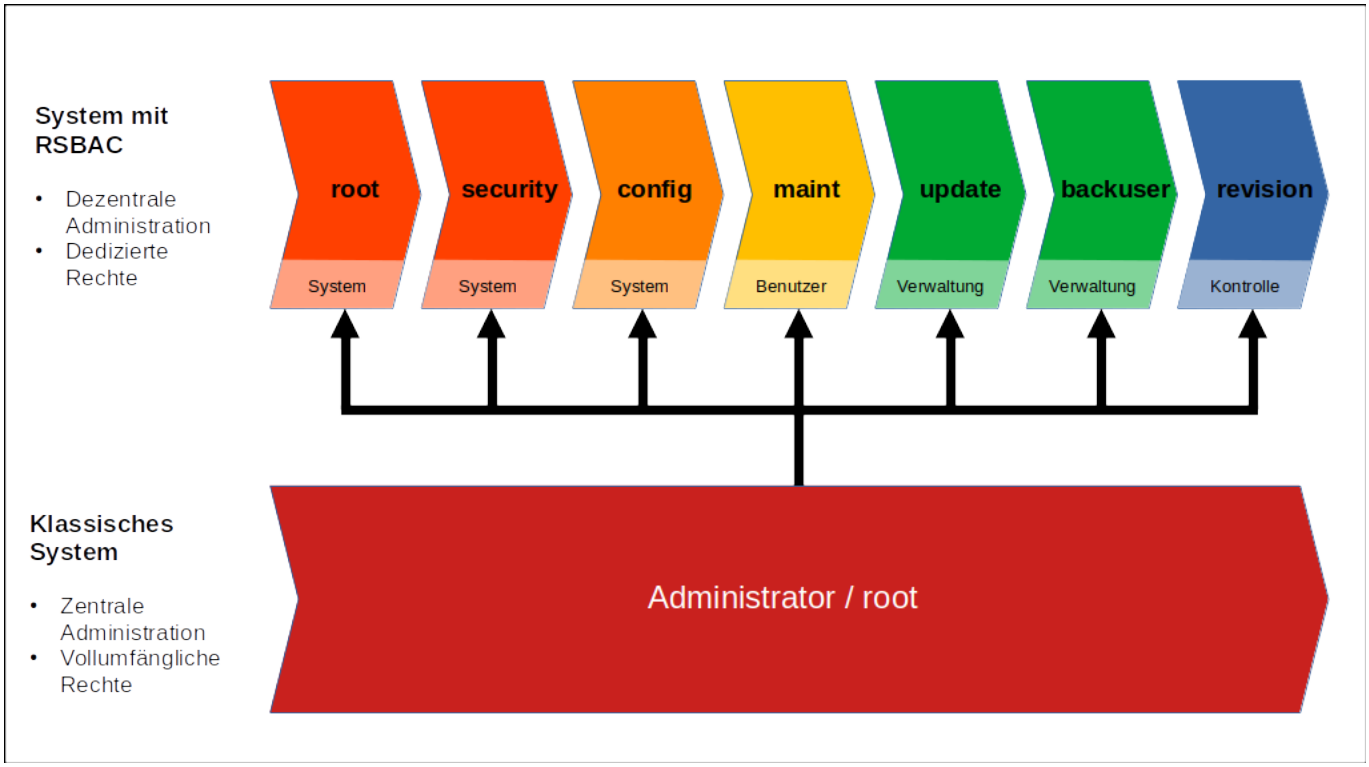
Sichere Startbedingungen

Jede Benutzersitzung auf TightGate-Pro startet in einem sicheren Ausgangszustand. Wesentliche Sicherheitsoptionen sind serverseitig fixiert. Nachgeordnete Konfigurationsänderungen, beispielsweise durch Einstellungen im Programmmenü des TightGate-Viewers, werden im Benutzerkontext nicht dauerhaft gespeichert und nach Beendigung der Benutzersitzung (Session) auf die vorgegebenen Standardwerte zurückgesetzt. Weiterhin bleiben auf TightGate-Pro keine aktiven Inhalte aus einer Internetsitzung nach deren Beendigung erhalten. Alle auf TightGate-Pro im Benutzerkontext gestarteten Programme und Applikationen werden bei der Abmeldung von TightGate-Pro automatisch beendet. Eine wechselseitige Beeinflussung von Applikationen auf TightGate-Pro, insbesondere im Hinblick auf den verwendeten Internetbrowser, ist durch vollständige Kapselung aller Softwarekomponenten in separaten Berechtigungssphären ausgeschlossen.

Mehrdimensionale Systemhärtung und Fehlerresistenz

Die Kombination unterschiedlicher Härtungs- und Kapselungsmaßnahmen zum Eigenschutz von TightGate-Pro nach dem Stand der Technik in Verbindung mit einem funktionsspezifischen Protokoll zur Kommunikation mit den Klientenrechnern bewirkt ein außerordentliches Maß an sicherheitstechnischer Robustheit. Dies gilt insbesondere auch unter der A-Priori-Annahme, dass einzelne Programmkomponenten von TightGate-Pro mit Unzulänglichkeiten hinsichtlich Programmlogik respektive Implementierung behaftet sein 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 die System- und Sicherheitsadministration von TightGate-Pro wurde das Administratorkonto ***config*** geschaffen. Dieses ist zuständig für die Netzwerkeinstellungen und systemweite Vorgaben z. B. für Benutzerkonten. Keinen Zugriff hingegen hat diese Administrationsrolle auf Benutzerverzeichnisse und Benutzereinstellungen. Die meisten Wartungsaufgaben können damit datenschutzrechtlich bedenkenlos delegiert werden.

Personenbezogener Bereich

Dem Administrationsaccount ***maint*** obliegt die Benutzerverwaltung von TightGate-Pro. Es können Benutzer angelegt, Zugangsberechtigungen und -einschränkungen vorgenommen und Passwörter geändert werden. Dieser Administrator hat ebenfalls die Möglichkeit, einzelne Dienste neu zu starten und ggf. einen Fernwartungszugang freizuschalten. Eine inhaltliche Kontrolle von Benutzerverzeichnissen und -daten durch ***maint*** ist ausgeschlossen.

Wartungsbereich

Für Wartungsaufgaben von TightGate-Pro wurden die Administratorkonten ***backuser*** und ***update*** vorgesehen. Sie haben nur einen sehr begrenzten Funktionsumfang und speziell definierte Rechte. Dabei ist der ***backuser*** ausschließlich für das Erstellen und Verwalten von Backups und die dafür notwendigen Einstellungen verantwortlich. Gleiches gilt für die Rolle ***update*** bei der Pflege des Systems. Beide Rollen haben weder Zugriff auf die Netzwerkeinstellung noch dürfen sie Benutzerverzeichnisse einsehen.

Sicherheitsbereich

Die zentrale Sicherheit von TightGate-Pro wird über den Zugriffsrechteschutz RSBAC gewährleistet. Die RSBAC-Konfiguration ist bei Auslieferung komplett konfiguriert und darf regelmäßig nicht von Administratoren verändert werden. Zur Bearbeitung der RSBAC-Sicherheitseinstellungen gibt es die Administratoren ***root*** und ***security***.

[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.