INTERNE MITTEILUNG: GS-AG, 2011-02-04

LINUX: ES SIND WIEDERHOLT NEUE FS-FEHLER AUF EXTERNEN LAUFWERKEN (FAT32, NTFS, EXT2, EXT3, EXT4) PRODUZIERT WORDEN, WO VORHER KEINE WAREN ! Dubioses "Distribution-Tuning" an Kernel-nahen Komponenten, zweifelhafte ATTR-Privilegien, Pseudo-Security, fehlende Informations-Transparenz usw sind auffällig - für den Datenbestand gefährliche und verwanzte Trend-Betriebssysteme sind keine Empfehlung, trotz imposantem Screendesign, Multimedia-Netzwerk und Weltretter-Propaganda. Die Kurzinfo bietet hoffentlich genügend Hintergrund die aktuellen Tendenzen zur Kenntnis zu nehmen.

ABHILFE: Für die fehlerfreie Sicherung von Datenbestand per externem Backup ist ein "Trend-Linux" zuweilen gefährlich unzuverlässig. Beschädigung oder Vernichtung von Arbeitsdaten auf externen Backup-Archiv-Storage-Systemen ist im Jahr "2011" nicht wirklich witzig - zumal seit Jahren genügend Hinweise von aufmerksamen Usern in den Bug-Reports zu finden sind.

* Eine "zuverlässige" LiveCD (Knoppix, OpenBSD, PartedMagic u.a.) ist notwendig, wo derart destruktive Probleme NICHT auftraten. Diese "provisorische" Abhilfe ist für den Notfall oder den privaten Anwender noch akzeptabel, Sicherheit-Strukturen verlangen jedoch seriöse Betriebssysteme.
* Die Fehlinterpretation von Exec-Strings und File-Folder-Namen kann man vermeiden durch die Filterung und Umbenennung von kritischen Sonderzeichen wie etwa [+;|?":/=\] mittels "find (*) -exec rename (*)". Die Beseitigung der Namens-Konflikte werden vor dem Backup auf dem Quellen-Laufwerk durchgeführt. Beispielsweise für Dateien: **find /dir1/dir2 -type f -name '*[;|?":=]*' -exec rename -v 's/\;/_/g; s/\|/_/g; s/\?/_/g; s/"/_/g; s/\:/_/g; s/'='/_/g;' {} \;** und ein Beispiel für Verzeichnisse: **find /dir1/dir2 -depth -type d -execdir rename -v 's/\;/_/g; s/\|/_/g; s/\?/_/g; s/"/_/g; s/\:/_/g; s/'='/_/g;' {} \;**. Ein Shell-Script erledigt diese Aufgaben ohne großen Aufwand. Als Soforthilfe vorgesehen, lösen diese Maßnahmen nicht die noch bestehenden Probleme.

BEMERKUNG: Da schwerwiegende fs-Unstimmigkeiten, die "Langzeit-Bugs" stets an strategischer Position - bisher NICHT dokumentiert oder kommentiert sind, statt dessen man die Idealisten mehrere Jahre herumrätseln läßt, ist von fahrlässiger Ignoranz auszugehen. Es ist unmöglich für Professionals (zuverlässige und kontrollierte Arbeitsorganisation) wiederholt an gleicher Stelle gravierende Fehler der OS-Basis über mehrere Jahre zu übersehen. Wenn dennoch "versehendliche Bugs" argumentativ schöngeredet werden, dubiose Merkwürdigkeiten ein Dauerzustand bleiben, dann sollte die Seriösität von diesem OS-Distributor realistisch einzuordnen sein. Auf die Spy-Mechanismen im OS, auf das zweifelhafte Software-Center und auf verborgenes Datenabgreifen beim Firefox-Browser haben wir bereits hingewiesen. Die auffällig sympathische Gutmensch- und Weltretter-Propaganda (Menschlichkeit, Miteinander, Transparenz, Non-Profit usw) mag den privaten Nutzer begeistern, Berufserfahrung darf sich jedoch nicht von Geschwätz beeindrucken lassen - OS-Analyse bzw IT-Forensik beantworten alle weiteren Fragen.

IT-Forensik (itf-dummy) ist eine möglichst detailierte System-Analyse zwecks Sicherung von Beweisen der funktionalen Aktivitäten über einen hinreichend großen Zeitraum. Grundlegende Methoden sind beispielsweise ein Disk-Snapshot (A-B=DIF), Memory-Snapshots (A-B=DIF), Process-Tracing, Process-Debugging, String-Filter und HEX-BIN-TXT-Inspektion. Diagnostische Befunde werden chronologisch protokolliert, einschließlich deren Entstehungs-Situation. (Siehe auch: bug_reports_ubu_E03.htm, security_ubu_A07.htm)

WARNUNG: Als "berufliche" Workstation, als Backup/Storage-Server im Netzwerkverbund oder in öffentlichen Netzwerken ist dieses OS aus unserer Sicht nicht vertretbar. Sowohl die Sicherheit des Datenbestandes wie auch die Diskretion von Arbeitsdaten sind erheblicher Gefahr ausgesetzt.

EMPFEHLUNG: Die Minimal-Anforderung für ein Desktop-System oder die Workstation wäre das verwendete OS zu entmisten, zu entwanzen und eine umfangreichen Security-Conf vorzunehmen. Bei Web- und Storage- oder NC-Processing-Servern sind nicht nur System-Tools, der Kernel und kernelnahe Komponenten (Compiler-ENV, Memory-Adressing, Random, HW-Driver usw) von Relevanz. Die GUI (Gnome v.2.3x bei Ubuntu 10.04 LTS) und einige kritische Anwendungen sind ein vermeidbares Risiko und sollten vollständig deinstalliert werden. Xorg erzeugt Memory-Leaks und es sind Auffälligkeiten mit dem Standard-Keyboard nicht zu übersehen. Der Kernel und die Boot-Sequenz (GRUB) sind scheinbar angreifbar (Buffer/Stack-Overflow, Adressierung, Root/ATTR, Injektion) und somit auch ein möglicher Exekutiv-Zugang zum BIOS (Kernel-Inspektion und PW-Schutz für das BIOS sind anzuraten. VOR den BIOS-Einstellungen bitte stets das System AUSSCHALTEN für wenigstens 60 Sekunden, dann einschalten und die neuen BIOS-Parameter eingeben, sodaß wenigstens der Cold-Cache-Angriff auf die Boot-Sequenz vermieden werden kann). Automatisiertes Datensammeln und Unterschlagung fundamentaler Information sind schon eine deutliche Warnung. Vergrabene Remote-Prozesse sind hingegen ein gefährlicher Angriff auf die Integrität des Anwenders. Glaubensbekenntnisse und Meinungen oder verwirrte Empfehlungen helfen uns nicht weiter. Wir brauchen JETZT eine klare Entscheidung, weil ansonsten die administrative Verantwortung naheliegende Konsequenzen ziehen muß.

Dieses Betriebssystem sollte nicht nur einer gründlichen Revision unterzogen werden. Ideal wäre eine bereinigte Variante mit verifiziertem Kernel als Live-CD zu erstellen. Wie geht es weiter ? Konstruktive Infos an eMax sind erwünscht und notwendig.

A157 ### secur-2011-02-04-A157.htm -- (ref: secur-2011-01-18-A154.htm, secur-2010-12-09-A151.htm)
