CoCoSys Endpoint Protector 4.4

Vollsperrung auf Wunsch

von Jürgen Heyer

Wenn Schnittstellen wie USB und CD/DVD-Geräte für die Benutzer frei zugänglich sind, ist es ein Leichtes, Unternehmensdaten unbeaufsichtigt zu kopieren und aus der Firma zu schaffen. Ebenso gefährlich ist es, wenn Mitarbeiter Software mittels tragbarer Datenspeicher mitbringen und Malware im Gepäck haben. Der Endpoint Protector aus dem Hause CoCoSys verspricht umfassende Sicherheit vor solchen Szenarien.

Bekanntermaßen schlummert die größte Gefahr für das unkontrollierte Zu- und Abwandern von Unternehmensdaten bei den eigenen Mitarbeitern, wenn diese unbeaufsichtigt Kopien anfertigen, aber auch beliebige Software mitbringen können. Dabei muss es sich noch gar nicht mal um den Vorsatz handeln, der Firma etwas zu stehlen und somit eine kriminelle Handlung zu begehen. Häufig ist es Leichtsinn, wenn Mitarbeiter Informationen über soziale Medien preisgeben oder vorschnell per E-Mail verschicken. Oft sind es auch wohlgemeinte Ansätze, dass sich ein Mitarbeiter Arbeit mit nach Hause nimmt, um auf dem heimischen PC daran weiterzuarbeiten. Wird dieser PC gehackt, gelangen die Daten schnell in die falschen Hände.

Ebenso wohlgemeint wie gefährlich ist es, wenn Mitarbeiter irgendwelche Softwaretools mitbringen, um sich die Arbeit zu erleichtern und dabei Malware mit einschleppen. Auch müssen Firmen auf die Einhaltung der Lizenzvorschriften achten und es besteht die Gefahr, dass so lizenzpflichtige Software genutzt wird, ohne diese korrekt erworben zu haben. Diese und weitere Aspekte adressiert die Software Endpoint Protector (EPP) von CoCoSys.

Komfortables Setup dank fertiger Appliance

Für eine schnelle Bereitstellung der Software hat der Hersteller den Appliance-Ansatz gewählt, in dem das Produkt wahlweise als virtuelle oder Hardware-Appliance bereitgestellt wird. Bei der Hardwarelösung gibt es aktuell acht unterschiedliche Modelle, die fest mit einer bestimmten Anzahl von zu schützenden Systemen (20 bis 4000) gekoppelt sind. Sie unterscheiden sich hinsichtlich der Rechenleistung, um entsprechend viele Clientanfragen parallel bearbeiten zu können. Die virtuelle Appliance ist in den Formaten OVF, VMX, VHD, XVA sowie PVM erhältlich, um die verbreiteten unterschiedlichen Virtualisierungsplattformen nutzen zu können. Wir wählten für den Test die OVF-Vorlage für die Installation unter VMware vSphere.

Die Appliance basiert auf Ubuntu und das Einspielen der rund 3,5 GByte großen Vorlage lief erfreulich unproblematisch ab, wobei bei der Bereitstellung keine besonderen Parameter abgefragt werden und der Ressourcenbedarf gering ist. Nach dem Einschalten muss der Administrator die Konsole öffnen, um dort eine IP-Adresse aus dem Netzwerk einzutragen oder DHCP auszuwählen. Im späteren Betrieb dient die Konsole dazu, eine Systemsicherung durchzuführen oder ein erstelltes Backup wieder einzuspielen. Wir entschieden uns für eine feste IP-Adresse und konnten anschließend für die weitere Bedienung über den Webbrowser auf die eigentliche Bedienerkonsole, genannt Administrations- und Reporting-Cockpit, zugreifen.

Breite Agentenunterstützung

Beim ersten Zugriff auf das Cockpit öffnet sich automatisch eine Download-Seite für die unterschiedlichen Clientversionen. Als Besonderheit unterstützt EPP nicht nur Windows-Clients, sondern auch solche unter macOS sowie den Linux-Distributionen Ubuntu und OpenSUSE. Auf jedem zu schützenden System ist ein entsprechender Client zu installieren, der mit der EPP-Appliance kommuniziert und die Zugriffe sowie den Datenverkehr überwacht und dann auch gegebenenfalls einschränkt. Damit sich ein Anwender nicht der Kontrolle entziehen kann, lässt sich optional

Bild 1: Das Cockpit-Dashboard des Endpoint Protector liefert die wichtigsten Informationen auf einen Blick.

ein Deinstallationspasswort vorgeben, ohne das eine Entfernung nicht möglich ist.

Die Installation der Clients kann auf verschiedenen Wegen erfolgen, manuell, skriptgesteuert, über AD-Regeln oder über eine Softwareverteilungslösung. Gefallen hat uns, dass die zum Download bereitgestellten Clientdateien mit der IP-Adresse der Appliance und den durch den Administrator wählbaren Kommunikationsports so vorkonfiguriert sind, dass bei der Installation nichts dergleichen abgefragt werden musste und die Endpunkte dennoch nach dem Aufbringen des Clients in EPP erschienen. Das erleichtert und vereinfacht die Einrichtung enorm.

CoCoSys Endpoint Protector 4.4

Produkt
Software zum Schutz vor Datendiebstahl, Datenverlust, Datenlecks, Datenklau über interne Clients.

Hersteller
CoCoSys
www.endpointprotector.de

Preis
Endpoint Protector 4 als virtuelle Appliance für 50 Endpunkte kostet 1188 Euro, mit Content Aware Protection 1980 Euro. Für den Schutz von mehr Endpunkten gibt es Staffelpreise.

Systemvoraussetzungen
Hardware-Appliance: IP-Adresse aus dem Netzwerk.

Virtuelle Appliance: Bereitstellung in den Formaten OVF, VMX, VHD, XVA oder PVM für diverse Virtualisierungsplattformen mit einem Ressourcenbedarf von 2 vCPU, 2 GByte vRAM, 60 GByte Plattenkapazität.

Technische Daten
www.it-administrator.de/downloads/datenblaetter

Ist der Client installiert, ist dies am Endpunkt in der Standardeinstellung an einem Ampelsymbol in der Taskleiste sichtbar. Durch Anklicken des Symbols erhält der Anwender einige Informationen zu den effektiven Einstellungen. So sieht er in einer Liste über einen grünen oder roten Punkt, welche Geräte er nutzen kann und welche nicht. Darüber hinaus findet er beispielsweise in der Laufwerksübersicht kein DVD-Laufwerk, wenn dieses nicht zur Nutzung freigegeben ist. Ändert der Administrator im Cockpit Einstellungen, so werden diese in der Regel nach kurzer Zeit an den Clients aktiv. Es gibt zusätzlich die Möglichkeit, eine Aktualisierung des Clients zu forcieren.

EPP lässt sich auch für Endpunkte wie Notebooks, die zeitweise offline genutzt werden, einsetzen. Dies gelingt, weil der Client die letzten Einstellungen zwischenspeichert und auch offline anwendet. Änderungen an den Einstellungen greifen verständlicherweise erst dann, wenn das Gerät wieder online ist. Für den Offlinebetrieb gibt es aber zusätzlich die Möglichkeit einer temporären Gerätefreischaltung über eine Kombination aus Code und Passwort. Hierzu muss der Anwender diese Kombination beim Administrator erfragen, der diese wiederum im Cockpit erzeugen muss. Das Zeitintervall für eine Freischaltung kann zwischen 30 Minuten und 30 Tagen liegen.

Neben der beschriebenen Standardeinstellung des Clients (Normal Mode) gibt es noch fünf weitere Betriebsarten, die sich für Benutzer, Computer und Gruppen individuell einstellen lassen: Im transparenten Modus ist alles blockiert und der Client arbeitet völlig unsichtbar. Im Stealth-Modus zeichnet der Client alle Aktivitäten für den Administrator auf, blockiert aber gar nichts. Der Panic-Modus ist für Notsituationen gedacht und blockiert grundsätzliche alles, ohne dass dazu die bestehenden Vorgaben geändert werden müssen. Der Hidden-Icon-Modus arbeitet wie der normale Modus, nur ist das Icon in der Taskleiste nicht sichtbar. Auch der Silent-Modus ist dem "Normal Mode" ähnlich, zeigt dem Anwender aber keine Benachrichtigungen an.

Umfassende Kontrolle des Datentransfers

Die Kernfunktion von EPP besteht im Überwachen und Steuern des Zugriffs sowie im Kopieren von Daten durch Anwendungen in eine Cloud, auf Datenspeicher sowie über Schnittstellen. Im Englischen wird dies als Data Loss Prevention (DLP) bezeichnet. In der Basiskonfiguration überwacht EPP über die auf den Endpunkten installierten Clients alle vorhandenen Datenschnittstellen wie beispielweise USB-Speichergeräte, Kartenleser, CD-, DVD- und Floppylaufwerke, Digitalkameras, lokale Drucker, serielle und parallele Ports, zusätzliche Tastaturen, WiFi sowie Bluetooth. Das Cockpit listet insgesamt 35 Gerätetypen auf.

Der Administrator kann nun für jedes dieser Geräte den Zugriff steuern. In den meisten Fällen bedeutet dies, dass er den Zugriff erlaubt oder sperrt, für Kartenleser und CD/DVD-Brenner kann er aber auch einen reinen Lesezugriff vorgeben. Die meisten Optionen gibt es bei USB-Speichergeräten, denn hier unterstützt EPP die TrustedDevices-Technologie mit den Sicherheitsstufen 1 bis 4 und kann den Zugriff entsprechend granular festlegen. Bei der Beschreibung der EasyLock-Option gehen wir darauf noch genauer ein.

Recht komplex wird die Rechtevergabe angesichts der verschachtelten Abhängigkeiten, was eine entsprechende Einarbeitung

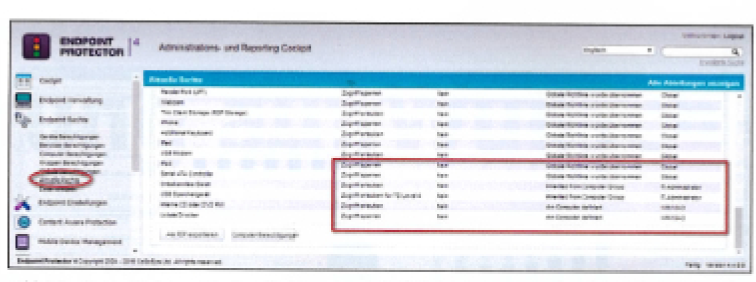

Bild 2: In der Ansicht der aktuellen Rechte erkennt der Administrator gut, auf welchem Weg das Recht vergeben wurde und welche Vererbung gegriffen hat.

erfordert. Darüber hinaus empfiehlt sich die Vorplanung eines Rechtekonzepts. So kennt EPP Geräte-, Benutzer-, Computer-, Gruppen- und globale Rechte. Wichtig ist daher für den Administrator die Kenntnis über die Vererbung, bei der die globalen Rechte die unterste Ebene darstellen und die Computerrechte die oberste. Darf also nach dem globalen Recht ein Arbeitsplatz ein bestimmtes Gerät nicht nutzen, entsprechend der Computerrechte aber schon, dann gilt letzteres. Im Test haben wir gezielt für einige Gerätetypen unterschiedliche Rechte vergeben und dann versucht, dies einige Tage später nachzuvollziehen. Sehr hilfreich ist dazu die Ansicht "Aktuelle Rechte", in der der Administrator für einen Computer genau sieht, welche effektiven Rechte für welchen Gerätetyp vergeben wurden. Zu beachten ist dabei, dass die Auflistung ähnlich wie ein Firewallregelwerk von oben nach unten zu lesen ist und hier der unterste Eintrag maßgeblich ist, wenn ein Gerät mehrfach auftaucht.

Wirksame Prüfung auf sensible Dateiinhalte

Die zweite Kernfunktion von EPP ist die Prüfung auf Dateiinhalte beim Kopieren oder Versenden, genannt Content Aware Protection (CAP). Sie ist extra zu lizenzieren, aber nicht für Linux-Endpunkte nutzbar. Ziel ist es, zu verhindern, dass sensible Daten über Anwendungen wie Dropbox oder per E-Mail das Unternehmen verlassen.

Um die CAP einzurichten, muss der Administrator zuerst entsprechende Policies anlegen, also Filterregeln, getrennt für Windows- und Mac-Endpunkte. Dabei kann er das Regelverhalten genau vorgeben, also ob eine Policy einen Datentransfer nur im Report dokumentieren oder auch blockieren soll. Optional lässt sich eine Benachrichtigung auf Clientseite unterdrücken. Auch kann der Administrator einen Schwellenwert hinsichtlich der Dateianzahl angeben, sodass es beispielsweise möglich ist, bis zu drei Textdateien an eine E-Mail anzuhängen, aber nicht mehr. Und dann kann er aus einer Vielzahl an Anwendungen auswählen, die in Rubriken (Browser, E-Mail-Clients, Instant Messaging, Cloud Dienste und Social Media) unterteilt sind. Unterbinden lassen sich auch das Kopieren auf eine Netzwerkfreigabe sowie der Transfer über die Zwischenablage oder die PrintScreen-Funktion. Hier weist das Handbuch allerdings darauf hin, dass bei PrintScreen die Windows-Funktion kontrolliert wird, sich aber kein zusätzlich installiertes Tool überwachen lässt.

Zuletzt muss der Administrator ein Filterkriterium für die Dateien angeben, also ob beispielsweise bestimmte Text- oder Grafikdateien blockiert werden sollen. Es gibt hier die Möglichkeit, nach Dateityp zu filtern oder auch nach Inhalt, wobei dann anhand von Wörterbüchern verglichen wird. Dazu kann der Administrator innerhalb von EPP eine oder auch mehrere Wörterlisten anlegen und je nach Bedarf einem Filter zuweisen. So ist es möglich, gezielt nach einzelnen Schlagworten zu filtern. EPP schaut dann tatsächlich in die Textdateien hinein und prüft sie auf die Schlagworte.

Ist eine Policy erstellt, muss der Administrator sie einer Gruppe, Abteilung, Computer oder einem Benutzer zuweisen. Gut gefallen hat uns, dass sich die angelegten Regeln unabhängig von der Zuordnung direkt in der CAP-Richtlinienansicht ein- und ausschalten lassen. Um eine Policy also nur zeitweise greifen zu lassen, ist es nicht notwendig, das ganze Regelwerk zu verändern, sondern der Administrator kann einzelne Policies einfach aus- und auch wieder einschalten. Von dieser Übersicht aus kann er die Regeln ebenso editieren oder bei Bedarf duplizieren, wenn er eine ähnliche Regel erstellen will. Wichtig ist bei Regelkonflikten zu beachten, dass die Policies entsprechend ihrer Priorität angewendet werden, letztendlich auf der CAP-Richtlinienansicht von links oben nach rechts unten. Durch Verschieben kann der Administrator die Priorität ändern.

Neben den erwähnten individuellen Wörterbuchlisten lassen sich auch URL Whitelists, Domain Whitelists sowie Regular Expressions, also bestimmte Zeichen- und Buchstabenfolgen definieren, um diese bei der Filterdefinition zu verwenden. Im Test erzeugten wir eigene Filter und versuchten dann, diese zu überlisten. So haben wir beispielsweise Dateien von MS Word blockiert und dann versucht, doch eine durch den Filter zu schleusen, indem wir sie umbenannten. So leicht lässt sich EPP allerdings nicht überlisten, da er in jedem Fall die Datei öffnet und dann sehr wohl erkennt, um welchen Dateityp es sich handelt.

Mobile Geräte fest im Griff

Während bei den bisher beschriebenen Funktionen stets PC-Systeme und Notebooks als Endpunkte im Fokus standen, unterstützt EPP mit der Option Mobile Device Management (MDM) auch die Überwachung von mobilen Geräten unter iOS sowie Android. Die Aufnahme in EPP läuft in beiden Fällen ähnlich ab.

Für den Test hatten wir ein Android-Tablet von Samsung zur Verfügung, das wir einbinden wollten. Die Kommunikation erfolgt grundsätzlich über einen Push-Dienst, und bei Android ist dazu Google Cloud Messaging (GCM) einzurichten. Die Vorgehensweise zur Erstellung des notwendigen GCM Accounts wird durch Google definiert und ändert sich hin und wieder, wie wir bereits in der Vergangenheit schon selbst bei anderen Tests feststellen mussten. Auch im vorliegenden Fall passte die von CoCoSys erstellte Beschreibung nicht mehr ganz, aber nach

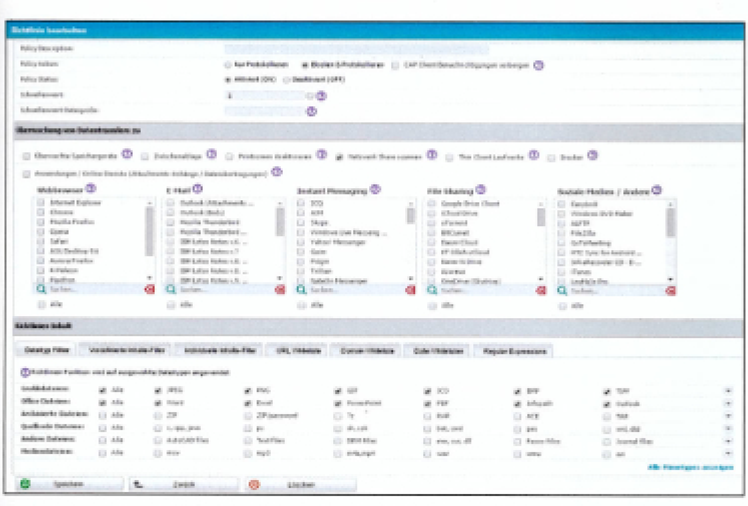

Bild 3: Die Definition einer CAP-Policy beinhaltet eine Vielzahl an Optionen, um hier sehr granulare Einstellungen vornehmen zu können.

einigen Versuchen gelang es dann doch, ein Google-API-Projekt korrekt anzulegen, um schließlich die Projektnummer und den erzeugten API-Key im EPP-Cockpit einzutragen.

Ist diese einmalige Vorarbeit erledigt, sind für jedes einzurichtende Gerät nur noch wenige Schritte notwendig. So stehen für eine Geräteregistrierung vier Möglichkeiten zur Verfügung. Dies sind der Versand einer E-Mail, einer SMS, die Eingabe der Adresse im Browser oder das Einscannen eines QR-Codes aus dem Cockpit. Bei der Einladung per E-Mail oder SMS werden die MDM ID und ein One Time Code (OTC) mitgeliefert. Bei der Browser-Eingabe oder der Nutzung des QR-Codes kommt nur die MDM ID mit. Der OTC ist dann einer Liste im Cockpit zu entnehmen. Nach der Authentisierung ist der EEP-Client herunterzuladen, wobei in der Regel der Hinweis auftaucht, dass es sich hier um einen Download aus einer unsicheren Quelle handelt, was der Anwender explizit erlauben muss. Nach der Installation fragt der Client den Benutzernamen und die Telefonnummer ab. Sofern der Mitarbeiter im MDM Management von EPP angelegt wurde, erfolgt eine entsprechende Zuordnung.

Übrigens gibt es noch einen anderen Installationsweg, denn der EPP-Client ist auch im Google Play Store erhältlich und kann von dort installiert werden, um den Download aus unsicherer Quelle zu umgehen. Allerdings sind dann im Client sämtliche Daten inklusive der MDM ID manuell einzugeben. Für die Einrichtung liefert CoSoSys ein eigenes MDM-Handbuch mit.

Befindet sich ein mobiles Gerät unter der Kontrolle von EPP, stehen dem Administrator vielfältige Steuermöglichkeiten zur Verfügung, wobei dies systembedingt bei iOS umfangreicher ist als bei Android. So lassen sich Passwortrichtlinien vorgeben und bei iOS Gerätefunktionen wie unter anderem die Kamera sperren, In-App-Käufe unterbinden sowie die Nutzung von Siri verbieten. Auch gibt es die Möglichkeit zur Ortung des Geräts inklusive Historie, sodass sich nachvollziehen lässt, wo sich das Gerät in der letzten Zeit befunden hat.

Weiterhin kann der Administrator ein Gerät sperren und löschen, WiFi und die installierten Apps sowie Kontakte verwalten, auch sieht er in einer Historie die Liste sämtlicher Aktivitäten. Insgesamt konnten wir uns davon überzeugen, dass EPP eine sehr umfassende Kontrolle über die verwalteten mobilen Geräte besitzt. Aus Sicht eines Anwenders stellen wir uns allerdings die Frage, ob es diesem gefällt, wenn beispielsweise die regelmäßige Aufzeichnung der Ortungsdaten dem Chef verrät, wo sich der Mitarbeiter überall aufgehalten hat – auch in der Freizeit, wenn er sein Smartphone stets mitführt, um für die Firma erreichbar zu sein, oder gar sein eigenes dafür nutzt.

Verschlüsselter Datentransfer

Wie schon erwähnt sind innerhalb von EPP einige Module wie das MDM oder die CAP extra zu lizenzieren. Darüber hinaus gibt es die Option EasyLock für einen verschlüsselten Datentransfer, indem es einen USB-Datenträger in ein Trusted Device der Stufe 1 verwandelt. Hintergrund ist, dass die Stufe 1 erreicht wird, indem die Daten auf einem USB-Datenträger in einem verschlüsselten Container gespeichert werden. Die drei nächsten Stufen sind nicht so einfach realisierbar und erfordern speziell zertifizierte Hardware. Die Stufe 2 wird beispielsweise durch eine zusätzliche biometrische Prüfung oder eine

erweitere Verschlüsselung per Software erreicht. Die Stufe 3 muss die Regularien wie SOX, HIPAA, GBLA, PIPED, Basel II, DPA oder PCI 95/47/EC erfüllen. Die Stufe 4 bietet maximale Sicherheit für militärische und staatliche Belange.

Für die Verwendung eines Trusted Device muss es vom EPP-Server als solches erkannt werden, andernfalls ist es nicht nutzbar. Mit der EasyLock-Option ist es nun relativ einfach, einen normalen USB-Datenträger in ein Trusted Device 1 zu verwandeln. Hierzu lädt der Administrator aus dem Cockpit die EasyLock-Software herunter und kopiert sie in das Root-Verzeichnis des Datenträgers. Dann muss er sie an der Stelle aufrufen und ein Verschlüsselungspasswort sowie einen Hinweis dazu eingeben. In diesem Zug legt das Tool eine Containerdatei an, in der die Dateien mit 256 Bit AES verschlüsselt gespeichert werden. Die Bedienung von EasyLock ist recht einfach, denn der Administrator sieht in der Oberfläche zwei Fenster: im linken den Inhalt des Endgeräts, ähnlich wie im Explorer, und im rechten den Inhalt des gesicherten Bereichs. Indem er nun Dateien oder auch ganze Verzeichnisse von links nach rechts kopiert, werden diese verschlüsselt abgelegt. Das Konzept erlaubt es übrigens, auf einem Datenträger Dateien auch unverschlüsselt abzulegen und nur einen Teil im verschlüsselten Container.

In Verbindung mit EPP funktionierte der Schutz im Test auch problemlos, nur war etwas Geduld gefordert. Sind an einem Endgerät nur Trusted Devices der Stufe 1 zugelassen, so erscheint trotzdem beim Einstecken eines mit EasyLock versehenen Datenträgers erst einmal eine Meldung des EPP-Client, dass am Endgerät ein nicht zugelassenes Gerät eingesteckt wurde. Davon darf sich der Anwender nicht beirren lassen, denn der EPP-Client schaut nun auf dem Datenträger nach, ob er im Root-Verzeichnis die EasyLock-Datei findet und startet diese. Nach der Eingabe des Passworts hat der Anwender dann Zugriff auf den verschlüsselten Inhalt. Mit dem Explorer kann er den Datenträger übrigens nicht öffnen, es besteht also wie beabsichtigt kein Zugriff auf eventuell darauf befindliche unverschlüsselte Dateien, und er kann dort auch nichts ablegen.

EasyLock beinhaltet die Möglichkeit, den Container sicher zu löschen und das auch ohne vorherige Passworteingabe. Das ist letztendlich auch die letzte Möglichkeit zur Bereinigung, wenn das Passwort vergessen wurde und auch der hinterlegte Hinweis nicht mehr weiterhilft.

Umfassende Aufzeichnung der Aktivitäten

EPP verhindert nicht nur einen ungewünschten Datentransfer, sondern protokolliert auch alle derartigen Aktivitäten sehr detailliert. Das ist insofern wichtig, da es wie schon erwähnt die Möglichkeit gibt, nur zu dokumentieren, aber nicht zu reglementieren. Die beiden Cockpit-Menüpunkte "Reporte und Analysen" sowie "Benachrichtigungen" beschäftigen sich damit.

Im Abschnitt "Benachrichtigungen" kann der Administrator Systembenachrichtigungen, normale sowie CAP-Benachrichtigungen und solche für mobile Geräte erstellen. Zur Filterung stehen Gerät, Benutzer, Gruppen und Abteilungen sowie das Ereignis zur Verfügung. Unter "Reporte und Analysen" hat der Administrator die Möglichkeit, diverse Berichte und Datenprotokollierungen abzurufen, getrennt nach normalen und CAP-Berichten sowie Historien bezogen auf Computer, Benutzer und Geräte. Aufgezeichnet werden auch die Aktionen der Administratoren und es lassen sich Statistiken abrufen nach der Datentransfermenge oder der Anzahl der Geräteverbindungen, um die aktivsten Endpunkte oder Benutzer zu ermitteln und so eventuell auf ungewöhnlich häufige Aktivitäten aufmerksam zu werden.

Fazit

Endpoint Protector ist eine leistungsfähige Software zum Schutz vor Datendiebstahl, Datenverlust, Datenlecks, Datenklau und Insider-Bedrohungen für Endpunkte sowie mobile Geräte. Als Lösung für Data Loss Prevention und Schnittstellensicherheit bietet das Tool Schutz gegen unerlaubten Transfer von Daten per E-Mail, Webmail, Cloud-Dienste sowie tragbare Datenspeicher wie USB-Sticks in Unternehmen und Behörden. Dank der Realisierung als virtuelle oder Hardware-Appliance kann die Lösung sehr schnell in Betrieb genommen werden. Auf den zu schützenden Endpunkten werden neben Windows auch macOS und Linux Ubuntu/openSUSE sowie iOS als auch Android unterstützt, sodass das Tool auch für heterogene Umgebungen geeignet ist.

Insgesamt hat uns EPP durch seine sehr umfassenden Möglichkeiten überzeugt, die Datenbewegungen von und zu den Endpunkten wirksam und unter verschiedenen Gesichtspunkten zu überwachen. Gut gefallen hat uns auch, dass ein Anwender durchaus einzelne Dateien beispielsweise an eine E-Mail anhängen kann, EPP aber Alarm schlägt oder sogar sperrt, wenn große Datenmengen bewegt werden. Immerhin darf das Werkzeug nicht zum Hemmschuh der Arbeit der Kollegen werden. In Unternehmen mit Betriebsrat sollte der Einsatz auch mit diesem besprochen werden, da EPP sehr viel über das Arbeitsverhalten aufzeichnen und bei mobilen Geräten durch eine regelmäßige Ortung ein Bewegungsprofil erstellen kann. *(jp)*

So urteilt IT-Administrator

Clientunterstützung	9
Schnittstellenüberwachung	9
Dateiinhaltsüberwachung	8
Management mobiler Geräte	8
Reporting	8

Die Details unserer Testmethodik finden Sie unter www.it-administrator.de/testmethodik

Dieses Produkt eignet sich

optimal für Unternehmen, die auch in einer heterogenen Umgebung verhindern wollen, dass über die Mitarbeiter Daten unkontrolliert das Unternehmen verlassen oder eingeschleust werden.

bedingt für Unternehmen, die bereits andere Maßnahmen ergriffen haben oder ein anderes Produkt nutzen, um einen Datenklau zu verhindern. Hier sollte erst einmal ein Leistungsvergleich erfolgen.

nicht, wenn es aus der Unternehmensphilosophie heraus nicht gewünscht ist, die Mitarbeiter auf diese Art und Weise zu kontrollieren.