Integritätsprüfung (intern / extern)

TightGate-Pro kann auf Systemintegrität geprüft werden, um eine mögliche Kompromittierung der Programmkomponenten respektive Pakete zu erkennen und geeignete Gegenmaßnahmen einzuleiten. Es wird zwischen interner und externer Integritätsprüfung unterschieden.

Genereller Ablauf

Jedes in einem TightGate-Pro installierte Paket enthält MD5- und SHA256-Hashwerte für diejenigen darin enthaltenen Dateien, die im System nicht verändert werden dürfen. Die Tabelle mit den Hash-Werten ist herstellerseitig mit GnuPG signiert.

Die Integritätsprüfung durchläuft die Liste aller installierten Pakete, prüft zunächst die Signatur der MD5-Hashtabelle anhand des zur Signatur verwendeten Public Keys und anschließend die MD5-Hashwerte aller dort gelisteten Dateien. Jede Abweichung wird im Protokoll mit Paket- und Dateiname festgehalten.

Der Administrator ***update*** verfügt hierzu über die gesonderte Menüoption **Integritätsprüfung**, über die eine interne Integritätsprüfung im laufenden Systembetrieb veranlasst werden kann. Weiterhin besteht die Möglichkeit, nach dem Systemstart von einem Installationsmedium die Menüoption **tightgate-install > Integrity Check** auszuwählen.

Der Unterschied zwischen der Prüfung als Administrator ***update*** im laufenden System und vom Installations- und Rettungs-System im Vorfeld eines sogenannten OE.Resets besteht nicht im Algorithmus, sondern nur darin, wo verwendete Programme und der Public-Key gespeichert sind. Im Fall der internen Integritätsprüfung durch den Administrator ***update*** befinden diese sich auf der Festplatte des zu prüfenden Systems und könnten prinzipiell manipuliert worden sein, während beim Aufruf vom Rettungssystem bzw. einem Installationsdatenträger im Vorfeld eines OE.Resets alle Programme und Public Keys ausschließlich vom nur lesbaren Medium geladen werden. Die signierten Hashtabellen befinden sich dagegen immer auf der Festplatte. Dies stellt kein Sicherheitsrisiko dar, da die Signaturprüfung deren Manipulation zuverlässig ausschließt.

Maßnahmen bei Abweichungen im Zuge der Integritätsprüfung

Sollte die Integritätsprüfung eine Veränderung entdecken, ist die Protokolldatei per SCP auf ein anderes System zu übertragen und zwecks weiterer Untersuchung an die m-privacy GmbH zu übermitteln. Anschließend muss das System durch eine Neuinstallation (OE-Reset) in den Auslieferungszustand zurückgesetzt werden. Die Konfiguration, die Benutzerkonten und ihre Daten sind danach wie vorgesehen zurückzuspielen. Dadurch wird sichergestellt, dass eventuelle Manipulationen an den Dateien beseitigt sind. Bei Verdacht auf einen Fehlalarm empfiehlt es sich, die Integritätsprüfung erneut durchzuführen.

Verfahrensweise zur internen Integritätsprüfung

Die interne Integritätsprüfung prüft die installierten Pakete von TightGate-Pro im laufenden Systembetrieb auf Integrität. Die Prüfung wird durch den Administrator ***update*** ausgelöst und umfasst die folgenden Schritte:

- Anmeldung als Administrator ***update*** an der Konsole.
- Auswahl der Menüoption **Integritätsprüfung**.

Die Integritätsprüfung wird gestartet. Der Prozess kann je nach Systemleistung und Anzahl der zu überprüfenden Programmpakete einige Zeit in Anspruch nehmen. Mittels der Tastenkombination **CTRL+C** beziehungsweise **STRG+C** kann die Integritätsprüfung unterbrochen werden. Es wird ein Hilfsmenü angezeigt, in dem die Prüfungsergebnisse angezeigt oder per SCP übertragen werden können. Auch der definitive Abbruch der Integritätsprüfung ist möglich.

Das Ergebnis der Integritätsprüfung wird durch eine Ergebnismeldung zusammengefasst und in einer detaillierten Protokolldatei gespeichert. In der Ergebnismeldung werden folgende Werte angezeigt:

Wert	**Beschreibung**	**Handlungsempfehlung**
korrekt:	Anzahl der korrekt geprüften Pakete	Es ist nichts zu unternehmen.
fehlerhaft:	Anzahl der fehlerhaften Pakete	Es ist ein Bericht zu erzeugen und an die m-privacy GmbH zu übermitteln.
gesamt:	Gibt die Gesamtzahl der geprüften Pakete an	Es ist nichts zu unternehmen.
übersprungen:	Gibt die Anzahl der übersprungenen Pakete an. Pakete, die als Binärpakete eingebunden sind, können nicht geprüft werden und werden daher übersprungen. Dies sind z.B. der Virenscanner oder der Chrome Browser.	Es ist nichts zu unternehmen.
nicht mehr installiert:	Gibt die Anzahl der Pakete an, welche nicht mehr installiert sind, da sie in der Zwischenzeit gelöscht wurden.	Es ist nichts zu unternehmen.

Die detaillierte Protokolldatei kann mittels der Menüoption **Bildschirm** angezeigt werden. Anm Ende der Bildschirmanzeige sollte folgender Satz stehen:

```
Alle untersuchten Pakete sind korrekt!
```

Achtung

Wird die Funktion vorzeitig abgebrochen, kann der ausgegebene Ergebnisbericht fehlerhaft oder unvollständig sein.

Verfahrensweise zur externen Integritätsprüfung

Die externe Integritätsprüfung prüft die installierten Pakete von TightGate-Pro gegen die Daten eines

externen, unveränderlichen Datenträgers. Dabei kann es sich um ein Rettungssystem oder ein Installationsmedien handeln. Die Prüfung wird nach dem Systemstart (Bootvorgang) vom externen Datenträger durch Wahl der entsprechenden Menüoption ausgelöst und umfasst die folgenden Schritte:

- Systemstart (Bootvorgang) vom Rettungssystem oder Installationsdatenträger.
- Auswahl der Menüoption **tightgate-install > Integrity Check**
- Einhängen der Festplatte(n) des Systems in den Verzeichnisbaum: /dev/sda1 ist die Root-Partition, Rest entsprechend Vorgabe.
- Auslösung des Prüfvorgangs.
- Auswertung des Ergebnisses mit der Menüoption **Screen** beziehungsweise Versand des Prüfergebnisses per E-Mail.

Die Integritätsprüfung wird gestartet. Der Prozess kann je nach Systemleistung und Anzahl der zu überprüfenden Programmpakete einige Zeit in Anspruch nehmen. Mittels der Tastenkombination **CTRL+C** beziehungsweise **STRG+C** kann die Integritätsprüfung unterbrochen werden. Es wird ein Hilfsmenü angezeigt, womit die Prüfungsergebnisse angezeigt oder per E-Mail oder SCP versandt werden können. Auch der definitive Abbruch der Integritätsprüfung ist möglich.

Das Ergebnis der Integritätsprüfung wird durch eine Ergebnismeldung zusammengefasst und in einer temporären Protokolldatei im Verzeichnis /tmp des laufenden Systems gespeichert. Ergebnismeldungen lauten beispielhaft:

```
Positiv: "All 1265 packages passed!"
```

```
Negativ: "2 of 1265 packages failed. Please contact m-privacy support."
```

Die Zahl der zu prüfenden Pakete kann abweichen und hängt von der tatsächlichen Systemkonfiguration ab. Die temporäre Protokolldatei kann mittels der Menüoption **Screen** angezeigt sowie ausschließlich über die jeweiligen Menüoptionen per SCP übertragen oder per E-Mail versandt werden, sofern dies in der Einsatzumgebung vorgesehen ist.

Achtung

Wird die Funktion vorzeitig abgebrochen, kann der ausgegebene Ergebnisbericht fehlerhaft oder unvollständig sein.