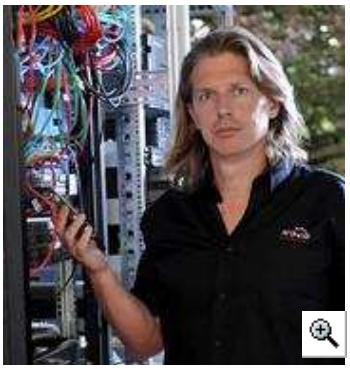
Attingo/DeepSec: Datenrettungspartner vorab auditieren

Notfallplan für den Datengau

23-5-2012 | Channel: Security

Unternehmen verfügen oft über ausgefeilte Security-Policies und Prozessbeschreibungen vom Backup bis zur Datenwiederherstellung. Was aber zu tun ist, wenn sich defekte Datenträger nicht mehr hausintern wiederherstellen lassen, ist zumeist nicht festgelegt. Dann folgt der Gang zum Datenretter, wobei aber leider allzu oft blindes Vertrauen gegenüber dem Dienstleister herrscht, warnt René Pfeiffer, Geschäftsführer der Wiener Sicherheitskonferenz DeepSec.

"Bei kritischen Systemausfällen werden oft plötzlich zentrale Security-Regeln außer Acht gelassen und in Windeseile Server, RAID-Systeme oder Festplatten mit hochsensiblen Informationen an externe Dienstleister übergeben - ohne dass diese im Vorfeld auf Sicherheit geprüft wurden", erklärt Pfeiffer.



"In mehr als 80 Prozent aller Fälle, bei denen selbstständig Rettungsversuche unternommen werden, vergrößert sich der Schaden dadurch letztendlich", unterstreicht Nicolas Ehrschwendner von Attingo.

Gefahr dabei sei, dass so mancher Datenrettungsanbieter defekte Medien an Recovery-Labore im benachbarten Ausland schicke, ohne Kunden explizit davon zu informieren. "Organisierte Datendiebe zapfen aber nicht selten Quellen über Dritte in Insider-Branchen an. Wenn auf diesem Weg Daten verloren gehen oder entwendet werden, hat das Unternehmen den doppelten Schaden", betont Pfeiffer. Denn es kommt auch noch das Haftungsrisiko hinzu.

"Laut Datenschutzgesetz haftet der Eigentümer dann voll für seine Informationen, wenn er es verabsäumt, die 'sichere Datenverarbeitung' durch seinen Dienstleister vorab zu prüfen", ergänzt Nicolas Ehrschwendner, Geschäftsführer des heimischen Datenrettungsunternehmens Attingo. De facto fordere das DSG damit die Durchführung von Dienstleister-Audits.

Nach dem Motto: "Prüfe deinen Datenretter, so lange die IT-Welt noch in Ordnung ist", bietet Attingo Kunden die gemeinsame Erarbeitung von Notfallplänen schon im Vorfeld an, so Ehrschwendner. Das Unternehmen betreibe das eigene Reinraumlabor in Wien, wodurch ein Versand ins Ausland kein Thema sei.

Das weitaus größte technische Risiko liege aber in unsachgemäßen Wiederherstellungsversuchen. "In mehr als 80 Prozent aller Fälle, bei denen selbstständig Rettungsversuche unternommen werden, vergrößert sich der Schaden dadurch letztendlich", schildert Ehrschwendner. "Bei Ausfall von Servern oder RAID-Systemen werden in der Hektik oft hausintern Schritte unternommen, die zwar logisch erscheinen, aber aufgrund der Komplexität gerade diesmal nicht funktionieren."

Typische Fehler seien etwa das unkontrollierte Tauschen defekter Festplatten, Löschen und neu-Anlegen von RAID-Konfigurationen, das Erzwingen des Online-Status von RAID oder Ausprobieren von unbekannten Funktionen. Generell seien Daten auf einem defekten Speichermedium im Reinraumlabor bis zu 100 Prozent rekonstruierbar, solange die betreffenden Sektoren nicht durch falsch veranlasste Vorgänge im Betriebssystem überschrieben wurden. Ein schädigender Vorgang kann aber schon ein simpler Systemstart sein.