Als entscheidend für die Akzeptanz von Linux als Desktop-Betriebssystem für Unternehmen könnte sich die Verfügbarkeit von inhaltsbasiertem Data Leak Prevention herausstellen. (Bild: CoSoSys Ltd.)

Datensicherheit

Braucht Linux DLP?

15.04.16 | Autor / Redakteur: Michael Bauner / Peter Schmitz

Linux ist auf dem Vormarsch. Seine Schutzmechanismen gegen Bedrohungen von außen und die Verfügbarkeit von Business-Anwendungen machen es als Betriebssystem für Arbeitsplatz-Rechner salonfähig. Eine Bedrohung jedoch bleibt: der Datenverlust durch die eigenen Mitarbeiter. Jetzt sind die Hersteller von Lösungen für Data Leak Prevention aufgerufen, die Lücke zu schließen.

Als Server-Betriebssystem ist Linux nicht mehr aus den IT-Infrastrukturen wegzudenken, aber auf Desktops fristete Linux lange ein Nischendasein. Ihm haftete der Ruf einer Lösung für Geeks an. Aufgrund kurzer Lebenszyklen, einer verwirrend großen Anzahl unterschiedlicher Distributionen, gewöhnungsbedürftiger Benutzeroberflächen und Einschränkungen bei den Anwendungen galt es als untauglich für Arbeitsplätze in Unternehmen.

Doch inzwischen wächst die Zahl der Business-Anwender. Der Statistik von Net Applications zufolge hatte das Betriebssystem auf Desktops Anfang 2015 weltweit einen Marktanteil von 1,34 Prozent, zum Jahresende 2015 lag er bei 1,66 Prozent und steigt kontinuierlich.

Hürden für Linux sinken

Wachstumstreiber ist dabei, dass zum einen einschlägige Kommunikationstools und Business-Anwendungen auch für Linux verfügbar sind; zum anderen sinkt mit der zunehmenden Verlagerung der Anwendungen in den Browser der Stellenwert des Betriebssystems und verringert die Hürden für den Einsatz von Linux. Daneben kommt die Abkehr von den Marktführern Firmen und Organisationen mit überschaubaren IT-Budgets entgegen. Weil weniger leistungsstarke Rechner für Linux ausreichen, kann preisgünstigere Hardware gekauft oder eine bestehende Ausstattung länger genutzt werden – ein Anreiz insbesondere für kommunale Behörden oder öffentliche Einrichtungen. Auch die Software-Lizenzen schonen die Budgets, je nach Distribution sind sie kostenlos zu haben oder aber für überschaubare Summen.

Alternative für Sicherheitsbewusste

Der ausschlaggebende Faktor für die wachsende Akzeptanz von Linux sind jedoch Sicherheitsfragen. Das Design des Betriebssystems bildet einen zuverlässigen Schutz vor Bedrohungen von außen; Linux wird selten durch Malware infiziert und gilt als sehr schwer zu hacken. Langjährige Nutzer sind deshalb Unternehmen der Luft- und Raumfahrt, Forschungseinrichtungen, Banken und Versicherungen sowie Bundesbehörden – Wirtschaftszweige und Organisationen also, die sehr großen Wert auf Sicherheit legen, weil sie Investitionen und Betriebsgeheimnisse schützen müssen oder weil Arbeitsbereiche der Geheimhaltung unterliegen. Dass insbesondere viele kleinere und mittelgroße Unternehmen den Wert ihrer Daten deutlich unterschätzt haben und sich nicht vorzustellen vermochten, dass sie für Wirtschaftsspione interessant sein könnten, hat sich als Folge des NSA-Skandals geändert. Seit sich Windows 10 als Betriebssystem mit unstillbarem Kommunikationsbedürfnis bei der Übermittlung von Nutzerdaten geoutet hat, wird Linux für immer mehr Unternehmen zu einer echten Option – wenn nur das Problem mit den Mitarbeitern nicht wäre.

Der Anwender als Sicherheitslücke

Die Tools nämlich, die für den aktuellen Aufschwung von Linux mitverantwortlich sind, stellen gleichzeitig ein erhebliches Sicherheitsrisiko dar. Wie der Branchenverband Bitkom im Studienbericht „Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter“ oder IBM im „2015 Cyber Security Intelligence Index“ zu erfolgten Datenverlusten und Diebstählen aufgezeigt haben, sind an mehr als der Hälfte der Daten-Vorfälle die eigenen Mitarbeiter beteiligt. Sie sind diejenigen, die täglich mit Unternehmensdaten umgehen und sie auf USB-Sticks kopieren, per E-Mail versenden oder in einen Cloud-Speicher laden. Dass bei durchaus berechtigen Datentransfers Fehler und Versehen passieren können, liegt in der menschlichen Natur. Dann gelangt mit einem Mausklick ein internes Dokument an den falschen Adressaten oder eine Datei mit personenbezogenen Daten in die Dropbox. Diese Sicherheitslücke besteht unabhängig vom Betriebssystem und betrifft selbstverständlich auch Linux.

Zurück in die Kommunikations-Steinzeit?

Aber während für Windows- und Mac-Nutzer Lösungen für Data Leak Prevention mit umfassendem Schutz vor Datenverlust durch Gerätekontrolle und Inhaltsfilterung bereitstehen, mit denen die Unternehmen den gesamten Datentransfer überwachen und protokollieren und unerwünschte Transfers nach außen blockieren können, lassen sich an Linux-Desktops lediglich angeschlossene Geräte überwachen. Auf USB-Sticks beispielsweise können somit nur dann regelmäßig Daten kopiert werden, wenn die Benutzung des Devices für einen bestimmten Mitarbeiter oder eine Gruppe freigegeben ist. Eine differenzierte, inhaltsbezogene Betrachtung der Dateien, die auf dem Stick gespeichert werden sollen, war bislang jedoch ebenso wenig möglich wie die Prüfung von Daten, die über internetbasierte Kommunikationstools das Unternehmen verlassen. Soll also verhindert werden, dass sensible Daten außer Haus gelangen, bleibt nur: kein Webmail, kein ownCloud, kein Skype, mit der Folge erheblicher Produktivitätseinbußen.

Den Teufel mit Beelzebub austreiben

Michael Bauner, Geschäftsführer, Endpoint Protector GmbH (Bild: CoCoSys)

Selbstverständlich kann das Unternehmen den Mitarbeitern Einschränkungen im Kommunikationsverhalten auferlegen und die Nutzung bestimmter Tools untersagen. Dennoch dürfte sich eine derartige Maßnahme für die meisten der an Linux interessierten Unternehmen nicht eignen. Die Mitarbeiter sind daran gewöhnt, über unterschiedliche Anwendungen mit Kollegen, Kunden, Partnern und Dienstleistern zu kommunizieren und Dateien mit ihnen zu teilen. Ganze Abteilungen, beispielsweise der Vertrieb, sind darauf angewiesen, dass sie bestimmte Daten unterwegs zur Verfügung haben. Das macht es sehr wahrscheinlich, dass Regeln missachtet werden, wenn sie nicht durch eine technische Lösung überwacht werden können. So entsteht die paradoxe Situation, dass ein Unternehmen, das aus Sicherheitsgründen einen Umstieg auf Linux erwägt, den Teufel mit Beelzebub auszutreiben versucht und die Migration auf Linux aufschieben muss, solange sich die Lücke nicht schließen lässt.

Jetzt sind die DLP-Hersteller am Zug

Mit der Weiterentwicklung des Betriebssystems zu einer business-tauglichen Alternative zu den vorherrschenden Lösungen ist die Linux-Gemeinde in Vorlage gegangen. Damit das Wachstum nicht gleich wieder gebremst wird – und in diesem Fall durch einen Faktor, der mit dem Betriebssystem nicht das Mindeste zu tun hat – sind jetzt die Hersteller von Produkten für Data Leak Prevention gefragt. Es ist Zeit für eine Lösung, die den Linux-Anwendern denselben Schutz vor Datenverlust und Datendiebstahl an die Hand gibt wie den Nutzern anderer Betriebssysteme. Er soll ihnen ermöglichen, die Überwachung auf alle internetbasierte Schnittstellen auszuweiten, den Transfer sensibler Informationen zu protokollieren und gegebenenfalls zu unterbinden.