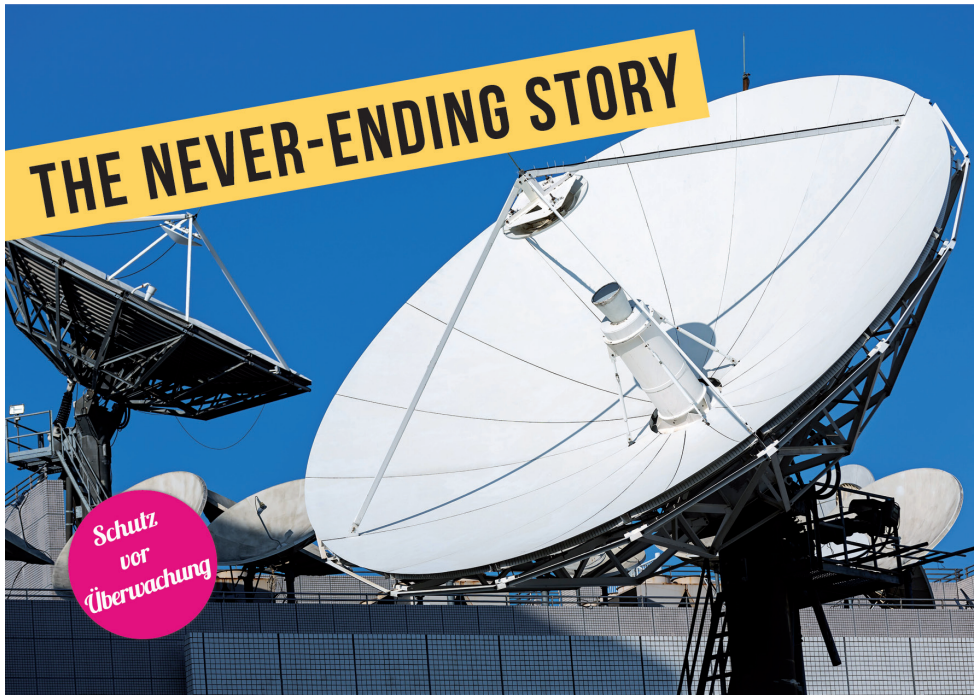
Notizen:



ANTI-PRISM-PARTY

4. Staffel

KARLSRUHE SCHÜTZT SICH SELBST
ANTI-PRISM-PARTY
WWW.ANTI-PRISM-PARTY.DE

- STATION NR. 2 -

Wie verschlüssele ich Datenträger?

Veranstalter

KA-IT-Si Karlsruher IT-Sicherheitsinitiative
//////// KIT zkm karlsruhe
CyberForum HIGHTECH. UNTERNEHMER. NETZWERK.
KASTEL

WIE VERSCHLÜSSELE ICH DATENTRÄGER?

Welches Problem wird gelöst?

- Daten liegen in der Regel unverschlüsselt auf Speichermedien (Festplatte, USB-Sticks) oder werden als unverschlüsselter E-Mail-Anhang verschickt.

- Lösung: Daten werden in verschlüsselten „Datencontainern“ oder auf komplett verschlüsselten Partitionen einer Festplatte gespeichert.

Wo gibt es gute Anleitungen im Netz?

TrueCrypt

- Jochen Bake: http://www.jochenbake.de/truecrypt-anleitung/
- F!XMBR: http://www.fixmbr.de/truecrypt-anleitung/

Alle Links finden Sie auch unter:
www.anti-prism-party.de/downloads

Wie heißt die Lösung? Wo kann sie bezogen werden? Welche Alternativen gibt es?

- Einige Betriebssysteme bieten eine Komplettverschlüsselung der Festplatte (bspw. BitLocker von Windows)

- **TrueCrypt 7.1a**
  Verfügbar für Windows (2000-7), Linux, OS/X (MAC)
  http://www.heise.de/download/truecrypt.html (kostenlos)

- **WinZIP**
  http://www.winzip.de/ (kostenpflichtig)

Was sind die Grenzen der Lösung?

- Daten eines Datencontainers oder auf einer verschlüsselten Festplatte sind während der Nutzung des Rechners auch Schadsoftware zugänglich.
- Geöffnete Dateien werden während des Betriebs und im „Ruhezustand“ in Auslagerungsdateien auf der ggf. unverschlüsselten Systempartition gespeichert.
- Verschlüsselte Datencontainer können entwendet oder kopiert werden und sind einer „Offline-Attacke“ zugänglich, daher sollte ein ausreichend langes Passwort gewählt werden.
- eine geringe „Beschädigung“ eines verschlüsselten Datencontainers zerstört nicht eine einzelne Datei, sondern den ganzen Container. Daher ist ein regelmäßiges Backup hier besonders wichtig.

secorvo
security consulting