TightGate-Pro

Dediziertes Remote-Controlled Browser System
zum Schutz vor Gefahren aus dem Internet

Anhang zum Administrationshandbuch

Sicherheitskonzept
Monitoring mit Nagios

m-privacy_AGD-OPE
Build 1.4-844

Herausgeber:
m-privacy GmbH
Technische Redaktion
Werner-Voß-Damm 62
12101 Berlin

Fon: +49 30 243423-34
Fax: +49 30 99296856

support@m-privacy.de
help.m-privacy.de/tightgate-pro

Inhaltsverzeichnis

Versionshistorie

Ver.	Datum	Änderung	Redakteur
0.50	05.12.2013	Ausgliederung aus Administrationshandbuch Ver. 1.87.	ple
1.00	06.05.2013	Finalisierung und Veröffentlichung der Urversion.	ple
1.10	19.02.2014	Ergänzung der MIME-Typen.	ple
1.11	19.01.2016	Ergänzung Passwort-Optionen / Stand Build 1.4-844	hom

Allgemeine Hinweise zu diesem Handbuch

Alle Materialien und Ausführungen wurden mit größter Sorgfalt erarbeitet und zusammengestellt. Dennoch sind Fehler nicht auszuschließen. Die m-privacy GmbH übernimmt keine Haftung für Schäden, die aus Unrichtigkeit einzelner Angaben entstehen.

Im Sinne einer raschen Orientierung und zur Vermeidung von Sicherheitsrisiken werden besonders wichtige Aspekte durch wiederkehrende Stichworte gekennzeichnet. Diese sind:

Hinweis
Unter diesem Stichwort werden nützliche Details zur rationellen Verwendung von TightGate-Pro erläutert.

Achtung
Unter diesem Stichwort erfolgen Hinweise zur Problemvermeidung bzw. zur Vorbeugung von Betriebsstörungen bei TightGate-Pro.

Warnung
Unter diesem Stichwort erfolgen Hinweise auf mögliche Fehler bei der Konfiguration und Verwendung von TightGate-Pro, die weitreichende Sicherheitsrisiken bergen oder zu schwerwiegenden Betriebsstörungen führen können.

Hinweise zu den Ergänzungsspalten der tabellarischen Darstellungen

Die tabellarischen Darstellungen der Einstelloptionen tragen die Ergänzungsspalten C, E und F. Die Bedeutung der darin enthaltenen Codes ist dem Anhang 15.6 zu entnehmen.

Hinweis: Die mit einem Stern (*) gekennzeichneten Einstelloptionen betreffen in Verbundrechnersystemen (Clustersystemen) sämtliche Einzelrechner (Nodes) gleichermaßen.

1 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 jedes filternde System wie Virenscanner, Firewalls oder Intrusion Detection Systems (IDS). Es handelt sich um ein dediziertes Schutzsystem, das als Appliance dem internen Unternehmens- oder Behördennetzwerk vorgeschaltet wird. Internetgebundene Applikationen wie beispielsweise der Internetbrowser werden nicht mehr auf dem Arbeitsplatzrechner, sondern auf TightGate-Pro Server ausgeführt. Deren Zugriffe in das Internet erfolgen ausschließlich vom vorgeschalteten Schutzsystem aus. Lediglich die Bildschirmausgabe der betreffenden Programme wird in das interne Netzwerk übertragen und auf den Arbeitsplatzrechnern angezeigt. Zugleich werden Maus- und Tastaturinformationen von den Arbeitsplatzrechnern an TightGate-Pro Server übermittelt und die dort ausgeführten Programme aus sicherer Distanz ferngesteuert. Zur Datenübertragung dient vorrangig ein funktionsspezifisches VNC-Protokoll mit dem Übertragungsstandard RFB (Remote Frame Buffer). Das entsprechende Viewer-Programm (VNC-Viewer) wird seitens der m-privacy GmbH in speziell angepassten und optimierten Versionen lizenzkostenfrei zur Verfügung gestellt.

TightGate-Pro bietet volle Internetfunktionalität auch in kritischen Infrastrukturen und Betriebsumgebungen mit hohem Schutzbedarf. Das System unterbindet infolge der physikalischen Trennung von der „Gefahrenquelle Internet“ zuverlässig jede Form von Angriffen auf die Arbeitsstation und das interne Netzwerk, wie sie beispielsweise infolge von Sicherheitslücken in internetgebundenen Applikationen realisierbar sind. Die Nutzung aktiver Inhalte sowie die Wiedergabe von Multimediainhalten ist dennoch vollumfänglich und ohne Gefährdung interner Ressourcen möglich. TightGate-Pro Server verfügt weiterhin über einen starken Eigenschutz durch das Konzept der „administrativen Gewaltenteilung“ (rollenbasierte Administration ohne Root- oder Superuser-Konto) in Verbindung mit feingranularer Zugriffsrechtekontrolle und starker Härtung des zugrunde liegenden Serverbetriebssystems nach dem aktuellen Stand der IT-Sicherheitstechnik.

1.1 Terminologie

Dieses Administrationshandbuch dient als Anleitungs- und Nachschlagewerk für alle, die sich mit der Konfiguration und Verwaltung von TightGate-Pro befassen. Erläuterungen, Hinweise, Warnungen und Tabellen schildern die korrekte Verwendung des Schutzsystems und unterstützen den Administrator bei der Vermeidung von Sicherheitsrisiken infolge fehlerhafter Konfiguration oder Nutzung. Ergänzende Hintergrundinformationen ermöglichen es, die Leistungsfähigkeit von TightGate-Pro voll auszuschöpfen und auch auf seltenere Spezialfälle im Produktivbetrieb angemessen zu reagieren.

Im Rahmen der folgenden Erläuterungen wird zwischen Benutzern und Administratoren unterschieden. Benutzer melden sich ausschließlich an der grafischen Benutzeroberfläche über die Viewer-Software an TightGate-Pro Server an. Ein Benutzer des dedizierten ReCoB-Systems TightGate-Pro ist in der Lage, mit dem Internetbrowser auf Webinhalte zuzugreifen, Textinhalte über die Zwischenablage zwischen TightGate-Pro Server und dem eigenen Arbeitsplatzrechner auszutauschen sowie optional den Audiokanal zur Tonwiedergabe zu nutzen (z. B. zur Wiedergabe von Multimediainhalten). Weiterhin besteht für Benutzer die technische Möglichkeit zum Dateiaustausch zwischen TightGate-Pro Server und dem eigenen Arbeitsplatzrechner über eine gesicherte Dateischleuse. Im Bedarfsfall kann der Benutzer in Eigenregie auf Sicherungskopien eigener Daten zugreifen und diese zurückspielen.

Administratoren arbeiten im Verwaltungsbereich von TightGate-Pro Server und nutzen regelmäßig Konsolenzugänge über SSH. Für die speziellen Administratorenrollen ***root*** und ***security*** (bei TightGate-Pro (CC) Version 1.4 Server nur im sogenannten Softmode verfügbar) muss der Administratorenzugang über SSH vor Benutzung explizit freigegeben werden. Administratorenzugänge direkt an der Konsole (am Gerät) sind in jedem Fall und zeitlich unbegrenzt möglich.

1.2 TightGate-Pro und TightGate-Pro (CC) Version 1.4

Das ReCoB-System TightGate-Pro ist in zwei Varianten verfügbar. Diese sind TightGate-Pro für Standardumgebungen (im Folgenden nur als „TightGate-Pro“ bezeichnet) und TightGate-Pro (CC) Version 1.4 für CC-konforme Umgebungen. TightGate-Pro (CC) Version 1.4 unterscheidet sich von TightGate-Pro für Standardumgebungen maßgeblich durch einige Voreinstellungen sowie die Handhabung des Dateiaustauschs zwischen Server und Klientenrechner:

- TightGate-Pro (CC) Version 1.4 Server wird mit werkseitig deaktiviertem Textaustausch via Zwischenablage ausgeliefert. Diese Einstellung kann durch den Administrator config geändert werden. Das Viewer-Programm TightGate-Pro (CC) Version 1.4 Client wird werkseitig mit der Voreinstellung zur Einzelbestätigung eines jeden Texttransfers ausgeliefert.
- Die Administrationsrollen ***root*** und ***security*** sind auch in TightGate-Pro (CC) Version 1.4 Server vorhanden, können sich jedoch nur im sogenannten Softmode (bei deaktivierter RSBAC-Kontrolle) anmelden. Zugleich wird der VNC-Server aus Sicherheitsgründen deaktiviert, sodass eine Anmeldung von Klienten über den Viewer nicht möglich ist.

Hinweis: Weitere Detailunterschiede werden bei den jeweiligen Einstelloptionen erläutert.

Achtung: TightGate-Pro Server und TightGate-Pro (CC) Version 1.4 Server dürfen nur mit Viewer-Programmen (Klienten) der m-privacy GmbH verwendet werden. TightGate-Pro Client beziehungsweise TightGate-Pro (CC) Version 1.4 Client sind daher obligatorisch, alternative Viewer-Programme sind nicht nutzbar. Die Systemadministration muss sicherstellen, dass Installation und Betrieb alternativer Klientenprogramme (VNC-Viewer) auf den Arbeitsplatzrechnern (Klientenrechnern) nicht möglich sind. Ein CC-konformes Gesamtsystem ergibt sich nur in der Kombination TightGate-Pro (CC) Version 1.4 Server und TightGate-Pro (CC) Version 1.4 Client.

2 Sicherheitskonzept

2.1 Einsatzbereich und Benutzeroptionen

Der vorrangige Einsatzbereich von TightGate-Pro ist die Nutzung des Internets zur Recherche und E-Mail-Kommunikation an Arbeitsplätzen mit erhöhtem Schutzbedarf. Dabei kann dieser erhöhte Schutzbedarf aus der Art der intern verarbeiteten Daten oder aus gesetzlichen Vorgaben resultieren. Mitunter setzen auch interne Fachanwendungen den Einsatz älterer oder weniger stark gesicherter Applikationen voraus, sodass aus diesem Grund eine Trennung des internen Netzwerks vom Internet geboten erscheint.

Ein Benutzer des dedizierten ReCoB-Systems TightGate-Pro ist in der Lage, mit dem Internetbrowser auf Webinhalte zuzugreifen, Textinhalte über die Zwischenablage zwischen TightGate-Pro Server und dem eigenen Arbeitsplatzrechner auszutauschen sowie optional den Audiokanal zur Tonwiedergabe zu nutzen (z. B. zur Wiedergabe von Multimediainhalten). Weiterhin besteht für Benutzer die technische Möglichkeit zum Dateiaustausch zwischen TightGate-Pro Server und dem eigenen Arbeitsplatzrechner über eine gesicherte Dateischleuse. Im Bedarfsfall kann der Benutzer in Eigenregie auf Sicherungskopien eigener Daten zugreifen und diese zurückspielen.

Hinweis: Ein Benutzer kann auf TightGate-Pro Server generell keine Administratorrechte ausüben und darf die betreffenden Einstellmenüs von Administratorrollen nicht einsehen. Administratorrechte können nicht auf einen Benutzer übertragen werden, die Berechtigungen des Benutzers sind bei TightGate-Pro Server auch nicht über Einstelloptionen erweiterbar. Administrative Eingriffe müssen durch dedizierte Administratorenrollen bewerkstelligt werden, die über separate Zugänge verfügen.

2.2 Sicherheitskomponenten und -prinzipien

Das Konzept von TightGate-Pro beruht auf dem Zusammenspiel mehrerer Sicherheitskomponenten und -prinzipien.

2.2.1 Gehärtetes Server-Betriebssystem

- Beschränkung auf notwendige Dienste und Komponenten
- Bevorzugte Auswahl sicherheitsoptimierter Dienste
- Feingranulare Zugriffskontrolle mittels RSBAC
- Kern-Sicherheitserweiterung PaX gegen Buffer-Overflows
- Sicherheitsoptimierte Kompilierung quelloffener Programme mit Stack-Schutz und Kapselung überlaufgefährdeter Funktionen.

2.2.2 Abbildung organisatorischer und rechtlicher Vorgaben

- Alle Dienste laufen mit angepassten RSBAC-Rollenrechten, welche u. a. für Netzwerkzugriffe nur positiv definierte Aktionen zulassen.
- Die Administrationsrechte wurden in bereichsspezifische Rollen aufgeteilt – es gibt keinen „Superuser“.
- Lokale Firewall-Regeln nach dem Minimalprinzip verhindern IP-Spoofing, unerwünschte Verbindungsaufbauten und Sicherheitsrisiken z. B. durch vertauschte Netzwerkkabel.
- Bereits implementierte zweckgebundene Rollen (z. B. Revision/Datenschutzbeauftragter) erleichtern die verteilte Aufgabenerfüllung und setzen organisatorische und rechtliche Vorgaben verbindlich um („Abbildung von Recht in Technik“).
- Revisionssichere Protokollierung aller sicherheitsrelevanten Änderungen von Systemeinstellungen.
- Zugriff auf Backup-Daten, eigenständige Rücksicherung durch den jeweiligen Benutzer und optionale Verschlüsselung des Backups, sobald es das gesicherte System verlässt.
- Unterstützung von Log-Pseudonymisierung und externem Logserver.

2.2.3 TightGate-Pro Server ist stellvertretende Ausführungsumgebung

- Interpreter-Programme mit Internetfunktionalität (Browser, Mail-Client und Viewer) werden stellvertretend in sicherer Umgebung ausgeführt und vom Arbeitsplatz aus fernbedient.
- Ein Programm im internen Netz (Intranet) kann nicht direkt auf Programme mit Internetfunktionalität zugreifen (Datenabfluss, Fernsteuerung, etc.)
- Ein Programm im Intranet kann über den TCP/IP-Stack nicht direkt mit dem Internet kommunizieren.
- Ein sich im Intranet ausbreitender Virus o. ä. kann sich praktisch nicht auf den TightGate-Pro Server fortpflanzen.
- Ein im internen Netz installiertes Programm mit bekannten Sicherheitslücken führt nicht zur Verwundbarkeit durch externe Angreifer.
- Alle Benutzer sind vollständig voneinander getrennt und unterliegen Ressourcen-Beschränkungen. Ein erfolgreicher Angriff auf einen Benutzerzugang kann die Sicherheit der anderen Konten nicht beeinträchtigen. Eine einfache Wiedereinrichtung des Benutzers mit anschließender eigenständiger Wiederherstellung der Daten aus dem letzten Backup erlaubt eine sehr schnelle Wiederaufnahme der unterbrochenen Internetkommunikation mit minimalem Administrationsaufwand.
- Jeder versuchte Regelverstoß (z. B. bei einem Angriff) wird präventiv abgewehrt und protokolliert.

2.2.4 Interpreter

Die Internetbrowser, Mail-User-Agents, Entpacker und Viewer lassen sich als “Interpreter” zusammenfassen. Sie müssen empfangene Daten darstellen oder umwandeln. Auf der Anwendungsebene ist dies der Weg, über den Angriffe durch manipulierte Daten erfolgen. Eine Sicherheitslücke in einem der Interpreter hätte auf dem internen Arbeitsplatz-Rechner möglicherweise weitreichende Folgen:

- Lesen, Löschen oder Verändern von Daten oder Programmen lokal oder im Netzwerk
- Belauschen (sog. „sniffen“) von Netzwerkverbindungen und Tastatureingaben
- Verbreitung auf andere erreichbare Rechner

Da der betroffene Rechner selbst die Möglichkeit hat, ins Internet zu kommunizieren, bestehen auch noch folgende Gefahren:

- Fernsteuerung/Fernwirken auf dem Rechner durch entfernten Angreifer
- Einrichtung einer dauerhaften Hintertür (resistent gegen Sicherheits-Updates)
- Rückfluss gesammelter Daten an Angreifer (Spionage)

Zusammenfassung
Durch die strikte Trennung der Ausführungsumgebung in Kombination mit zusätzlicher Kapselung der ausführbaren Programme lässt sich auf TightGate-Pro Server ein höheres Sicherheitsniveau erreichen, als es im internen Netz (Intranet) möglich ist. TightGate-Pro Server hat nicht den Status eines vorgeschalteten Opfersystems, sondern ist ein auf die Aufgabenstellung „Internetkommunikation“ spezialisiertes System, welches bekannten wie zukünftigen Angriffen bestmöglich standhält.

3 Gesicherte Dateischleuse

Die Umsetzung der Schleusenfunktionalität auf TightGate-Pro folgt dem Grundprinzip: Kein Automatismus zur Durchleitung und Weiterverarbeitung von Inhalten. Benutzer sollen aktiv (also bewusst) die Übergabe steuern.

3.1 Kopieren und Einfügen (Copy&Paste)

Zur komfortablen Übertragung von Textpassagen dient die Funktion zum Kopieren und Einfügen (Copy&Paste) über die Zwischenablage. Sie kann sowohl auf TightGate-Pro Server als auch am VNC-Klienten TightGate-Pro Client auf eine Richtung beschränkt oder ganz deaktiviert werden.

Über die Zwischenablage können nur Inhalte mit dem Formatmerkmal TEXT[1] transferiert werden. Per Vorgabewert kann der Transfer über die Zwischenablage in eine Richtung beschränkt werden. Der Transfer über die Zwischenablage kann global oder benutzerindividuell zugelassen oder gesperrt werden.

Für CC-konforme Umgebungen ist der Transfer über die Zwischenablage so eingestellt, dass jede Datenübertragung durch den Benutzer explizit auszulösen ist.

3.2 Dateischleuse

Als Dateischleuse dient das benutzereigene Transferverzeichnis, in welches die zu transferierenden Dateien kopiert werden müssen. Jeder Benutzer kann dies mittels des Dateibrowsers bewerkstelligen. Die Nutzung des Dateitransfers kann wiederum durch die Administration auf TightGate-Pro Server für jeden Benutzer individuell freigegeben oder gesperrt werden.

Aufseiten des internen Netzes erfolgt der Zugriff mittels SFTP[2].

3.3 Sicherheitsmerkmale der Schleusenfunktion

Die Berechtigungen zur Nutzung des Datentransfers zwischen TightGate-Pro Server und internem Netzwerk können in verschiedenen Abstufungen und für einzelne Benutzer eingestellt werden. Alle die Transfer-Ordner passierenden Dateien können optional mittels On-Access-Scanner geprüft werden. Die Ausführung von Programmen im Transfer-Ordner wird unterbunden, so auch das Anlegen von speziellen Dateien (FiFOs, Devices, etc.).

3.3.1 Transfer per SFTP-Dienst

Der SFTP-Server-Dienst auf TightGate-Pro Server ist mittels RSBAC-Rechten so gekapselt, dass er

- nur in die zugelassenen Transfer-Verzeichnisse transferieren kann
- nur normale Files erzeugen kann (also keine Pipes/FIFOs oder Devices)
- keine Kommandos übergeben kann
- keine Programme starten kann
- keine Ports umleiten kann
- selbst in einem RSBAC-Jail gestartet wird, also andere Prozesse nicht „sieht“

Der Filetransfer per SFTP kann für jeden Benutzer einzeln freigegeben oder gesperrt werden.

Wenn auf TightGate-Pro Server ein Virenscanner aktiviert ist, werden alle Dateien, welche das Schleusenverzeichnis passieren, automatisch gescannt. Wird dabei eine Virusinfektion erkannt, wird der Zugriff auf diese Datei gesperrt. Nur das Löschen der Datei ist dann noch möglich.

1 Das bedeutet nicht, dass nur Texte transferiert werden können. So kann theoretisch jeglicher Inhalt transferiert werden, wenn dieser zuvor in ein TEXT-Format konvertiert wurde z. B. nach base64, welches aber auf der Gegenseite wieder decodiert werden muss.
2 SFTP steht für „Secure File Transfer Protocol“ und ermöglicht den authentifizierten und verschlüsselten Zugriff auf die freigegebenen Ressourcen.

3.3.2 Das Filter-Prinzip

Das Filtern oder Scannen ist ein Pattern-Vergleich. Virenscanner sind ein gutes Beispiel: Von bekannten Viren, Würmern und Trojanern werden als relevant betrachtete Codesegmente zum Vergleich bereitgehalten (die sog. Virenpattern oder Virensignaturen). Auf dem gleichen Prinzip basieren URL- und Web-Content-Filter und auch Paketfilter-Firewalls. Unterschieden werden die Filter-Systeme nach ihrer Grundregel in Positivlisten (Whitelist) oder Negativlisten (Blacklist). Die Whitelist-Systeme folgen dabei dem Prinzip „Alles was nicht explizit erlaubt, ist verboten“. Die Listen enthalten die erlaubten Pattern. Diese Filterart ist bei Paketfiltern die Regel.

Anders die Blacklists: Hier ist alles erlaubt, was nicht explizit auf der „schwarzen Liste“ steht und damit verboten ist. Dies ist das Prinzip von Virenscannern. Beim URL- und Web-Content-Filter sind beide Methoden verbreitet. Mit Hilfe von Listen lassen sich bestimmte Seitenaufrufe recht wirksam verhindern. Als verlässliches Sicherheitssystem genügen sie nicht, da sie schädliche Inhalte nicht als solche identifizieren können. Selbst wenn beispielsweise eine ausnutzbare Sicherheitslücke im Browser bekannt ist, kann man nicht zuverlässig vorhersehen, wie ein zu erwartender Angriff (Exploit) aussehen wird.

Eine URL-Whitelist wäre eine rigorose Maßnahme, deren Einsatz meist schon ob der massiven Beschränkungen bei der Internetnutzung in der Regel unmöglich ist. Doch auch ein solches Vorgehen vertraute auf die Unversehrtheit anderer Systeme, wie z. B. des DNS-Systems und der Anbieter-Website.

3.3.3 Risikoabschätzung

Für eine Risikoabschätzung (tragbar oder nicht tragbar) ist zuvor eine umfassende Analyse und Risikobewertung vorzunehmen. Hierbei sind nicht nur einzelne Risiken und Gegenmaßnahmen zu untersuchen, sondern diese immer im Kontext des Gesamtsystems zu sehen.

Beispiel 1: URL-Whitelist und DNS-spoofing
Die URL-Whitelist, welche den Abruf von unerwünschten Inhalten unterbinden soll, kann mittels DNS-Spoofing ausgehebelt werden. Ist also die Beschränkung mittels URL-Whitelist ein Sicherheitsfeature, so muss das Gefahrenpotenzial von DNS-Spoofing deutlich höher bewertet werden als im Normalfall, bei dem die Sicherheit auf anderen Mechanismen beruht.

Beispiel 2: (Provoziertes) „Verklicken“ des Benutzers
Zu bewerten ist das Risiko eines erfolgreichen Angriffs (oder einer Systemstörung), welche keine programmtechnische Sicherheitslücke ausnutzt, sondern eine Benutzerinteraktion benötigt. Bekannte Beispiele hierfür sind z. B. Werbelinks, auf denen ein „Schließen“-Button gezeigt wird – ein Klick auf das Bild aber direkt zum Werbeangebot führt.

Die Gefahr ist umso größer zu bewerten, je weniger Schritte durch den Benutzer benötigt werden. In der Regel sind viele Angriffe in einem direkt angebundenen System mit einem Klick erfolgreich. In TightGate-Pro muss der Benutzer immer auf beiden Seiten (intern und auf TightGate-Pro Server) aktiv werden und mindestens zwei Klicks in zwei verschiedenen Umgebungen ausführen.

Beispiel 3: Temporäre Gefahren durch bekannte Sicherheitslücken in Softwarekomponenten
Bekannte Sicherheitslücken in internen Programmen (insbesondere in Interpretern) können solange durch gezielte Angriffe ausgenutzt werden, bis ein Sicherheitspatch eingespielt ist. Dieser Zeitraum ist nicht nur vom Hersteller und der Reaktionszeit der internen Administration abhängig, sondern auch von der Kompatibilität (des Patches) mit bestehenden Anwendungen. Insbesondere Fachanwendungen sind oft auf eine bestimmte Softwareversion zugeschnitten und nicht mit aktualisierten Versionen zu betreiben.

In direkt angebundenen Netzwerken müsste bei Nutzung bekannt unsicherer Softwarekomponenten die Internetfunktionalität bis zur Schließung der Sicherheitslücken abgeschaltet werden. Die Zeit bis zur Bereitstellung eines Patches kann längere Zeit dauern - im Fall von Inkompatibilitäten wäre der Aufwand zur Problemlösung noch höher.

3.3.4 Folgerungen für die Nutzung der Schleusenfunktionalität

Man muss das Risiko abschätzen, welcher Schaden für das interne Netz entstehen kann, wenn die Schleuse geöffnet wird und wenn sie geschlossen bleibt.

Einige Gefahren werden beispielhaft untersucht:

Risiko	Direkte Anbindung	TightGate-Pro ohne Schleuse	TightGate-Pro mit Schleuse
Virusinfektion im internen Netz	hoch	sehr gering	gering (Virus-Datei muss aktiv transferiert werden)
Wurminfektion (Mailzugriff per Skript)	hoch	gering (Mail-Skripte kaum ausführbar, Browser hat keinen Zugriff auf Mail-Server oder Mail-Prozess)	gering (Mail-Skripte kaum ausführbar, Browser hat keinen Zugriff auf Mail-Server oder Mail-Prozess)
Datenspionage oder Hintertür-Programme (Rückkanal) im internen Netz	mittel (Rückkanal z. T. per Firewall blockierbar)	sehr gering (kein Zugang zum internen Netz)	gering (Schadprogramm muss aktiv transferiert werden, direkter Internetzugang muss bestehen)
Datenspionage oder Hintertür-Programme (Rückkanal) auf TightGate-Pro Server	n. a.	sehr gering (keine Ausführung unbekannter Programme, kein Netzwerkzugriff für normale Benutzerprogramme, außer E-Mail keine vertraulichen Daten)	gering (keine Ausführung unbekannter Programme, kein Netzwerkzugriff für normale Benutzerprogramme, vertrauliche Daten müssen aktiv transferiert werden)
Datenlöschung oder -veränderung im internen Netzwerk	mittel	sehr gering (kein Zugang zum internen Netz)	gering (Schadprogramm muss aktiv transferiert werden)
“Verklicken” des Benutzers	mittel bis hoch (z. B. gef. Menüs)	sehr gering (Benutzer müsste mehrschrittiger “Anleitung” folgen)	gering (Schadfunktion müsste auf beiden Seiten aktiv sein!)
Sicherheitslücken in anderen eingesetzten Softwarekomponenten	mittel bis sehr hoch (umstandsabhängig)	sehr gering (interne Programme haben keine Internetkommunikation)	gering (Transfer kann bis zum Update temporär unterbrochen werden)

Die Tabelle zu Risiken kann nur als Orientierungshilfe dienen. Sie erhebt keinen Anspruch auf Vollständigkeit und ersetzt nicht die Risikoanalyse im internen Netz.

3.4 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 Server 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 Benutzer account 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 Server 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 Server) 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 Server 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 des TightGate-Pro Server. ***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 Server 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 Server 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	TSF-related	**Rollenbezeichnung**									
	(needed for AGD_OPE 1-2 and 1-3)	**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 Zugriffsrechten	+	-	-	-	-	-	-	-	+	-	-
Shell-Zugriff	-	- **Non-CC: opt. (***)**	-	-	-	-	-	-	+	+	+
Grafische Oberfläche	-	+	-	-	-	-	+	-	-	-	-
Auf Menüfunktionalität beschränkte Benutzerverwaltung (inkl. Benutzerverz. Anlegen und löschen)	-	-	-	+	-	-	-	-	-	-	-
Neustart des Systems und einzelner Komponenten	-	-	+ **anwenden**	+	+	-	-	-	-	+	+

Funktion / Berechtigung	TSF-related	**Rollenbezeichnung**									
	(needed for AGD_OPE 1-2 and 1-3)	**BENUTZER**	**CONFIG**	**MAINT**	**UPDATE**	**BACKUP**	**REVISION**	**TRANSFER**	**SECURITY (*)**	**ROOT (*)**	**ROOT-WARTUNG (*)**
Zeitbeschränkte Zulassung von Administratoranmeldungen per SSH über Netzwerk (***)	**-**	**-**	**-**	**+**	**-**	**-**	**-**	**-**	**manuell (**)**	**-**	**-**
Zulassung von Anmeldungen per SSH über Netzwerk von außerhalb des vorgesehenen Klientennetzwerks (***)	**-**	**-**	**+ einzelne IP-Netze**	**+**	**-**	**-**	**-**	**-**	**-**	**manuell (**)**	**manuell (**)**
Installation von Programmpaketen	**+**	**-**	**-**	**-**	**+ nur vorgegebene Liste**	**-**	**-**	**-**	**-**	**-**	**-**
Über Menüfunktionalität beschränkte Aktualisierung der installierten Programmpakete			**-**	**-**	**+**	**-**	**-**	**-**	**-**	**-**	**-**
Zugriff auf /home-Verzeichnisse	**+**		**-**	**-**	**-**	**-**	**+ nur lesend**	**-**	**+ nur lesend**	**-**	**+**
Editieren von geschützter Konfigurationsdateien			**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	-
Sichern und Zurückspielen der RSBAC-Konfiguration			**-**	**-**	**tw. zurückspielen**	**-**	**-**	**-**	**+**	**-**	**-**
RSBAC-Konfiguration ändern			**-**	**-**	**-**	**-**	**-**	**-**	**+**	**-**	**-**

Funktion / Berechtigung	TSF-related	**Rollenbezeichnung**									
	(needed for AGD_OPE 1-2 and 1-3)	**BENUTZER**	**CONFIG**	**MAINT**	**UPDATE**	**BACKUP**	**REVISION**	**TRANSFER**	**SECURITY (*)**	**ROOT (*)**	**ROOT-WARTUNG (*)**
Voller Zugriff mittels Interpreter auf Abbilder der gewählten Benutzerverzeichnisse			-	-	-	-	+	-	-	-	-
Nur-Lesezugriff auf Systemprotokolle (Logs)			-	-	-	-	+	-	+	+	+
Schreibzugriff auf Systemprotokolle			-	-	-	-	-	-	-	-	-
Netzwerkzugriff			-	-	**eingeschränkt**	**eingeschränkt**	-	-	**eingeschränkt**	**eingeschränkt**	**eingeschränkt**
Prüfen aller Protokolldateien			-	-	-	-	+	-	+	+	+
Nur-Lesezugriff auf Benutzerdaten			-	-	-	-	+	-	+	-	-
Editieren der Konfiguration von ungeschützten Systemdiensten		-	-	-	-	-	-	-	-	-	+
Nutzung von Test-Tools (z. B. netstat)		-	-	**nur iptraf**	-	-	-	-	-	+	+
Aufruf von „rsbac_menu“ (nur lesend)		-	-	-	-	-	-	-	-	+	+

Legende:
(*) Rolle bei TightGate-Pro (CC) Version 1.4 Server im Regelbetrieb nicht verfügbar.
(**) Option ist nur manuell über die Konsole einstellbar, nicht über eine Menüoption.
(***) Kann bei TightGate-Pro (CC) Version 1.4 Server nicht gewählt werden, optional jedoch bei TightGate-Pro Server.

3.5 MIME-Types

MIME ist die Abkürzung für Multipurpose Internet Mail Extensions. Es handelt sich um ein Schema, das TightGate-Pro Server einen Hinweis auf den verwendeten Datentyp gibt.

3.5.1 Medientype und Subtype

Der MIME-Type besteht aus der Angabe eines Medientyps und eines Subtype, die durch einen Schrägstrich voneinander getrennt sind. Z. B. text/html oder image/jpeg.

Folgende Medientypen gibt es:

Medientype	Beschreibung
application	Dateien, die an ein bestimmtes Anwendungsprogramm gebunden sind
audio	Audio-Dateien
image	Bilder, Grafiken, Fotos
message	Nachrichten
text	Dateien mit ASCII-Text
video	Videodateien

Aus dem Medientype ergibt sich die Art der Datenstruktur, also ob die Daten binär oder nach ASCII abgelegt sind. Der Subtype bezieht sich auf die Dateiformate, die an ein bestimmtes Programm gebunden sind oder mit speziellen Programmen oder Plug-ins ausgeführt werden müssen. Subtypes, die mit einem “x-” beginnen, sind Dateien, die auf einem Server ausgeführt werden.

MIME-Type	Beschreibung
inode/x-empty	Leere Datei+Hochladen
application	Alle Applikationen
application/dicom	application/dicom
application/epub+zip	
application/jar	Jar-Archiv
application/javascript	Javascript
application/mac-binhex40	application/mac-binhex40
application/marc	MARC21
application/msword	MS-Word-Datei
application/octet-stream	Unbekannte Binärdatei
application/ogg	OGG-Daten
application/pdf	PDF-Datei
application/pgp	PGP-Daten
application/pgp-encrypted	PGP-verschlüsselte Daten
application/pgp-keys	PGP-Schlüssel
application/pgp-signature	PGP-Signatur
application/postscript	Postscript-Datei

MIME-Type	Beschreibung
application/vnd.cups-raster	Cups-Raster-Datei
application/vnd.fdf	FDF-Dokument
application/vnd.font-fontforge-sfd	Spline-Font-Database
application/vnd.google-earth.kml+xml	OpenGIS-KML-Dokument
application/vnd.google-earth.kmz	Compressed-Google-KML-Document
application/vnd.iccprofile	ICC-Profil
application/vnd.lotus-wordpro	Lotus-WordPro
application/vnd.ms-cab-compressed	CAB-Archive
application/vnd.ms-excel	Excel-File
application/vnd.ms-fontobject	MS-Embedded-OpenType
application/vnd.ms-msi	MS-Installations-Archiv
application/vnd.ms-office	MS-Office-Datei
application/vnd.ms-opentype	OpenType-Font
application/vnd.ms-powerpoint	Powerpoint-Datei
application/vnd.ms-tnef	TNEF-Archive
application/vnd.oasis.opendocument.	Alle OpenDocument
application/vnd.oasis.opendocument.chart	OpenDocument Chart
application/vnd.oasis.opendocument.chart-template	OpenDocument Chart-Template
application/vnd.oasis.opendocument.database	OpenDocument Datenbank
application/vnd.oasis.opendocument.formula	OpenDocument Formel
application/vnd.oasis.opendocument.formula-template	OpenDocument Formel-Template
application/vnd.oasis.opendocument.graphics	OpenDocument Grafik
application/vnd.oasis.opendocument.graphics-template	OpenDocument Grafik-Template
application/vnd.oasis.opendocument.image	OpenDocument Bild
application/vnd.oasis.opendocument.image-template	OpenDocument Bild-Template
application/vnd.oasis.opendocument.presentation	OpenDocument Präsentation
application/vnd.oasis.opendocument.presentation-template	OpenDocument Präsentations-Template
application/vnd.oasis.opendocument.spreadsheet	OpenDocument Tabelle
application/vnd.oasis.opendocument.spreadsheet-template	OpenDocument Tabellen-Template
application/vnd.oasis.opendocument.text	OpenDocument Text
application/vnd.oasis.opendocument.text-master	OpenDocument Text-Master
application/vnd.oasis.opendocument.text-template	OpenDocument Text-Template
application/vnd.oasis.opendocument.text-web	OpenDocument Text-Web

MIME-Type	Beschreibung
application/vnd.openxmlformats-officedocument.wordprocessingml.document	Microsoft Word 2007+
application/vnd.openxmlformats-officedocument.presentationml.presentation	Microsoft PowerPoint 2007+
application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	Microsoft Excel 2007+
application/vnd.rn-realmedia	RealMedia-Datenstrom
application/vnd.symbian.install	application/vnd.symbian.install
application/vnd.tcpdump.pcap	tcpdump-Capture-Datei
application/warc	WARC-Archiv
application/x-123	Lotus-1-2-3
application/x-7z-compressed	7z-komprimierte Datei
application/x-adrift	application/x-adrift
application/x-arc	ARC-Archiv
application/x-archive	application/x-archive
application/x-arj	ARJ-Archiv
application/x-awk	AWK-Skript
application/x-bittorrent	Bittorrent-Datei
application/x-bzip2	BZip2-komprimierte Datei
application/x-compress	Compress-komprimierte Datei
application/x-coredump	Linux-Elf-Coredump
application/x-cpio	CPIO-Archiv
application/x-dbase	DBase-Datei
application/x-dbf	DBF-Datei
application/x-dbm	application/x-dbm
application/x-debian-package	Debian-Paket
application/x-dosexec	DOS-Programm
application/x-dvi	DVI-Datei
application/x-eet	application/x-eet
application/x-elc	Emacs-Lisp
application/x-epoc-agenda	Epoc-Agenda
application/x-epoc-app	Epoc-OPL-Programm
application/x-epoc-data	Epoc-Daten
application/x-epoc-jotter	Epoc-Jotter-Datei
application/x-epoc-opl	Epoc-OPL-Programm
application/x-epoc-opo	Epoc-OPL-Programm
application/x-epoc-sheet	Epoc-Sheet-Datei
application/x-epoc-word	Epoc-Word-Datei

MIME-Type	Beschreibung
application/x-executable	Linux-Elf-Programm
application/x-freemind	Freemind-Dokument
application/x-freeplane	Freeplane-Dokument
application/x-font-sfn	X11-SNF-Font
application/x-font-ttf	X11-TTF-Font
application/x-gdbm	application/x-gdbm
application/x-gnumeric	application/x-gnumeric
application/x-gzip	GZip-komprimierte Datei
application/x-hdf	Hierarchical-Data-Format
application/x-hwp	Hangul (Korean) Word Processor File 2000
application/x-ia-arc	Internet-Archive-Datei
application/x-ichitaro4	Ichitaro-Dokument-v4
application/x-ichitaro5	Ichitaro-Dokument-v5
application/x-ichitaro6	Ichitaro-Dokument-v6
application/x-ima	Floppy-Image
application/x-iso9660-image	ISO9660-CD-Image
application/x-java-applet	application/x-java-applet
application/x-java-jce-keystore	application/x-java-jce-keystore
application/x-java-keystore	Java-KeyStore
application/x-java-pack200	Java-Pack-200
application/x-gnucash	GnuCash-Datei
application/x-gnumeric	Gnumeric-Spreadsheet
application/x-gnupg-keyring	GnuPG-Keyring
application/x-kdelnk	KDE-Link
application/x-lha	LHA-Archiv
application/x-lharc	LHArc-Archiv
application/x-lrzip	LRZIP-komprimierte Datei
application/x-lzma	LZMA-komprimierte Datei
application/x-mdx	MDX-Datei
application/x-mif	FrameMaker-Datei
application/x-msaccess	MS-Access-Datei
application/x-ms-reader	Microsoft-Reader-eBook-Data
application/x-object	Linux-Elf-Objekt-Datei
application/x-pgp-keyring	PGP-Keyring
application/x-pnf	Windows Precompiled iNF
application/x-quark-xpress-3	Quark-Xpress-Datei
application/x-quicktime-player	Quicktime-Player

MIME-Type	Beschreibung
application/x-rar	RAR-Archiv
application/x-rpm	RPM-Paket
application/x-sc	SC-Spreadsheet
application/x-scribus	Scribus-Dokument
application/x-setupscript	Microsoft-Windows-Autorun-Skript
application/x-sharedlib	Linux-Elf-Bibliotheks-Datei
application/x-shockwave-flash	Shockwave-Flash
application/x-stuffit	StuffIt-Archiv
application/x-svr4-package	pkg-Datenstrom (SVR4)
application/x-tar	TAR-Archiv
application/x-tex-tfm	TeX-Schrift
application/x-tokyocabinet-btree	Tokyocabinet-Btree
application/x-tokyocabinet-fixed	Tokyocabinet-Fixed
application/x-tokyocabinet-hash	Tokyocabinet-Hash
application/x-tokyocabinet-table	Tokyocabinet-Table
application/x-wine-extension-ini	Windows-INI
application/x-xz	XZ-komprimierte Datei
application/x-zoo	ZOO-Archiv
application/xml	XML-Datei
application/xml-sitemap	XML-Sitemap
application/zip	ZIP-Archiv
audio	Alle Audio
audio/basic	Basic-/mu-law-/PCM-Audio
audio/midi	Midi-Audio-Datei
audio/mp4	MP4-Audio-Datei
audio/mpeg	MPEG-ADTS-Datei,MP3
audio/vnd.dolby.dd-raw	ATSC A/52,AC-3,Dolby Digital stream
audio/x-adpcm	ISDN mu-law compressed audio
audio/x-aiff	AIFF-Audio
audio/x-ape	Monkey's Audio compressed format
audio/x-dec-basic	Basic-/mu-law-/PCM-Audio
audio/x-flac	Flac-Datei
audio/x-hx-aac-adif	MPEG-ADIF,AAC
audio/x-hx-aac-adts	MPEG-ADTS,AAC
audio/x-mod	audio/x-mod
audio/x-mp4a-latm	MPEG-4 LOAS
audio/x-musepack	Musepack-Audio

MIME-Type	Beschreibung
audio/x-pn-realaudio	RealAudio
audio/x-w64	Wave-64-Audio
audio/x-wav	WAV-Audio-Datei
audio/x-unknown	Unbekannte-Audio-Datei
chemical	Alle Chemicals
chemical/x-pdb	Protein Data Bank data
image	Alle Bilder
image/gif	GIF-Bild
image/jp2	JP2-Bild
image/jpeg	JPEG-Bild
image/jpm	JPM-Bild
image/jpx	JPK-Bild
image/pcx	PCX-Bild
image/png	PNG-Bild
image/svg+xml	SVG+XML-Grafik
image/tiff	TIFF-Bild
image/vnd.adobe.photoshop	Photoshop-Grafik
image/vnd.djvu	Dejavu-Grafik
image/vnd.dwg	DWG AutoDesk AutoCAD
image/x-award-bioslogo	Award-BIOS-Logo
image/x-award-bmp	Award Bitmap
image/x-canon-cr2	Canon-CR2-raw-image
image/x-canon-crw	Canon-CIFF-raw-image
image/x-coreldraw	CorelDraw-Datei
image/x-cpi	CPI-Grafik
image/x-dpx	DPX-Grafik
image/x-epoc-mbm	Epoc-MBM-Grafik
image/x-epoc-sketch	Epoc-Sketch-Grafik
image/x-exr	EXR-Grafik
image/x-icon	MS-Windows-Icon
image/x-lss16	SYSLINUX-LSS16-Image
image/x-ms-bmp	MS-Bitmap-Grafik
image/x-niff	image/x-niff
image/x-olympus-orf	Olympus-ORF-raw-image
image/x-paintnet	Paint.NET-Grafik
image/x-pcx	PCX-Datei
image/x-portable-bitmap	image/x-portable-bitmap

MIME-Type	Beschreibung
image/x-portable-greymap	image/x-portable-greymap
image/x-portable-pixmap	image/x-portable-pixmap
image/x-quicktime	Quicktime-Grafik
image/x-unknown	unbekannte Grafik
image/x-x3f	Foveon-X3F-raw-image
image/x-xcf	GIMP-XCF-Grafik
image/x-xcursor	Xcursor-Daten
image/x-xpmi	XPM-Bild
image/x-xwindowdump	XWD-X-Window-Dump-image
message	Alle Nachrichten
message/news	News-Nachricht
message/rfc822	rfc822-Nachricht
model	Alle Modelle
model/vrml	VRML-Datei
model/x3d	X3D-Datei
rinex	Alle RINEX-Dateien
rinex/broadcast	RINEX-Daten: GEO SBAS Broadcast
rinex/clock	RINEX-Daten: Clock
rinex/meteorological	RINEX-Daten: Meteorologisch
rinex/navigation	RINEX-Daten: Navigation
rinex/observation	RINEX-Daten: Observation
text	Alle Texte
text/calendar	vCalendar-Datei
text/html	HTML-Daten
text/inf	Windows-Setup-Informationen
text/PGP	GPG-verschlüsselte Daten
text/plain	Einfacher Text
text/rtf	RTF-Text
text/texmacs	TeXmacs-Dokument
text/troff	Troff-Dokument
text/vnd.graphviz	Graphviz-Grafik-Text
text/x-asm	Assembler-Quelltext
text/x-awk	AWK-Skript
text/x-bcpl	BCPL-Quelltext
text/x-c	C-Quelltext
text/x-c++	C++-Quelltext
text/x-diff	Diff-Ausgabe

MIME-Type	Beschreibung
text/x-fortran	Fortran-Quelltext
text/x-gawk	GNU-AWK-Skript
text/x-info	text/x-info
text/x-inform	text/x-inform
text/x-java	Java-Quelltext
text/x-lisp	Lisp-/Scheme-Quelltext
text/x-lua	Lua-Skript
text/x-m4	M4-Makro
text/x-makefile	Makefile-Skript
text/x-msdos-batch	DOS-Batch-Datei
text/x-nawk	New-AWK-Skript
text/x-pascal	Pascal-Quelltext
text/x-perl	Perl-Skript
text/x-php	PHP-Skript
text/x-po	GNU-Gettext-Nachrichten-Katalog
text/x-python	Python-Skript
text/x-ruby	Ruby-Skript
text/x-shellscript	Shell-Skript
text/x-tcl	Tcl/Tk-Skript
text/x-tex	TeX-Quelltext
text/x-texinfo	text/x-texinfo
text/x-vcard	VCard
text/x-xmcd	XMCD-Datei
text/xml	XML-Datei
video	Alle Videos
video/3gpp	MPEG4-3GPP
video/3gpp2	MPEG4-3GPP2
video/mp4	video/mp4
video/h264	H264-Video
video/mj2	JPEG-MJ2-Video
video/mp2p	MP2P-Video
video/mp2t	MP2T-Video
video/mp4	MPEG4-Video
video/mp4v-es	video/mp4v-es
video/mpeg	MPEG-Video
video/mpeg4-generic	MPEG4-Generisch
video/mpv	video/mpv

MIME-Type	Beschreibung
video/quicktime	Quicktime-Video
video/sgi	SGI-Video
video/unknown	unbekanntes Video
video/vnd.rn-realvideo	Real-Video
video/webm	WebM-Video
video/x-flc	video/x-flc
video/x-fli	video/x-fli
video/x-flv	video/x-flv
video/x-jng	video/x-jng
video/x-matroska	Matroska-Video
video/x-mng	MNG-Video
video/x-ms-asf	Microsoft-ASF-Video
video/x-msvideo	video/x-msvideo
video/x-sgi-movie	video/x-sgi-movie
video/x-unknown	Unbekanntes Video-Format
x-epoc/x-sisx-app	Symbian-Installationsdatei

3.6 Zusatzmodul „Zentraler GnuPG-Key“

Als Zusatzmodul zu TightGate-Pro Server bietet die m-privacy GmbH ein Modul zur zentralen GnuPG-Integration (PGP). Durch die Kapselung von GnuPG auf TightGate-Pro Server kann allen Benutzern die E-Mail-Verschlüsselung auf sichere Weise zur Verfügung gestellt werden. Die zentrale GnuPG-Integration bietet folgende Vorteile:

- Sichere Verwahrung des geheimen Schlüssels (secret key) auf TightGate-Pro Server
- Kein ungewolltes Auslesen oder Verändern des geheimen Schlüssels durch Benutzer, Programme oder Angreifer
- Zentrale Pflege der Benutzer-IDs des öffentlichen Schlüssels
- Zentrale Administration eines gemeinsamen Schlüsselverzeichnisses
- Benutzerfreundliche Integration von GnuPG / PGP
- Vorbereitet für die Einbindung in eine PKI-Struktur

Die Installation des Moduls für den zentralen GnuPG-Key erfolgt nur durch den Support der m-privacy GmbH oder einen autorisierten Fachpartner. Sobald das Modul „zentraler GnuPG-Key“ installiert ist, erscheint im Menü des Administrators ***maint*** ein weiterer Menüpunkt „GnuPG-Identitäten“. Dort können weitere Benutzer-IDs für den zentralen Schlüssel hinzugefügt und vorhandene entfernt werden. Alle weiteren Änderungen am zentralen geheimen Schlüssel werden durch den Administrator ***maint*** vorgenommen und den Benutzern automatisch zugewiesen.

Der Administrator ***maint*** hat folgende Einstellungsmöglichkeiten für den zentralen GnuPG-Key:

Menüpunkt	Beschreibung
Öff. Schlüsselpfleger	Benutzerkennung, die öffentliche PGP-Keys zentral bereitstellen darf.
Schlüssel auflisten	Anzeige aller Identitäten, die für den geheimen Schlüssel existieren
Primär ID	Auswahl der primären ID für den geheimen Schlüssel

Hinzufügen	Hinzufügen einer neuen Identität für den zentralen Schlüssel
Entfernen	Entfernen einer neuen Identität für den zentralen Schlüssel
Passwort	Ändern des Passwortes für den geheimen Teil des zentralen Schlüssels **Hinweis**: Das Passwort ist auch bei zentralem Schlüssel ebenso wirksam wie bei einem persönlichen Schlüssel.

3.6.1 Verwendung des zentralen GnuPG-Keys bei den Klienten

Sobald der Administrator ***maint*** die Identitäten der einzelnen Benutzer dem zentralen Schlüssel hinzugefügt hat, können diese von den Benutzern verwendet werden. Nachdem die Schlüssel importiert wurden, werden alle Änderungen (Änderungen der Schlüsselidentitäten durch den Administrator ***maint***) bei den Benutzern automatisch bei jeder Neuanmeldung übernommen. Anschließend können die Benutzer im E-Mail-Programm den geheimen Schlüssel einstellen und verwenden.

3.6.2 Pflege des öffentlichen Schlüsselbundes

Die Pflege des öffentlichen Schlüsselbundes erfolgt durch die als Administrator ***maint*** bestimmte Benutzerkennung.

3.7 Passwortvorgaben

Die Passwortvorgaben für eine Anmeldung eines VNC-Benutzers oder Administrators am TightGate-Pro entsprechend dem Stand der Technik und können weder durch Benutzer noch durch Administratoren verändert oder ausgehebelt werden.

Die nachfolgende Tabelle gibt einen Überblick über die Passwortvorgaben für VNC-Benutzer und Administratoren:

Beschreibung	VNC-Benutzer	Administrator
Wann muss ein Initialpasswort geändert werden?	Bei der ersten Anmeldung	Nie
Wie lange ist die Gültigkeitsdauer eines regulären Passwortes?	Ablaufzeit wird von ***config*** vorgegeben	Keine Ablaufzeit
Wie viele Tage vor Ablauf eines Passwortes bekommen Benutzer einen Hinweis, dass das Passwort ungültig wird?	14 Tage	Kein Hinweis
Welche Mindestlänge gilt für Passwörter?	8 Zeichen Ausnahme: Das Initialpasswort eines neuen Benutzers ist nicht an die Mindestvorgaben für Passwörter gebunden.	8 Zeichen
Wie oft wird die erneute Verwendung bereits verwendeter Passworte verhindert?	8 Wiederholungen	8 Wiederholungen

4 Ergänzungsspalten der Optionstabellen

Die tabellarische Beschreibung der Konfigurationsmenüs dient der verbesserten Übersicht hinsichtlich der zahlreichen Einstelloptionen. Die Ergänzungsspalten unter der Rubrik „Hinweise“ beinhalten erweiterte Informationen, die zum Verständnis der jeweiligen Einstelloption nicht zwingend erforderlich sind, und haben folgende Bedeutung:

4.1 Ergänzungsspalte C: Einstelloptionen für Standardumgebungen

Ist eine Einstelloption in dieser Spalte mit „nc“ gekennzeichnet, so bedeutet für TightGate-Pro (CC) Version 1.4 Server jede Abweichung von den vorgegebenen Werten den Verlust der CC-Konformität. Die betreffenden Parameter sind zwar veränderbar, jedoch weist ein Farbwechsel des Bildschirmhintergrunds nach Orange sowie zusätzliche Statusmeldungen bei den Einstelloptionen und in der Statuszeile auf den nicht CC-konformen Betriebszustand des Systems im Fall einer Abweichung hin. Weiterhin wird dieser nicht CC-konforme Betriebszustand auf der Statusseite von TightGate-Pro Server angezeigt.

Ist eine Einstelloption in dieser Spalte nicht mit „nc“ gekennzeichnet, so ist die betreffende Funktion sowohl für TightGate-Pro Server als auch für TightGate-Pro (CC) Version 1.4 Server relevant. Der Menüpunkt wird in den Administrationsmenüs dargestellt und kann gewählt werden. Die Parameter sind teilweise vorbelegt, können jedoch verändert werden. Die zulässigen Parametertypen und Wertebereiche sind zu beachten.

4.2 Ergänzungsspalte E: Parametertypen und Wertebereiche der Eingabewerte

Nachfolgende Übersicht verdeutlicht die Form der Eingabewerte, die von TightGate-Pro Server erwartet werden. Eingabewerte und Wertebereiche unterscheiden sich je nach Einstelloption. Alle Eingabewerte werden systemseitig geprüft. Ungeeignete bzw. unplausible Eingabewerte werden abgelehnt und können nicht übernommen werden. In manchen Fällen unterliegen die Eingabewerte individuellen Beschränkungen, die teilweise mit Sicherheitsimplikationen einhergehen. Dies betrifft insbesondere Passworte, die nicht alle möglichen Zeichen enthalten dürfen und überdies gegen eine interne Passworthistorie sowie gegen weitere Kriterien geprüft werden.

Code	Parametertyp und Wertebereich, besondere Hinweise zum Eingabewert
E0	**Kein Eingabewert.** Die betreffende Aktion wird nach Anwahl des Menüpunkt ohne weitere Rückfrage ausgeführt. Es wird ein Hinweistext angezeigt, der die Ausführung der Aktion bestätigt. Umfangreiche Aktionen haben u. U. die Anzeige einer ausführlichen Statusinformation zur Folge. Nach Abschluss der Aktion erfolgt Rückkehr in das jeweilige Administrationsmenü.
E1	**Auswahlliste.** Setzen einer Option durch Aktivierung und Betätigung der Leertaste. Alternativ kann eine Option durch Zeigen und Klicken mit der Maus gesetzt werden. Es können ausschließlich die Elemente der Auswahlliste selektiert werden. Die Eingabe freier Parameter ist nicht möglich.
E2	**Sicherheitsabfrage bzw. zu bestätigender Hinweistext.** Nach Anwahl der jeweiligen Einstelloption erscheint ein Hinweistext mit entsprechender Sicherheitsabfrage. Nur bei Bestätigung der Sicherheitsabfrage wird die betreffende Einstelloption wirksam bzw. die ausgewählte Aktion wird ausgeführt. Der angezeigte Hinweistext erläutert die Funktion und die Auswirkungen der Einstelloption bzw. Aktion. Die Sicherheitsabfrage dient dazu, die ungewollte Auslösung weitreichender Aktionen bzw. Einstelloptionen zu verhindern.
E3	**E-Mail-Adresse(n).** Die Adresse ist in der Form <text>@<domain> anzugeben. Es können sämtliche Zeichen verwendet werden, die in standardkonformen E-Mail-Adressen zulässig sind. Groß- und Kleinschreibung wird nicht unterschieden. Werden unzulässige Zeichen für die Eingabe verwendet, erfolgt eine Fehlermeldung.
E4	**Freitexteingabe.** Die Freitexteingabe kann in ihrer maximalen Länge beschränkt sein. Zu ver-

Code	Parametertyp und Wertebereich, besondere Hinweise zum Eingabewert
	gebende Benutzernamen dürfen generell maximal 63 Zeichen umfassen, Passworte maximal 255 Zeichen. Näheres ist dem Hinweistext zur Einstelloption zu entnehmen, der am Bildschirm ausgegeben wird. Werden unzulässige Zeichen für die Eingabe verwendet, erfolgt eine Fehlermeldung.
E5	**IPv4-Adresse(n).** Eine oder mehrere IPv4-Adressen sind in CIDR-Notation a.b.c.d/e anzugeben. Die Anteile a bis d können einen dezimalen Wertebereich von 0-255 annehmen. Der Anteil e gibt die Zahl der Valid Bits an, deren Wert in der Subnetzmaske gleich „1“ ist. Die Anteile a bis d sind mit Punkten zu trennen, der Anteil e nach einem Schrägstrich anzuschließen. In einigen Fällen ist zusätzlich zur IPv4-Adresse ein konkreter Port anzugeben; dieser ist Dezimalwert mit einem Doppelpunkt als Trennzeichen dem Anteil d nachzustellen. IPv4-Adressen dürfen keine Leerzeichen oder sonstige Zeichen enthalten. Die Angabe eines Anteils e ist nicht in allen Fällen möglich.
E6	**Dezimalwert.** Dieser Parametertyp wird beispielsweise bei Zeitangaben in Sekunden oder Tagen verwendet. Hinsichtlich der kontextspezifischen Bedeutung der Angabe und der möglichen Beschränkung des zugelassenen Wertebereichs sind die jeweiligen Hinweistexte zu beachten.
E7	**Sonderformat.** Die Form der erwarteten Eingabe ist dem angezeigten Hinweistext auf dem Bildschirm zu entnehmen.

4.3 Ergänzungsspalte F: Fehlermeldungen und Hinweistexte

Die Menüführung von TightGate-Pro Server unterstützt den Systemadministrator durch eine Vielzahl von Fehlermeldungen und Hinweistexten. Diese werden kontextsensitiv entsprechend der bestehenden Fehlerbedingung bzw. Bediensituation ausgegeben. In allen komplexeren, konfigurationsspezifischen Zusammenhängen werden im Fehlerfall selbsterklärende Fehlermeldungen angezeigt, die eindeutige Rückschlüsse auf die Fehlerursache erlauben und Hinweise zur Fehlerbehebung vermitteln.

Code	Meldungsinhalt und Hinweise zur Fehlerbehebung
F0	**Kein Fehler.** Die Meldung weist auf den erfolgreichen Abschluss einer Aktion entsprechend des administrativen Eingriffs hin. Die Meldung muss durch den Systemadministrator bestätigt werden und hat keine weitergehenden Folgen. In einigen Fällen erfolgt die Rückkehr zum Menü, ohne dass eine Meldung ausgegeben wird.
F1	**Eingabewerte nicht angewendet.** In einigen Fällen müssen Eingabewerte explizit angewendet werden, um systemweit wirksam zu sein. Hierzu stehen die Menüpunkte ***Sanft Anwenden*** und ***Voll Anwenden*** zur Verfügung. Nicht angewendete Eingabewerte bleiben gespeichert. Auf gespeicherte, jedoch noch nicht angewendete Eingabewerte wird in einem farbigen Hinweistext am Bildschirm dauerhaft hingewiesen, solange die Werte noch nicht angewendet wurden. Bei erneuter Anmeldung des Administrators wird in einem zu bestätigenden Dialogfeld auf gespeicherte, jedoch noch nicht angewendete Eingabewerte hingewiesen.
F2	**Eingabewerte nicht gespeichert.** In einigen Fällen sind die Eingabewerte mittel Menüpunkt explizit zu speichern, bevor das betreffende Menü verlassen wird. Nicht gespeicherte Eingabewerte gehen bei Verlassen des Menüs verloren. Das Verlassen des Menüs kann abgebrochen und die Speicherung des Eingabewerts nachgeholt werden.
F3	**Fehlerhafte E-Mail-Adresse.** E-Mail-Adressen, die kein „@“-Zeichen enthalten, werden beanstandet. Die Eingabe ist zu wiederholen oder der Vorgang ist abzubrechen. Im letzteren Fall bleiben die bisherigen Eintragungen (sofern vorhanden) unverändert.
F4	**Netzwerkproblem.** Aufgrund fehlerhafter Netzwerkeinstellungen kommt eine Datenübertragung nicht zustande. Die Netzwerkeinstellungen sind zu prüfen und zu rekonfigurieren. Die betreffende Aktion muss im Anschluss erneut ausgelöst werden.
F5	**Fehlerhafte IPv4-Adresse.** Die IPv4-Adresse muss im erwarteten Format angegeben werden, andernfalls kann die Eingabe nicht vom System verarbeitet werden. Ist die Eingabe mehrerer

	IPv4-Adressen möglich, ist auf die korrekte Separierung der Adressen mittels des vorgeschriebenen Trennzeichens zu achten. Zusätzlich wird der vorgeschriebene Wertebereich der Anteile der IPv4-Adresse geprüft. Eingaben außerhalb des vorgeschriebenen Wertebereichs werden mit einer Fehlermeldung beanstandet. Die Eingabe ist zu wiederholen oder der Vorgang ist abzubrechen. Im letzteren Fall bleiben die bisherigen Eintragungen (sofern vorhanden) unverändert.
F6	**Unzulässiger Wertebereich.** Dezimalwerte, die den im jeweiligen Kontext vorgeschriebenen Wertebereich verlassen, werden mit einer Fehlermeldung zurückgewiesen. Dies betrifft auch die Anteile von IPv4-Adressen. Die Eingabe ist zu wiederholen oder der Vorgang ist abzubrechen. Im letzteren Fall bleiben die bisherigen Eintragungen (sofern vorhanden) unverändert.
F7	**Vorgeschriebenes Sonderformat nicht eingehalten.** In bestimmten Fällen sind Daten gemäß eines im Hinweistext auf dem Bildschirm spezifizierten Sonderformats einzugeben. Wird das vorgeschriebene Sonderformat nicht eingehalten, erfolgt Zurückweisung der Eingabe mit einer Fehlermeldung. Die Eingabe ist zu wiederholen oder der Vorgang ist abzubrechen. Im letzteren Fall bleiben die bisherigen Eintragungen (sofern vorhanden) unverändert.
F8	**Kontextspezifischer Fehler.** Aufgrund einer Fehlerbedingung im jeweiligen Konfigurationskontext wird eine spezifische Fehlermeldung ausgegeben. Diese ist selbsterklärend und gibt eindeutige Hinweise auf die Fehlerursache sowie zur Fehlerbehebung.

5 Systemüberwachung mit Nagios

Die Serversysteme der m-privacy GmbH verfügen über eine Nagios-Systemüberwachung. Damit lassen sich wichtige Betriebszustände aus der Ferne prüfen, sodass bereits vor einer Überschreitung kritischer Grenzwerte Gegenmaßnahmen ergriffen werden können. Nachfolgende Aufstellung gibt einen Überblick über die implementierten Nagios-Prüfpunkte (Checks).

Warnung: Zum Erhalt der CC-Konformität ist es bei TightGate-Pro (CC) Version 1.4 Server zwingend erforderlich, dass sich der als Nagios-Überwachunsstation agierende Rechner außerhalb des Klientennetzwerks befindet. Damit eine Verbindung mit TightGate-Pro (CC) Version 1.4 Server dennoch erfolgen kann, muss die IPv4-Adresse dieses Rechners unter ***config > Einstellungen > Wartung und Updates > Nagios / Storage IP*** hinterlegt sein.

Nicht jedes System verfügt über die Gesamtzahl der möglichen Sensoren, sodass nicht immer alle Prüfpunkte aktiv sein müssen. Die angegebenen Schwellwerte sind vordefiniert, können jedoch bei Bedarf geändert werden. Wird ein Nagios-Prüfpunkt nicht benötigt oder ist dessen Überwachung bzw. Anzeige nicht erwünscht, kann dieser Prüfpunkt aus den generierten Übersichten entfernt werden. Nähere Informationen erteilt der technische Kundendienst der m-privacy GmbH.

5.1 Übersicht der Sensoren, Prüfpunkte und Aktivitäten

Prüfpunkt	Beschreibung	OK	Warnung (warning)	Problem (critical)	Aktivität, falls Warnung ausgegeben	Aktivität, falls Problem gemeldet
backup	Prüft auf vorhandenes Backup und eventuell aufgetretene Fehler. Gibt Datum und Uhrzeit des zuletzt angelegten Backups zurück, falls gefunden.	Backup vorhanden und fehlerfrei.	Backup fehlerhaft.	Backup nicht vorhanden oder Dienst nicht verfügbar.	Als Administrator *backuser* anmelden und Protokoll auf Fehler überprüfen. Es kann mit dem Befehl ***Letztes Protokoll anzeigen*** aufgerufen werden.	Überprüfen, ob als Administrator *backuser* unter ***Konfiguration > Häufigkeit*** eventuell unpassende Einstellungen gewählt wurden. Dann z. B. im Protokoll nachsehen, ob ein Backup erstellt wurde und ggf. Fehler überprüfen.
bug	Sucht in der Datei kern.log nach Schlüsselworten, die auf Kernfehler hindeuten.	Kein Schlüssel-wort gefunden.	---	Schlüsselwort(e) gefunden.	Technischen Kundendienst der m-privacy GmbH informieren.	
check_apply	Zeigt an, ob ein ***Sanft Anwenden*** für den Administrator *config* aussteht und nachgeholt werden muss.	No config apply needed.	Config apply needed.	---	Fehlendes ***Sanft Anwenden*** sollte umgehend nachgeholt werden. Insbesondere im Rechnerverbund (Cluster) kann andernfalls instabiler Systembetrieb die Folge sein.	
cron	Prüft, ob und wie viele Cron-Jobs laufen.	1 bis 10 Cron-Jobs laufen	11 bis 20 Cron-Jobs laufen	mehr als 20 oder keine Cron-Jobs laufen	Als Administrator *root* anmelden und Konsole aufrufen. Befehlsfolge ***ps tree -ah*** lokalisiert den blockierten Cron-Job. Infrage kommende Dienste prüfen und entsprechende Maßnahmen ergreifen, z. B. als Administrator *config* ***Sanft Anwenden*** oder auch Neustart des Systems.	

Prüfpunkt	Beschreibung	OK	Warnung (warning)	Problem (critical)	Aktivität, falls Warnung ausgegeben	Aktivität, falls Problem gemeldet
disk	Prüft freien Speicher auf den Festplatten für / und inode.	> 20 % frei	> 10 %, aber < 20 % frei	< 10 % frei	Statusseite des entsprechenden Systems aufrufen und Massenspeicher auf Belegung überprüfen. Bei Platzmangel sollten insbesondere die Benutzerverzeichnisse in /home geprüft werden. Evtl. können z. B. alte Backups gelöscht werden. Weiterhin sollten die Logdateien in /var/log geprüft werden. Zu große Logdateien können gelöscht werden, um Platz auf dem Datenträger zu schaffen.	
dns	Prüft den eingetragenen DNS-Server. Gibt die IP-Adresse und die Antwortzeit des DNS-Servers zurück.	Auslösung der IP-Adresse möglich.	---	Auflösung der IP-Adresse nicht möglich.	DNS-Server überprüfen ggf. alternativen DNS-Server eintragen.	
homeuser-mount	Prüft, ob /home/user im Verzeichnisbaum eingehängt ist. Gibt den Pfad von /home/user zurück.	Eingehängt.	---	Nicht eingehängt.	Festplatte überprüfen, ggf. Benutzerverzeichnisse probehalber von Hand einhängen. Es könnte sich auch um einen Dateisystemfehler handeln, daher wird die Benachrichtigung des technischen Kundendienstes der m-privacy GmbH empfohlen.	
glusterhomeuser	Prüft, ob der für den Betrieb des Dateisystems entscheidende GlusterFS-Server für /home/user auf diesem System läuft.	Läuft.	---	Läuft nicht.	Sollte sich das Problem durch ***Sanft Anwenden*** nicht lösen lassen, ist der technische Kundendienst der m-privacy GmbH zu benachrichtigen.	
gluster-backup		Erreichbar.	---	Nicht erreichbar.	Sollte sich das Problem durch ***Sanft Anwenden*** nicht lösen lassen, ist der technische Kundendienst der m-privacy GmbH zu benachrichtigen.	
backup-mount	Prüft, ob /home/backuser /backup korrekt im Verzeichnisbaum eingehängt wurde.	Eingehängt.	---	Nicht eingehängt.	Festplatte überprüfen, ggf. Benutzerverzeichnisse probehalber von Hand einhängen. Es könnte sich um einen Dateisystemfehler handeln, daher wird die Benachrichtigung des technischen Kundendienstes der m-privacy GmbH empfohlen.	
license	Prüft auf gültige Lizenz und gibt das Ablaufdatum zurück.	Lizenz gültig.	---	Lizenz ungültig.	Die Lizenz muss über den technischen Kundendienst der m-privacy GmbH erneuert werden.	
load	Gibt die durchschnittliche Systemlast der letzten Minute, der letzten 5 bzw. 15 Minuten zurück.	Last < 40	Last > 40 (1,5,15 min)	Last > 80,70,70 (1,5,15 min)	Als Administrator *root* anmelden und eine Konsole öffnen. Der Befehl ***atop*** zeigt die Prozessübersicht unter Angabe der Last pro Prozess. Die Liste kann durch Eingabe von ***p*** im Fenster nach dem Lastwert sortiert werden. Prozesse, die besonders hohe Last verursachen, können mittels ***kill*** beendet werden. Auch ein Neustart des Systems kann dazu führen, dass diese Prozesse nicht mehr gestartet werden oder deutlich weniger Last verursachen. In jedem Fall ist bei übermäßiger Systemlast der technische Kundendienst der m-privacy GmbH zu informieren.	

Prüfpunkt	Beschreibung	OK	Warnung (warning)	Problem (critical)	Aktivität, falls Warnung ausgegeben	Aktivität, falls Problem gemeldet
ntp	Prüft die Erreichbarkeit des lokalen NTP-Zeitservers des jeweiligen Nodes und gibt spezifische Parameter zurück.	Erreichbar, Anzeige der Zeitdifferenz.		Nicht erreichbar oder erreichbar und Zeitdifferenz > 1h.	Insbesondere in Clustersystemen müssen alle Nodes dieselbe Systemzeit aufweisen. Ist die Zeitdifferenz zur Referenz des externen NTP-Servers > 1 h, besteht unbedingt Handlungsbedarf! In diesem Fall als *root* anmelden, eine Konsole aufrufen und folgende Schritte ausführen: 1. Lokalen NTP-Server anhalten: ***/etc/init.d/ntp stop*** 2. Lokalen NTP-Server aktualisieren: ***ntpdate IP_des_externen_Zeitservers*** 3. Lokalen NTP-Server wieder starten: ***/etc/init.d/ntp start*** Schlägt dieses Verfahren fehl, könnte der externe NTP-Server unerreichbar sein. Dies kann als Administrator *config* mit dem Menüpunkt ***Netzwerk prüfen*** festgestellt werden. Ggf. sollte ein alternativer externer NTP-Server konfiguriert werden, um einwandfreien Systembetrieb sicherzustellen.	
smart_sd* smart_hd*	Prüft den SMART-Status der jeweiligen Festplatte und gibt den festgestellten Status zurück.	Festplatte OK + aktuelle Temperatur	Temperatur > 45 °C	Temperatur > 50 °C	Wird eine zu hohe Temperatur ausgegeben, sollte die Kühlung des Systems geprüft werden. Falls Festplatte nicht ok ist, werden auch die Fehler des S.M.A.R.T.-Checks der Platte ausgegeben. Maßnahmen können ein Systemstart vom Rettungssystem oder Ausführung eines ***fsck*** sein.	
smtp	Prüft die Erreichbarkeit des SMTP-Servers und gibt dessen Antwortzeit zurück	Erreichbar		Nicht erreichbar.	Nach Anmeldung als Administrator *config* steht der Menüpunkt ***Netzwerk prüfen*** zur Verfügung. Damit kann auch erkannt werden, ob ein SMTP-Server erreichbar ist. Ggf. Konfiguration des Systems prüfen oder Erreichbarkeit des SMTP-Servers sicherstellen.	
ssh	Prüft die Erreichbarkeit einer Secure Shell und gibt die SSH-Version zurück.	Erreichbar.		Nicht erreichbar.	Falls SSH als unerreichbar moniert wird, sollte zunächst als Administrator *config* ein ***Sanft Anwenden*** ausgeführt werden. Wird SSH danach weiterhin in Nagios als nicht erreichbar ausgewiesen, ist ein Neustart des Systems im Recover-Modus erforderlich. Es empfiehlt sich in diesem Fall eine Rücksprache mit dem technischen Kundendienst der m-privacy GmbH.	
swap	Prüft auf freien Swap-Speicher und gibt den Wert des gesetzten Maximalwerts und des freien Speicherplatzes zurück.	> 50% des gesetzten Maximalwerts frei	< 50%, aber > 20% des gesetzten Maximalwerts frei	< 20% des gesetzten Maximalwerts frei	Bei dauerhafter Überschreitung der Grenzwerte zunächst lastreduzierende Maßnahmen ergreifen (z. B. Nutzung der Browser-Add-ons „Flashblock“, „Ad-Block“ und dergl.). Auch eine Erweiterung des Arbeitsspeichers kann Abhilfe schaffen. Es wird empfohlen, die Maßnahmen mit dem technischen Kundendienst der m-privacy GmbH zu erörtern.	
timedupdate	Anzeige de Datums und der Uhrzeit geplanter Updates bzw. Deaktivierung geplanter Updates.	OK: Timed update is disabled oder OK: Timed update on [Zeitstempel]	---	---		
total_procs	Prüft die Anzahl laufender Prozesse.	< 4000	> 4000 und < 6000	> 6000	Ein Neustart des Systems kann die Zahl laufender Prozesse vermindern. **Hinweis:** Dieser Prüfpunkt ist eher weniger aussagekräftig, da eine Warnung erst bei sehr hohen Werten erfolgt.	
user	Prüft die Anzahl der aller angemeldeten Benutzer (VNC, SSH und SFTP)	< 80	80 bis 90	> 90	Bei dauerhafter Überschreitung der Grenzwerte ist mit Performance-Einbußen zu rechnen.	

Prüfpunkt	Beschreibung	OK	Warnung (warning)	Problem (critical)	Aktivität, falls Warnung ausgegeben	Aktivität, falls Problem gemeldet
versions	Vergleicht die installierte Softwareversion mit dem aktuell verfügbaren Softwarestand.	Keine neuere Version verfügbar.	Updates verfügbar	Updates seit mehr als 6 Monaten verfügbar	Als Administrator *update* anmelden und ***Autoupdate*** durchführen	
vnc	Prüft die Erreichbarkeit des VNC-Servers und gibt dessen Antwortzeit sowie den gesetzten Port zurück.	Erreichbar.	---	Nicht erreichbar.	Ist VNC in der Konfiguration aktiviert und wird dennoch als unerreichbar moniert, sollte zunächst als Administrator *config* ein ***Voll Anwenden*** ausgeführt werden. Wird VNC danach weiterhin in Nagios als nicht erreichbar ausgewiesen, ist ein Neustart des Systems im Recover-Modus erforderlich. Es empfiehlt sich in diesem Fall eine Rücksprache mit dem technischen Kundendienst der m-privacy GmbH.	
zombie_procs	Unterminierte Zombieprozesse, können auf Fehler hinweisen.	Keine unterminierten Zombieprozesse vorhanden.	Bis zu 10 Zombieprozesse vorhanden.	Mehr als 10 Zombieprozesse vorhanden.	Zombieprozesse können gelegentlich auftreten und beeinträchtigen den Systembetrieb in der Regel nicht. Gehäuftes Auftreten von Zombieprozessen deutet auf Fehler in der Dateibehandlung hin. Es wird empfohlen, den technischen Kundendienst der m-privacy GmbH zu informieren.	
maint	Prüft, ob ein Node verfügbar und nicht im Wartungsmodus ist. Gibt ggf. den Zeitpunkt einer geplanten Wartung zurück.	Node verfügbar und nicht im Wartungsmodus.	Node im Wartungsmodus.		Nach beendeter Wartung als Administrator *maint* anmelden und Wartungsmodus beenden.	
gluster_error_user	Prüft auf Fehler in den Klienten-Logdateien und gibt sie (wenn vorhanden) aus.	Keine Fehler.	---	Fehler vorhanden.	Zunächst System neu starten. Falls danach weiterhin Fehler auftreten: Als Administrator *root* anmelden und /home/user/ manuell aus- und wieder einhängen. Dieser Vorgang kann nur als Administrator *root* manuell ausgeführt werden, nachdem alle Benutzer abgemeldet wurden. In jedem Fall sollte der technische Kundendienst der m-privacy GmbH benachrichtigt werden.	
gluster_error_backup	Prüft auf Fehler in den Logdateien des Administrators *backuser* und gibt sie (wenn vorhanden) aus.	Keine Fehler.	---	Fehler vorhanden.	Zunächst System neu starten. Falls danach weiterhin Fehler auftreten: Als Administrator *root* anmelden und /home/backuser manuell aus- und wieder einhängen. Dieser Vorgang kann nur als Administrator *root* manuell ausgeführt werden, nachdem alle Benutzer abgemeldet wurden. In jedem Fall sollte der technische Kundendienst der m-privacy GmbH benachrichtigt werden.	
temp	Prüft die Temperatur des Mainboards (falls Sensor vorhanden) und gibt sie aus.	< 50 °C	50 °C bis 60 °C	> 60 °C	Bei Temperaturüberschreitung gesamtes Kühlsystem der Hardware (Lüfter, Kühlkörper, Luftkanäle, etc.) sowie Klimatisierung der Betriebsumgebung prüfen.	
fan	Prüft, ob ein Lüfter läuft (falls Sensor vorhanden).	Läuft.		Läuft nicht.	Bei Problemmeldung Hardware überprüfen.	
fpupdate	Prüft, ob die Schadcodedefinitionen des F-Prot aktuell sind und ob der F-Prot-Monitor läuft.	Definitionen aktuell (oder nicht älter als 3 Tage) und F-Prot-Prozess (fpmon) läuft.	> 3 Tage alte Definitionen	F-Prot-Prozess (fpmon) läuft nicht.	Aktualität der F-Prot Lizenz überprüfen und Virendefinitionen gemäß Administrationshandbuch aktualisieren.	Korrekte Konfiguration als Administrator *config* entsprechend Administrationshandbuch vornehmen.
cups	Prüft auf Verfügbarkeit des CUPS-Dienstes.	CUPS- Prozess läuft.		CUPS- Prozess läuft nicht.	Sollte sich das Problem durch ***Sanft Anwenden*** nicht lösen lassen, ist der technische Kundendienst der m-privacy GmbH zu benachrichtigen.	