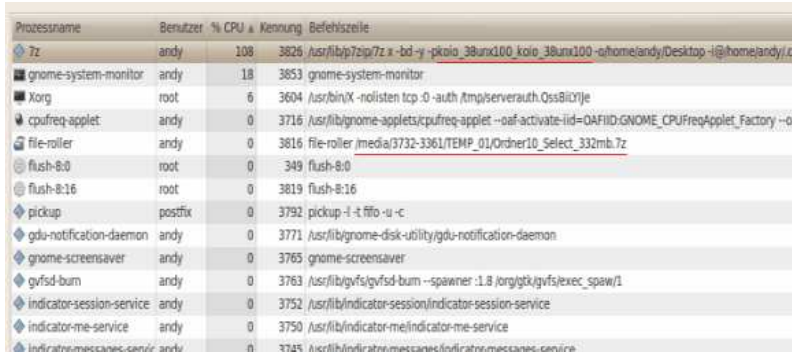


INTERNE MITTEILUNG: GS-AG, 2011-02-09

LINUX: Wenn beispielsweise eine AES-verschlüsselte Datei per 7zip geöffnet wird, dann ist die entsprechende Befehlszeile `/usr/lib/p7zip/*` mit den Übergabe-Parametern im [Speicher](#) abgebildet. Mit einem beliebigen [Process-Monitor](#) ist der vollständige Parameter-String mit dem Passwort als Klartext direkt auslesbar. Besteht während dem Öffnen eine aktive [Netzwerk-Verbindung](#) mit Zugriff auf den Speicher, dann ist die Entwendung des Passwortes eine reale Gefahr. Ist zudem das [Betriebssystem](#) nicht so seriös, wie es vorgibt zu sein, dann kann ein [Remote-Zugriff](#) auf diese Datei erfolgen. Ein Witz ? Leider nicht. Klartext-Probleme dieser Kategorie können JEDE Verschlüsselung gefährden.



Prozessname	Benutzer	% CPU	Kennung	Befehlszeile
7z	andy	108	3826	<code>/usr/lib/p7zip/7z x -bd -y -pkoio_38junc100_koio_38junc100 -q/home/andy/Desktop-1@home/andy.c</code>
gnome-system-monitor	andy	18	3853	<code>gnome-system-monitor</code>
Xorg	root	6	3604	<code>/usr/bin/X -nolisten tcp -o auth /tmp/serveauth.OssBILYje</code>
cpufreq-applet	andy	0	3716	<code>/usr/lib/gnome-applets/cpufreq-applet --oaf-activate-iid=OAFIID:GNOME_CPUFreqApplet_Factory --o</code>
file-roller	andy	0	3816	<code>file-roller /media/3732-3361/TEMP_01/Ordner10_Select_332mb.7z</code>
flush-8:0	root	0	349	<code>flush-8:0</code>
flush-8:16	root	0	3819	<code>flush-8:16</code>
pickup	postfix	0	3792	<code>pickup -l -t fifo -u -c</code>
gdu-notification-daemon	andy	0	3771	<code>/usr/lib/gnome-disk-utility/gdu-notification-daemon</code>
gnome-screensaver	andy	0	3765	<code>gnome-screensaver</code>
gvfsd-burn	andy	0	3763	<code>/usr/lib/gvfs/gvfsd-burn --spawner :1.8/org.gvfs:exec_spaw1</code>
indicator-session-service	andy	0	3752	<code>/usr/lib/indicator-session/indicator-session-service</code>
indicator-me-service	andy	0	3750	<code>/usr/lib/indicator-me/indicator-me-service</code>
indicator-mecanec-coniv	andy	0	3745	<code>/usr/lib/indicator-mecanec/indicator-mecanec-coniv</code>

WARNING: Man muß sich über Algorithmen und das Verbergen von Passwörtern beim Eintippen nicht wirklich Gedanken machen, wenn auf anderem Wege der Schlüssel ungeschützt sichtbar ist. Wie sicher eine [OS-Umgebung](#) tatsächlich ist, beantwortet die praktische Überprüfung. **Verschlüsseln- und entschlüsseln sie nichts während einer bestehenden Netzwerkverbindung !** ... Ob [TrueCrypt](#) eine sichere Alternative ist, kann man u.a. in <https://www.datenschutz.rlp.de/de/selbsts.php> nachlesen - siehe auch [GnuPG](#) und [Ecrypt-Utils](#).

A158 ### [secur-2011-02-09-A158.htm](#) -- (ref: [secur-2011-01-18-A154.htm](#))