onlinekosten.de

Tatort Arbeitsplatz: Computer-Sabotage aus Rache

Montag, den 17.12.07 17:01

Bernd ist sauer. Sein Chef hat ihm gekündigt. Und das bloß, weil er ein paar Mal zu spät gekommen ist. Heute hat Bernd seinen letzten Arbeitstag. Letzte Chance, dem Chef einen Denkzettel verpassen. Nur ein kleiner Befehl – und die Festplatte des Dienst-PCs ist gelöscht. Rache ist süß.

Kein Ausnahmefall, sondern Alltagsroutine: Racheakte per Computer sind scheinbar "en vogue". Nicolas Ehrschwendner, Geschäftsführer der Attingo-Datenrettung in Wien, registriert 2007 nahezu eine Verdoppelung von Fällen mit Sabotageverdacht im Vergleich zum Vorjahr.

Risikozeit Jahreswechsel

Retten, was zu retten ist:
Die Profis im Einsatz. Foto: Attingo

Eines haben alle gemeinsam: Sie sollen der Firma schaden. Die Methoden sind vielfältig. Zum Beispiel löschen Mitarbeiter absichtlich kostbare Unternehmensdaten oder formatieren Datenträger. Meistens handelt es sich um "Retourkutschen": Dem Rächer ist unversehens die Kündigung ins Haus geflattert oder er soll ungefragt versetzt werden.

Zum Jahreswechsel häufen sich solche Fälle, weiß man bei Attingo. Und das ist kein Zufall, denn da laufen Zeitverträge aus, Kündigungen werden wirksam oder der Mitarbeiter wechselt zur Konkurrenz.

System-Admin kann helfen

Ein System-Administrator, der die EDV-Systeme mit Sicherheitsfunktionen ausstattet und die Datensicherung überwacht, trägt zu mehr Sicherheit bei und kann den Schaden im Ernstfall begrenzen. Aber selbst große Konzerne mit eigener IT-Abteilung werden Opfer der "Dolchstoß-Attacken". Es sind eben nicht nur die Viren und Trojaner, die das Leben im IT Zeitalter erschweren. "Die Gefahr", so Ehrenschwendner, "kommt oft von innen."

Die Unternehmensberatung Woelke von der Brüggen führt auf dem Portal www.entscheiderkompass.de eine Umfrage bei mittelständischen Firmen zum Thema Datenschutz und -sicherheit durch. Von über 500 Teilnehmern besteht laut Auskunft des Münchner Unternehmens bei fast jedem Dritten generell akuter Handlungsbedarf im IT-Sicherheitsbereich. Über die Hälfte sind nicht ausreichend auf verschiedene Sicherheitsrisiken vorbereitet.

Fast die Hälfte der Unternehmen aus dem Mittelstand könne nicht gewährleisten, dass die Unternehmensdaten vor Manipulation, Diebstahl und Sabotage geschützt seien. "Leichtfertig" sei häufig auch der Umgang mit Informationen auf externen Datenträgern, so die Beraterfirma.

Hilfe im Ernstfall

Was also tun, wenn Daten vernichtet wurden? Bei Attingo rät man, das System nicht hoch zu fahren und nicht selbst Hand anzulegen. Jeder einzelne Vorgang im Betriebssystem - sogar das bloße Öffnen von Anwendungen - könne dazu führen, dass gelöschte Daten nicht mehr rekonstruierbar sind. Geschäftsführer Ehrschwendner: "Das Sicherste ist, das System abzuschalten und dem Spezialisten zur Analyse zu übergeben." Meistens holt der Fachmann das Kind auch aus dem Brunnen: In 90 Prozent der Fälle könnten die Daten rekonstruiert werden. Und manchmal klicken auch bald die Handschellen, denn forensische Untersuchungen weisen häufig auf den Täter hin. Das Landesamt für Verfassungsschutz Baden-Württemberg hat die häufigsten Gefahren, Anzeichen und Motive zusammengestellt.

Checkliste Computer-Sabotage

Häufigste Gefahren:

- Diebstahl von Personalcomputern, Laptops, Notebooks, Datenträgern und sonstigen Speichermedien
- Abhör- und Lauschangriffe auf Netze, IT-Systeme und Telekommunikationseinrichtungen
- Angriffe auf unternehmenseigene Computer
- Einschleusung von Viren und ausführbaren Programmen mit Schadfunktion
- Manipulation von System- und Anwendungssoftware

Anzeichen für Sabotage-Akte durch Mitarbeiter:

- Frustration, Unzufriedenheit im Beruf oder am Arbeitsplatz
- Besondere Neugier, auffälliger Arbeitseifer, nicht gerechtfertigtes Interesse an Dokumentationen und Berechtigungen
- Überqualifikation
- Vorschriftswidriges Verhalten am Arbeitsplatz
- Besitz/Nutzung von privaten Film-, Foto- und Textaufzeichnungsgeräten am Arbeitsplatz
- Auffällige und nicht plausible Verbesserung der finanziellen Situation, aufwändiger Lebensstil, Anzeichen für Bestechlichkeit
- Nicht eindeutig geklärter beruflicher Werdegang
- Abnehmende oder fehlende Identifizierung mit dem Unternehmen oder dessen Zielen

Motive beim Geschäftspartner:

- Verschleierung des eigentlichen Auftraggebers oder Geschäftsziels
- Vorsätzlich falsche Zolldeklarationen
- Warentransfer unter Umgehung der Zollbehörden
- Fälschung von Endabnehmerbescheinigungen
- Umleitung von Warensendungen über Drittländer mit Hilfe internationaler Speditionen
- Aufbau einer Organisation zur verdeckten Materialbeschaffung

Autor: Dorothee Monreal (dmo@onlinekosten.de)

Url dieses Artikels:
http://www.onlinekosten.de/news/artikel/27977

Links zu anderen Seiten in diesem Artikel:
