01 | 24 Sonderdruck für Deskcenter

IT Administrator
Das Magazin für professionelle System- und Netzwerkadministration

Risiken durch portable Apps vermeiden

www.it-administrator.de

Risiken durch portable Apps vermeiden

Schwarze To-Go-Schafe

von Winfried Metzger

Quelle: alenamostovich – 123RF

Portable Apps werden von Mitarbeitern rege genutzt, gern ohne Wissen der IT-Abteilung. Wer diesen Wildwuchs nicht eindämmt, riskiert Cyberattacken, Datenverlust und Lizenzverstöße mit gravierenden Folgen. Verbote und Richtlinien bewirken hier jedoch nicht all zu viel. Es geht stattdessen darum, dass die IT sämtliche Endpoints aktiv managt – egal, wer sie anschafft und ins Netz hängt.

In einer idealen Welt kümmern sich IT-Profis um alle Belange der Unternehmens-IT, steuern und verwalten sämtliche Hard- und Software. Und natürlich ist dem auch so – nur nicht ausschließlich. Denn zusätzlich existiert ein Paralleluniversum. Nach aktuellen Schätzungen von Experten nutzen zwischen 20 und mehr als 50 Prozent der Mitarbeiter IT-Equipment ohne Wissen und Genehmigung der IT-Abteilung. Darunter häufig zu finden: Die bei Usern sehr beliebten portablen Apps.

Büro to go

Portable Apps sind zweifellos praktisch, da sie nicht im Betriebssystem installiert werden müssen. Stattdessen lassen sich die Programme von einem mobilen Datenträger, einem beliebigen Verzeichnis auf der Festplatte oder einem Cloudlaufwerk ausführen. Sobald der USB-Stick oder die tragbare Festplatte eingesteckt oder ein Cloudlaufwerk synchronisiert ist, kann der User mit der Software arbeiten und auf seine persönlichen Daten zugreifen – genau wie bei einer unter dem Betriebssystem installierten Anwendung. Wird der mobile Datenträger ausgeworfen oder die Verbindung beendet, bleiben keine Systemdateien in der Registry oder persönlichen Daten auf dem verwendeten Endgerät zurück.

Im Internet finden sich die verschiedensten Programme als portable Version zum Download. Es gibt Werkzeuge zum Erstellen von Audios und Videos, Bildeditoren wie GIMP oder Programme zum Dateitransfer wie 7-Zip, Filezilla oder Dropbox. Der kostenlose E-Mail-Client Thunderbird und die Suiten OpenOffice und LibreOffice finden sich ebenso als portable Variante wie TeamViewer. Natürlich dürfen gängige Browser wie Google Chrome, Mozilla Firefox oder Opera nicht fehlen. Und sogar praktische Helfer für die Administration von PC und Laptop sind dabei: Von Tools zum Bereinigen der Festplatte oder Registry wie CCleaner über Werkzeuge zur Netzwerkdiagnostik bis hin zu Sicherheitsprogrammen von Avira oder McAfee.

Die Beliebtheit von portablen Apps kommt nicht von ungefähr:

- Sie sind schnell und überall einsetzbar.
- Sie sparen Platz auf der Festplatte und belasten das System nicht, weil es weder zu Einträgen in der Registry noch in den Benutzerkonten kommt.
- Ihre Ausführung erfordert keine Administratorenrechte – zumindest von wenigen Ausnahmen abgesehen. Dies soll auch dazu beitragen, dass die Programme bei ordentlicher Konfiguration des Wirtssystems keinen großen Schaden anrichten können.
- Sie sind jederzeit einfach und rückstandslos wieder zu entfernen.
- Über einschlägige Download-Sites aber auch Empfehlungen renommierter IT-Portale sind sie für jeden zugänglich.

Im Grunde sind das alles großartige Eigenschaften. Allerdings führen sie Unternehmen auch geradewegs in Sicherheits- und Compliance-Probleme.

An der IT vorbei

Als portable App besorgt sich der Anwender sein Lieblingsprogramm ganz schnell selbst im Web. Komplizierte Bestellprozesse, lange Wartezeiten oder die Ablehnung wegen mangelndem IT-Budget lassen sich so einfach umgehen. Nach dem Download wird das ZIP-Archiv entpackt und die EXE-Datei gestartet. Mit wenigen Klicks lässt sich eine portable Software so auf jedem Rechner ausführen – häufig ohne Admin-Berechtigung. Durch die Verwendung relativer Pfade oder einer eigenen virtuellen Umgebung ist portable Software unabhängig von einem festen Installationsort. Der Anwender kann somit den Speicherort frei wählen.

Doch die grundsätzlichen Vorteile einer portablen App werden für Unternehmen schnell zum Nachteil. Führt ein User portable Apps auf seinem Computer aus, sind Unternehmen noch anfälliger für Malwareinfektionen. Denn die direkt lauffähige Software stammt teilweise nicht von offiziellen Quellen und durchläuft in so einem Fall keine zuverlässige Sicherheitsprüfung durch den Hersteller. Damit besteht bereits bei der Speicherung des ZIP-Archivs oder der EXE-Datei ein erhöhtes

Risiko, dass integrierte Malware unentdeckt bleibt.

Kritisch ist auch, wenn über portable Apps Unternehmensdaten unbeabsichtigt oder unbemerkt aus dem Unternehmen abfließen. Viele Unternehmen haben bereits den Einsatz von USB-Sticks gesperrt und Peer-to-Peer-Verbindungen über entsprechende Spezialsoftware unterbunden. Doch portable Apps umgehen diese technischen Schutzwälle. Sie erlauben den Datenaustausch über Peer-to-Peer und einen Standard-Internetport trotz Sicherheitsmaßnahmen. Dies ermöglicht den unkontrollierten Datenaustausch mit Rechnern außerhalb des Unternehmens, vorbei an Proxy- und Mailfiltern.

Portable Anwendungen lassen sich außerdem nicht zentral administrieren oder updaten. Sie unterliegen somit keinen regelmäßigen Aktualisierungen und Patches. Da portable Software durch die Verwendung von Container-Technologie spezielle Nutzerrechte wie Admin oder Root umgeht, ist es kaum möglich, ihre Speicherung und Ausführung von vorneherein zu verhindern. Dazu müssten sämtliche Zugangswege inklusive Port 80, Bluetooth oder E-Mail-Attachments gesperrt werden. Für die meisten Unternehmen ist dies nicht praktikabel. Der einzige Schutzmechanismus besteht also darin, die IT-Infrastruktur kontinuierlich auf portable Apps zu prüfen und diese anschließend umgehend zu entfernen.

Versteckte Lizenzrisiken

Ein weiteres Risikofeld ist der Dauerbrenner Lizenz-Compliance. Grundsätzlich gilt: Wird eine lizenzpflichtige Software auf einer – beziehungsweise über eine – portablen App genutzt, ist sie ebenso zu lizenzieren wie die entsprechende installierte Version. Andernfalls handelt es sich um einen Lizenzverstoß. Unter Umständen untersagt der Hersteller sogar den Einsatz seiner lizenzpflichtigen Software über eine portable App.

Häufig wird allerdings Freeware als portable App genutzt; dann ist das Risikopotential ein anderes. Denn hier können Lizenzbestimmungen den kostenlosen Einsatz auf die private Nutzung beschränken. Die berufliche Anwendung erfordert dann eine Lizenz. Ein Beispiel hierfür ist TeamViewer. Durch Anwender, die dies nicht berücksichtigen, begeht das Unternehmen dann auch bei vermeintlicher Freeware einen Lizenzverstoß, der teuer werden kann.

Kontrolle durch Inventarisierung und Softwaremanagement

Verbote zur Nutzung privater Devices oder der eigenmächtigen Installation von Apps haben sich nicht als ausreichend wirkungsvoll erwiesen. IT-Admins bleibt daher nichts anderes übrig, als den Stier bei den Hörnern zu packen und sämtliche Endpoints effizient zu managen – auch diejenigen, die außerhalb ihrer Kontrolle ins Unternehmen gelangen. Im Kampf gegen die mit portablen Apps verbundenen Risiken verfügen sie jedoch über zwei scharfe Waffen: Inventarisierung und Softwaremanagement.

Softwarewerkzeuge zur Inventarisierung erkennen und erfassen sämtliche Hard- und Software inklusive aller Peripheriegeräte – vollständig und automatisiert. Sie arbeiten basierend auf Daten aus dem Active Directory über IP-Range-Scans oder DHCP-Scope- und Lease-Informationen. Hier ist allerdings darauf zu achten, dass wirklich alle Pfade einer Festplatte gescannt werden, denn viele Inventarisierungstools sind immer noch so konfiguriert, dass sie nur die Registry und den Program-Data-Pfad inventarisieren. Das war in der Vergangenheit aus Performance-Gründen sinnvoll, dank der heutigen Prozessoren ist dies aber hinfällig. Im Gegenteil: Es ist sogar gefährlich. Denn damit bleiben portable Apps unter dem Radar, da User diese bevorzugt auf dem Desktop oder im Pfad "Eigene Dateien" ablegen. Als Regel Nummer eins gilt deshalb: Immer die gesamte Festplatte scannen.

Auf die Inventarisierung folgt die Unterscheidung in erlaubte und unerlaubte Software. Im Falle einer portablen App ist dies alles andere als trivial. Denn dafür braucht es einen umfassenden Softwarekatalog, der portable Anwendungen als solche erkennt und direkt ausweist. Die Komplexität lässt sich an einem Beispiel gut illustrieren: Die Adobe Acrobat Suite etwa findet sich im Web auch illegal als portable App. Prüft eine Inventarisierungssoftware lediglich auf den App-Namen "Adobe Acrobat", könnte sie zum Schluss gelangen, hier sei eine korrekt lizenzierte Software versehentlich in einem falschen Verzeichnis installiert worden. Diese Software wäre nicht zu entfernen. Erst die Prüfung des App-Namens in Verbindung mit dem Hersteller gibt Aufschluss darüber, ob es sich um die Adobe Acrobat Suite von Adobe Systems Software oder um eine illegale Version handelt.

Die als unzulässig eingestufte Software zu entfernen, ist dann der nächste logische Schritt. Da portable Apps ohne eine Datei wie "uninstall.exe" kommen, läuft deren Löschung skriptbasiert. Eine definierte Löschroutine muss prüfen, in welchem Verzeichnis portable Anwendungen installiert sind und die Container anschließend automatisiert löschen. Über eine Verknüpfung zum Softwarekatalog lassen sich alle inventarisierten portablen Apps zuverlässig identifizieren und anschließend über das Skript in einem Schritt von unterschiedlichen Geräten entfernen. Damit lassen sich Sicherheits- wie Compliance-Risiken gleichermaßen eindämmen.

Fazit

Angesichts steigender Anforderungen, längerer Genehmigungs- und Bereitstellungszeiten und einer Fülle frei verfügbarer Anwendungen werden Mitarbeitende auch weiterhin eigenmächtig Tools und Geräte einsetzen. Portable Apps sind da nur ein Teil der weithin existierenden Schatten-IT. Unternehmen sind deshalb gut beraten, wenn sie Prozesse für eine automatisierte IT-Bereitstellung einführen und gleichzeitig Kontrollmechanismen etablieren. Dazu gilt es, die IT-Infrastruktur kontinuierlich zu prüfen – vollumfänglich, lückenlos und tagesaktuell. Mit einer regelmäßigen Inventarisierung und einem weitestgehend automatisierten Softwaremanagement lässt sich das Risiko von Cyberattacken und Lizenzverstößen so deutlich mindern. *(ln)*

Winfried Metzger ist Business Development Director / Strategic Channel Leader bei Deskcenter.