

Gebrauchte Geräte als Datenlecks

Datenretter warnt: Vollständige Datenvernichtung ist fast unmöglich.

Den Jahreswechsel haben viele Unternehmen zum Anlass genommen, PCs und Laptops auszutauschen und den Mitarbeitern neue Geräte zur Verfügung zu stellen. Die ausrangierten Exemplare werden an den Hersteller oder das Systemhaus zurückgesendet oder an eigene Mitarbeiter weitergegeben. Was dabei oft zu kurz kommt, falsch durchgeführt oder gar vergessen wird, ist die korrekte Datenlöschung der gebrauchten Datenträger. Besonders sensible Unternehmensdaten geraten auf diesem Wege schnell in falsche Hände.

Gerade bei Leasingverträgen – mittlerweile sind etwa 20 Prozent der Arbeitsplätze mit solchen Geräten ausgestattet – werden bei groß angelegten Systemumstellungen viele neue Geräte angeschafft. Die Leasingpartner erhalten die alten Systeme mit häufig nicht korrekt gelöschten Datenträgern retour.

Über Umwege werden die Festplatten und SSDs nicht selten auf Tauschbörsen wie eBay oder Willhaben angeboten. Nicolas Ehrschwendner, Geschäftsführer der Attingo Datenrettung, kennt die Problematik sehr gut: „Für unser Ersatzteillager mit über 10.000 Festplatten kaufen wir oft auch gebrauchte Festplatten. Wie viele – teils sehr sensible – Daten auf diesen noch vorhanden sind, überrascht uns immer wieder aufs Neue.“ Besonders in Branchen wie Healthcare, Industrie und dem öffentlichen Bereich kann das fatale Folgen haben, wenn die Daten in die falschen Hände geraten.

Gefahrenquellen oft nicht bewusst. Das Problem beschränkt sich nicht alleine auf Festplatten aus PCs und Laptops – auch andere Geräte speichern Daten, woran bei der Entsorgung oder Weitergabe oft nicht gedacht wird. Dazu zählen unter anderem Kopierer, Drucker und Multifunktionsgeräte, Diktiergeräte oder Fotospeicherkarten.

„Auch von einzelnen Festplatten aus RAID-Storages oder Servern, die beispiels-

weise bei Fehlermeldungen oder ersten Defekten ausgetauscht werden, ist es durchaus möglich, unternehmenskritische Informationen zu gewinnen. Besonders kleinere Dokumente oder sensible Datensätze einer Datenbank oder Tabellenkalkulation sind mit entsprechender Fachkenntnis zu extrahieren“, weiß Ehrschwendner.

Attingo rekonstruiert Daten unter anderem für Gerichte, Sachverständige und Polizei von vorsätzlich vernichteten Datenträgern. Häufig ist es auch bei solchen

toren ausgelagert werden. Diese werden in den meisten Fällen nicht vernichtet und können noch ausgelesen werden.

Viele vertrauen auch dem Versprechen der Hersteller, dass zertifizierte Datenvernichtungssoftware hundert Prozent der vorhandenen Daten löscht. Attingo konnte jedoch in eigenen Szenarien nachweisen, dass auch solche Programme manchmal noch Datenfragmente zurücklassen.

Eine besondere Problematik tritt bei SSDs und Flashmedien wie USB-Sticks und SD-Karten auf, da durch sogenanntes „Wear Leveling“ Rohdaten immer an anderen physischen Adressen gespeichert werden – einmaliges softwareseitiges Überschreiben ist hier nicht ausreichend. Eine vollständige Datenvernichtung kann vom Benutzer praktisch nicht überprüft werden.

Richtig vernichtet. Die korrekte Vernichtungsstrategie ist abhängig vom Sicherheitsbedürfnis des Anwenders und der Sensibilität der Daten. Dennoch gibt es ein paar To-Dos vor dem Verkauf oder der Weitergabe eines gebrauchten Datenträgers. Eine probate Lösung im

Vorfeld wäre die „Full Disc Encryption“, also die Verschlüsselung des kompletten Datenspeichers bereits vor der ersten Verwendung. Weiters ist das Überschreiben des Datenträgers, beispielsweise nur mit Nullen, ein Pflichtpunkt, bevor dieser in fremde Hände gegeben wird. Die verbreitete Meinung, dass mehrfaches Überschreiben einer Festplatte die Sicherheit erhöht, ist jedoch nicht mehr als ein Mythos. Wurden hochsensible Daten auf dem Datenträger gespeichert, ist nach einer korrekten Löschung auch die mechanische Vernichtung zu empfehlen, um einem Datenleck vorzubeugen.



Foto: Attingo

Attingo bietet sowohl Consulting im Bereich Datenvernichtung als auch die Verifikation von gelöschten Datenträgern an

Datenträgern noch möglich, verwertbare Beweise zu rekonstruieren.

Vollständiges Datenvernichten fast unmöglich. Nicht in allen Fällen wird auf eine Datenvernichtung verzichtet oder vergessen. Allerdings werden auch dabei viele Fehler gemacht, wie zum Beispiel die Daten einfach nur zu löschen oder den Datenträger zu formatieren. In diesen Fällen ist eine Datenrettung möglich. „Gelöschte Daten sind auf den Speichermedien physisch noch verfügbar und rekonstruierbar, solange die betroffenen Sektoren nicht überschrieben wurden“, so Ehrschwendner. „Eine Vernichtung wäre nur durch vollständiges Überschreiben aller Speicherbereiche der Festplatte oder SSD möglich, was technisch bedingt nur selten umsetzbar ist.“ Datenträger verfügen über versteckte Speicherplatzbereiche, wohin defekte Sek-