Attingo

Sicherheitsrisiko gebrauchte Festplatten

Datenrettungsspezialist gibt Tipps für die sichere Entsorgung von Datenträgern.

Foto: Attingo

Patienteninformationen, Kundendaten und sogar Unterlagen aus der Forschungs- und Entwicklungsabteilung eines internationalen Konzerns: Es waren teilweise hochsensible Daten, die der Datenrettungsspezialist Attingo auf gebrauchten Festplatten fand. Das Wiener IT-Unternehmen kauft zwecks Ersatzteilbeschaffung ältere Harddisk-Modelle über die Versteigerungsplattform Ebay und überprüft stichprobenartig, wie mit den alten Platten umgegangen wird. „Der Schaden für Unternehmen ist enorm, wenn beispielsweise Kundendaten in die falschen Hände geraten", erklärt Attingo-Geschäftsführer Nicolas Ehrschwendner. Nicht nur das Image werde nachhaltig beschädigt, auch Erpressung und Wirtschaftsspionage seien mögliche Szenarien.

Immerhin, die Hacking-Skandale der letzten Zeit scheinen viele User bezüglich Datensicherheit sensibilisiert zu haben. Der Umgang mit gebrauchten Festplatten hat sich seit der ersten Erhebung im Jahr 2011 merklich gebessert. Damals wurden noch mehr als vier von fünf Datenträgern nicht oder nicht vollständig gelöscht, bei der diesjährigen Stichprobe fanden die Security-Spezialisten nur noch bei weniger als einem Drittel Datenspuren des Vorbesitzers. Festplatten aus Servern sind dabei häufiger betroffen als Disks aus PCs und Laptops. Serverplatten mit speziellen Schnittstellen wie SCSI oder SAS seien einfach schwieriger zu löschen als Consumer-Produkte mit Standard-Interface, vermutet Ehrschwendner.

Vollständiges Datenlöschen technisch fast unmöglich. Doch auch umsichtige Anwender, die ihre Datenträger vor dem Weiterverkauf löschen, sind nicht davor gefeit, dass Informationen wiederhergestellt werden. Entsprechende Softwarelösungen, die die Speicherbereiche mit Nonsense-Code überschreiben und so unlesbar machen sollen, sind leicht erhältlich. Die Crux dabei ist der sogenannte Reservespeicher, erklärt Ehrschwendner. „Festplatten haben oftmals schon ab Werk defekte Sektoren, auch später kommt es häufig zu Ausfällen einzelner Bereiche. Diese werden durch den Reservespeicher ausgeglichen." Defekte Sektoren werden von der internen Verwaltung des Datenträgers ignoriert und somit auch von Datenlöschsoftware nicht überschrieben. Die Daten sind in den beschädigten Bereichen immer noch vorhanden und können – mit großem Aufwand – wiederhergestellt werden. „Software-Löschverfahren sind nur durchschnittlich sicher, es gibt keine Garantie, dass wirklich alle Daten vernichtet wurden", so der Attingo-Geschäftsführer. Die Löschung eines Datenträgers mit sensiblen Informationen sollte immer mit einem unabhängigen System verifiziert werden. Im „High Security"-Bereich bleibt als wirklicher Ausweg nur die physikalische Vernichtung des Datenträgers mittels Entmagnetisierung („Degaussing") oder Schreddern.

Als Alternative zur nachträglichen Datenlöschung rät Ehrschwendner zur konsequenten Verschlüsselung der Festplatte. Entsprechende Algorithmen und Passwortstärken vorausgesetzt sind die Daten so vom ersten Tag bis zum End-of-Life des Datenträgers vor Fremdzugriff geschützt. *-lh-*

Attingo
www.attingo.at

@Insider

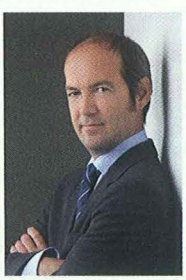
Gernot Pfannhauser, Head of Power Quality Sales Austria bei Eaton

Zahlen verraten bei USV-Anlagen mehr als tausend Worte. Wobei vor allem zwei Werte von besonderer Bedeutung sind: Der Leistungsfaktor und der Wirkungsgrad. Unsere dreiphasige 93PM USV beispielsweise glänzt mit einem Leistungsfaktor von 1 – das bedeutet kW=kVA! Best in class ist diese USV außerdem mit einem Wirkungsgrad von bis zu 97 % im Doppelwandlermodus.

Andreas Schmid, Senior Presales gateprotect

NETWORK PROTECTOR hat das Konzept der Next-Generation-Firewall revolutioniert. Der Schwerpunkt liegt auf der Verteidigung von Unternehmenswerten durch die Technologie der vollständigen Positivvalidierung in Kombination mit feingranularer Applikationsanalyse. Die Single-Pass-Engine garantiert hohe Performance bei gleichzeitiger Nutzung aller UTM-Funktionen.

Walter Huemer, GF Huemer Group



Mit der Zunahme von mobilen Endgeräten, Remote-Arbeitsplätzen und Virtualisierungen wachsen auch die Anforderungen an Unternehmensnetzwerke und -infrastrukturen. Damit erhöht sich auch der Bedarf an zuverlässigen IT-Sicherheitslösungen. Mit Hilfe eines kompetenten Partners können Unternehmen ihre IT-Systeme schon jetzt virtuell schützen.