

Stick als Virenschleuse

von Tom Schätz

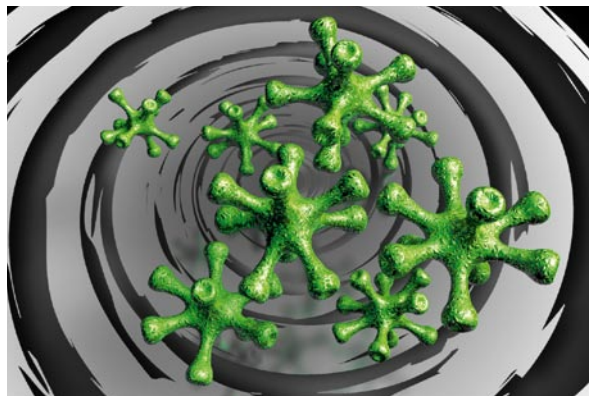
Notebooks, Handhelds oder USB-Sticks gefährden die Behörden-Netzwerke. Über die mobilen Geräte können Schadprogramme leicht eingeschleust werden. Dies zu verhindern gehört zu den größten Herausforderungen im IT-Security-Bereich.

Aufgrund von verteilten Standorten, Telearbeit und Vor-Ort-Terminen hat die Verbreitung mobiler Geräte wie Notebooks oder Handhelds und von Speichermedien wie USB-Sticks, Flash-Karten oder DVDs auch in der öffentlichen Verwaltung signifikant zugenommen. Bei allen Vorteilen eröffnet diese Mobilität auch vielfältige Angriffspunkte für Datenverlust oder gar -diebstahl.

Durch Wechselmedien wie USB-Festplatten und Speicherkarten, aber auch über Digitalkameras, Mobiltelefone oder PDAs mit eingebautem Speicher können unkontrolliert Daten aus dem Netzwerk kopiert oder in das Netzwerk eingeschleust werden. Kommunikationsgeräte wie WLAN-Sticks oder Bluetooth-Adapter können problemlos eingesteckt werden und für die Administratoren unbekannte, ungesicherte Schnittstellen zum internen Netzwerk darstellen. Hinzu kommt die Gefahr von Gerätediebstahl oder -verlust.

Um Datensicherheit auf mobilen Endgeräten zu gewährleisten, sind ganzheitliche Lösungsansätze erforderlich. Voraussetzung ist eine

mehrstufige Endpunkt-Datensicherheit, die sowohl Verschlüsselung als auch Data Leakage Prevention (DLP) umfasst. Klare Zugriffsregeln und konsequente Datenverschlüsselung stehen an oberster Stelle bei der Umsetzung einer umfassenden Sicherheitsstrategie. Unabdingbarer Bestandteil



Mobile Geräte können Viren übertragen.

einer zuverlässigen Sicherheitslösung ist die Dateiverschlüsselung nicht nur auf den Servern und lokalen sowie mobilen Rechnern der Benutzer, sondern insbesondere auch auf USB-Sticks, DVDs oder Speicherkarten. Idealerweise sollten die Daten auch gruppenbezogen verschlüsselt werden. Jeweils autorisierte Anwender können dann innerhalb ihrer Gruppe gemeinsam genutzte Informationen lesen beziehungsweise auf den dazu vorgesehenen Medien spei-

chern – ohne Gefahr des unberechtigten Zugriffs seitens Dritter.

Die Verschlüsselung von auf Servern abgelegten Daten sollte ebenfalls bereits am Endgerät vorgenommen werden und nicht erst auf dem Server selbst. Dies ermöglicht eine chiffrierte Übertragung der Daten zwischen Servern, Endgeräten und Speichermedien. Damit wird verhindert, dass Hacker mit einfach zugänglichen Sniffer-Programmen den Datenverkehr abhören.

Moderne Security-Software-Lösungen zeichnen sich durch die Möglichkeit aus, sowohl eine sektor- als auch eine dateibasierte Verschlüsselung vorzunehmen. Die sektorbasierte Verschlüsselung (Volume Based Encryption) stellt sicher, dass alle Daten inklusive Boot-Dateien, Swap Files, Hibernation Files, temporären Dateien oder Verzeichnisinformationen verschlüsselt sind. Die dateibasierte Verschlüsselung (Smart Media Encryption) garantiert, dass alle Daten außer Boot-Medien und Verzeichnisinformationen verschlüsselt sind – mit dem Vorteil, dass auch optische

Medien wie DVDs verschlüsselt werden oder, soweit von der Policy erlaubt, Daten passwortgeschützt mit Fremdrechnern ausgetauscht werden können, auf denen die Security Software nicht installiert ist. Ein flexibles Schlüsselringkonzept ermöglicht den komfortablen Austausch verschlüsselter Wechseldatenträger innerhalb von Benutzergruppen oder auch ein einfaches Recovery im Notfall, zum Beispiel das Andocken einer nicht mehr bootbaren Platte an einen Zweitrechner, auf dem der passende Schlüssel vorhanden ist.

Eine klassische Verschlüsselungslösung ist aber keineswegs immer ausreichend, da es sich in der Regel um autorisierte Mitarbeiter handelt, die mit vertraulichen Daten arbeiten. Ein Data-Leakage-Prevention-System (DLP) dagegen, das den Datenexport auf externe Medien überwacht und nur dann interveniert, wenn es sich um wirklich vertrauliche Daten handelt, verhindert effektiv den Verlust solcher Daten durch autorisierte Mitarbeiter. Mit einem DLP-System können alle als vertraulich klassifizierten Daten auf Notebooks, Desktops und Servern erkannt und Datentransfers auf unzulässige Ziele unterbunden werden. Das heißt, DLP ermöglicht eine Endpunktüberwachung in Echtzeit mit Geräte-Identifizierung und -sperrung, basierend auf von Administratoren definierten Richtlinien. Damit können alle lokalen, kabelgebundenen und drahtlosen Kommunikationsschnittstellen abgesichert werden – im Hinblick auf unterschiedlichste Datenübertragungsverfahren oder Zielgeräte wie Bluetooth, USB, FTP, HTTP, Instant Messenger oder Drucker.

Heute sind Sicherheitslösungen gefragt, die organisationsweit nur autorisierten Benutzergruppen Zugriff auf sensible Daten gewähren. Sie ergänzen technische Maßnahmen, die Schutz vor Angriffen von außen bieten. Außerdem gewährleistet nur eine starke Verschlüsselung maximale Sicherheit. Gelangt ein Endgerät in falsche Hände, so sind die Daten selbst beim Entfernen der Festplatte durch Unbefugte nicht mehr lesbar. Auch mobile Datenträger wie USB-Sticks, DVDs/CDs und Speicherkarten wie CF, SD oder MMC erhalten damit einen wirkungsvollen Rundumschutz. Mit der Möglichkeit, wahlweise eine sektor- oder dateibasierte Verschlüsselung vorzunehmen,

können Klartextdaten und verschlüsselte Daten auf beliebigen Datenträgern gespeichert und verwaltet werden. Dies erleichtert zudem den Datenaustausch zwischen Mitarbeitern und Geschäftspartnern erheblich. Nicht zuletzt ist es sehr empfehlenswert, eine DLP-Lösung zusätzlich zu implementieren, um eine unerlaubte Übertragung von Daten nach außen zu erkennen und zu unterbinden. Dadurch wird sowohl der versehentliche als auch der bewusste Datenmissbrauch durch befugte Benutzer zuverlässig verhindert.

Tom Schätz ist Bereichsleiter Security bei der Datagroup IT Services GmbH, Pliezhausen.