5 | 19 Sonderdruck für Endpoint Protector

IT Administrator
Das Magazin für professionelle System- und Netzwerkadministration

CoSoSys Endpoint Protector

www.it-administrator.de

CoSoSys Endpoint Protector

Wir haben eine undichte Stelle!

von Frank-Michael Schlede und Thomas Bär

Quelle: stylephotographs – 123RF

Nicht erst seit die DSGVO im Bedarfsfall eine komplette Löschung einzelner personenbezogener Daten erfordert, besteht die Notwendigkeit, sensible Speicherbereiche genau zu überwachen. Dazu zählt, sicherzustellen, dass Daten das Netzwerk nicht durch Hintertüren verlassen. Endpoint Protector von CoSoSys soll Unternehmensnetze vor Datenverlust und Datendiebstahl über Schnittstellen wie USB, browserbasierte Anwendungen und mobile Geräte schützen.

DLP ist kein stehender, abgegrenzter Begriff, der ein definiertes Set an Funktionalitäten umfasst. Bei der Abkürzung, die neben "Data Loss Prevention" mitunter auch für "Data Leakage Prevention" steht, handelt es sich eher um einen Marketingbegriff. Klassisch gesehen gehört DLP zu den Schutzmaßnahmen, die direkt den Schutz der Vertraulichkeit von Daten unterstützen und je nach Ausprägung direkt oder indirekt deren Integrität und Zuordenbarkeit. Letztendlich geht es bei DLP darum, genau zu ermitteln und zu protokollieren, wer was wann wie mit welchen Dokumenten durchgeführt hat. Dabei sind verschiedene Aktionen oder Reaktionen denkbar: Benutzer im Umgang mit schützenswerten Daten lediglich sensibilisieren, beispielsweise durch Warnhinweisfenster, oder Maßnahmen, wie etwa das Speichern von Daten auf ein USB-Device aktiv zu unterbinden. Eine wirksame Implementierung des DLP erfordert meist einen Softwareagenten auf den beteiligten Endgeräten. Die Verwaltung dieser Agenten erfolgt zumeist zentral.

In diesem Zusammenhang sei auch erwähnt, dass DLP in Bezug auf die Datenschutzbedenken nicht ganz unumstritten ist. Wer als IT-Verantwortlicher mit dem Gedanken spielt, eine solche Technologie in seinem Unternehmen einzuführen, ist somit gut beraten, die Personal- oder Mitarbeitervertretung frühzeitig in ein solches Projekt einzubinden.

CoSoSys bietet mit dem Endpoint Protector eine Komplettlösung für die Umsetzung von DLP in Unternehmen verschiedener Größen an. Das Portfolio umfasst die kleine KMU-Variante, eine SaaS/Cloud-Darreichung und eine Appliance-Installation für den On-Premises-Betrieb. Letztere ist gemäß Common Criteria EAL2 und von der ITSCC zertifiziert. Neben den Funktionen der Gerätekontrolle, USB-Schutz, erzwungener Verschlüsselung von USB-Datenträgern, DLP für alle gebräuchlichen Plattformen und Druckern hilft die Software bei der Sicherstellung der eigenen GDPR-Konformität und bietet darüber hinaus noch ein eigenes Mobile Device Management für iOS und Android zur Abbildung von BYOD-Szenarien.

In der Cloud nicht aktuell

Zunächst wollten wir uns cloudbasiertes DLP als "My Endpoint Protector" von CoSoSys anschauen und füllten das entsprechende Antragsformular auf der Webseite des Herstellers aus. Binnen kürzester Zeit bekamen wir die notwendigen Informationen per E-Mail zugeschickt und konnten uns, ebenfalls innerhalb von Minuten, auf der Managementoberfläche per Browser umschauen. Im Vergleich zu den uns vorliegenden Informationen fehlte jedoch ein entsprechender Punkt im Hauptmenü. Auf Nachfrage bestätigte uns CoSoSys, dass der SaaS-Dienst "MyEndpoint Protector" nicht dem technischen Stand des Endpoint Protector 5.2.0.5 entspricht.

Daher verlegten wir die Teststellung kurzerhand in unsere lokale Umgebung und importierten die OVF-Datei unter VMware Workstation 14. Zu der auf Ubuntu

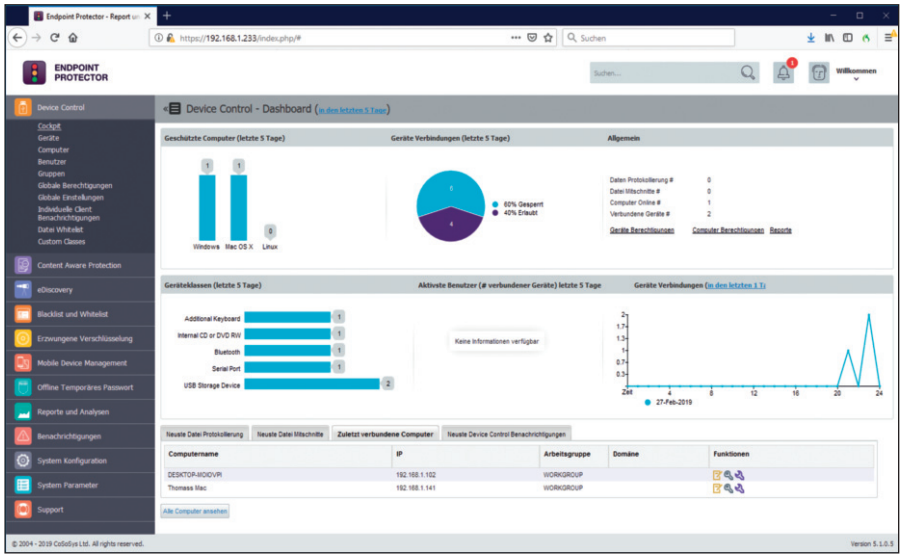

Bild 1: Das Dashboard für den Endpoint Protector von CoSoSys liefert alle aktuellen Ereignisse auf einen Blick.

basierenden Appliance gesellten wir einen Rechner mit macOs 10.13.6, virtualisiert mit Parallels Desktop 14 für Mac, und einen Windows-10-Pro-Computer, ebenfalls als Client. Die Cloudvariante bietet ein Subset der Funktionen des Endpoint Protector. Lediglich die Linux- und Thin-Client-Unterstützung, der Dateimitschnitt und die AD-Anbindung bleiben der SaaS-Variante vorenthalten.

Der Import und die Inbetriebnahme der Appliance gingen erfreulich rasch von der Hand. Ein Update zog sich die virtuelle Appliance noch während der Einrichtung, auch dies verlief ohne Probleme. Für die Nutzung bietet der Hersteller neben der kostenpflichtigen Vollversion eine 30-Tage-Testversion für alle Plattformen für maximal 50 herkömmliche und fünf mobile Endpoints. Für einen längerfristigen Test in einer reinen Windows-Landschaft mit jeweils fünf stationären und mobilen Endgeräten gibt es noch den "Appetizer" mit einer Laufzeit von bis zu einem Jahr.

Klar strukturierte GUI

Wie zu erwarten war, steuert der Administrator die Endpoint-Protector-Lösung komplett mit dem Browser. Nach der Anmeldung erscheint die GUI in einer klaren Strukturierung mit einem Hauptmenü auf der rechten Seite und einem großen Arbeits- und Informationsbereich auf der linken Seite. Das Design ist modern und spricht optisch an, ohne dass dabei zu viele Elemente den Blick auf das Wesentliche versperren. Einzig die Darstellung in der Richtlinienverwaltung ist ein wenig gewöhnungsbedürftig: Die Symbolik der zwei blauen "Blätter" könnten leicht mit "Bearbeiten" in Verbindung gebracht werden, dabei handelt es sich um den Befehl "Duplizieren", während der goldene Stift auf einem Papier den Bearbeitungsdialog öffnet.

Neben der zentralen Protector-Appliance sind logischerweise Clientsysteme erforderlich. Dabei kann es sich um Clients mit Windows-, macOS- oder Linux-Betriebssystem handeln, aber auch um Serverinstallationen. Für die Installation und Bereitstellung der Agentensoftware spielt die Variante kaum eine Rolle – für die Integration zur Verteilung im Active Directory bietet sich dem Admin eine eigene Anleitung an. Handelt es sich bei einem Server um einen Terminalserver, muss der zuständige Systembetreuer dies in der Computerübersichtsliste per Optionshäkchen hinterlegen. Der Einsatz der Endpoint-Protector-Software im RDP-Umfeld geht auch mit entsprechenden Lizenzkosten einher. Dieser ist aber erforderlich, um eine ordnungsgemäße Gerätesteuerung für "RDP Storage Devices" zu gewährleisten.

Richtlinien sicher, Daten flexibel

Richtlinien stellen ein wesentliches Element im Endpoint Protector dar. Die Richtlinie legt der Administrator über Benutzergruppen oder Abteilungen, die in den Tiefen der Dialoge feiner aufgegliedert werden können. Im Zweifelsfall hat der IT-Profi aber auch die Möglichkeit, seine Regelwerke auf einzelne Computer oder Benutzer anzuwenden – und das per Mausklick. Der Aufbau einer Richtlinie ist von Seiten des Herstellers in der Regel vorgegeben. Beispielsweise gibt es im Segment "eDiscovery" zunächst einmal Optionsfelder für die Betriebssysteme Windows, macOS und Linux. Folgerichtig ist es erforderlich, für jedes OS eine eigene Richtlinie zu erstellen. Dank der Kopierfunktion ist das mit wenigen Mausklicks erledigt.

Neben der Angabe eines Namens und einer Beschreibung gilt es von nun an, sehr überlegt an die Sache heranzugehen. Mit einem einfachen Schieber lässt sich die Regel aktivieren und anschließend

CoSoSys Endpoint Protector

Produkt
Software zur Sicherung sensibler Daten vor Bedrohungen durch tragbare Speichergeräte, Clouddienste und mobile Geräte.

Hersteller
Endpoint Protector GmbH
www.endpointprotector.de

Preis
Endpoint Protector wird als virtuelle oder als Hardware-Appliance ausgeliefert; ab 500 Endpunkten greifen Kunden in der Regel zur virtuellen Appliance. Die Module "Device Control" und "Content Aware Protection" kommen bei der virtuellen Appliance auf 26.180 Euro, so es sich ausschließlich um Windows-Rechner handelt. Sollen USB-Verschlüsselung und eDiscovery an Bord sein, steigt der Preis auf 52.360 Euro. Bei der Hardware-Appliance sind die Kosten für den Hardware-Anteil aufzuschlagen. Enthalten sind Updates und Support für ein Jahr.

Systemvoraussetzungen
Virtuelle Appliance (im Format OVF, OVA, VHD oder PVM): 2 CPU-Kerne, 4 GByte RAM, 320 GByte Festplattenspeicher. Hypervisor-Unterstützung (ab Version): VMware Player 7.1, VMware Workstation 11.1.0, Oracle VirtualBox 5.0.28, VMware Fusion 7.1.3, Parallels Desktop for Mac 11.1.3, VMware vSphere (ESXi) 6.0.0, Citrix XenServer 6.2 und Hyper-V Manager unter Windows Server 2016.

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

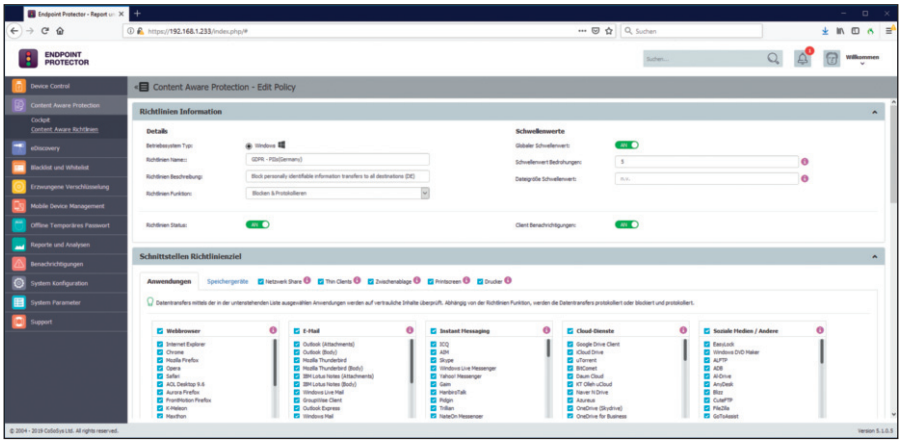

Bild 2: Richtlinien stellen das wichtigste Arbeitsmittel des Endpoint Protector dar. Explizit legt der Administrator fest, was erlaubt ist und was nicht.

über Schwellenwerte festlegen, welche gefundene Anzahl von zu definierenden Treffern eine "Bedrohung" aktiviert. Selbst die Dateigröße in MByte kann in einer Richtlinie als Kriterium für eine mögliche Gefahr des Datenverlusts gelten. Existieren plötzlich sehr große Datenmengen an einem ungewöhnlichen Ort, macht die Software den Administrator darauf aufmerksam.

Danach gliedert sich das Fenster in die Bereiche "Blacklist" und "Whitelist", über die IT-Profis mit der weißen Liste Ausnahmen festlegen, die in der Wertigkeit über einem Blacklist-Eintrag liegen. Ebenso sind Computer/Maschinen-Zuordnungen höherwertiger als Benutzer/Gruppen-Zuweisungen. Eine Blacklist setzt sich aus einer großen Anzahl von Auswahlfeldern zu Dateitypen, vordefiniertem Inhalt, individuellem Inhalt, Dateinamen, Scan-Location, regulären Ausdrücken oder HIPAA-Daten (Informationen aus dem Gesundheitssystem) zusammen.

Allein bei den Dateitypen gibt es 92 verschiedene Arten zur Auswahl und unter vordefinierten Inhalten versteht der Hersteller Kreditkartenformate, Bankverbindungssyntax, Zeichenfolgen für Personalausweise verschiedener Länder oder Sozialversicherungsnummern. Dateinamen und Scan-Location verstehen sich von selbst und unter regulären Ausdrücken konnten wir beliebige Pattern und Musterfolgen anlegen. In unserem Test verwendeten wir einige Schlüsselworte, um in einer Anzahl von Daten aus dem Gesundheitswesen diejenigen mit Gesundheits- und Krankenpflegeinhalt von den klassischen ärztlichen Dateien zu trennen. Die Software warnt jedoch, dass die intensive Nutzung von regulären Ausdrücken mit einer hohen Prozessorlast einhergehen kann.

Für den Gesundheitsbereich führt der Hersteller einen Reiter "HIPAA". Eine HIPAA-Richtlinie sollte personenbezogene Daten wie Adressen, Telefon- und Faxnummern, E-Mails und individuelle Wörterbücher enthalten. Dies sollte ein Administrator im Krankenhaus in den vorherigen Fenstern gleich berücksichtigen, denn im Abschnitt HIPAA selbst geht es nur um FDA-anerkannte Pharmaunternehmen, verschreibungspflichtige Medikamente nebst Generika und die Diagnose- und Prozedurencodes gemäß dem ICD9- beziehungsweise ICD10-Schema. In einer Klinik im deutschsprachigen Raum sind derlei Vorgaben komplett nutzlos, es sei denn, die Arbeitssprache ist Englisch, da alle vorgefertigten Richtlinien des Herstellers in eben dieser Sprache vorliegen.

Sensible Informationen lassen sich finden, aber nicht bewegen

Das Endpoint Protector eDiscovery prüft gespeicherte Dateien an den in der Richtlinie definierten oder ausgeklammerten Orten und identifiziert die als vertrauliche Informationen eingestuften Daten auf den zur Prüfung anvisierten Endpunkten. Als mögliche Schutzmaßnahmen kann der Administrator eine Verschlüsselung oder ein gezieltes Löschen vorgeben. Die Software unterscheidet bei Bedarf interne von externen Bedrohungen: nicht autorisierte Mitarbeiter, die sensible Daten auf ihren Computern speichern, sowie Angreifer, die es schaffen, den Netzwerkschutz zu umgehen, und versuchen, an Unternehmensdaten zu gelangen.

Zwar weist der Hersteller in seiner Dokumentation darauf hin, dass es zwingend erforderlich ist, Informationen wie Bankverbindungen, persönlich identifizierbare Informationen, Sozialversicherungsnummern und andere Mitarbeiter- und Geschäftsunterlagen rechtskonform zu speichern. Doch fehlte uns im Test die Möglichkeit, die über die Richtlinie identifizierten Dateien, die beispielsweise außerhalb eines zentralen Shares in lokalen Verzeichnissen zu finden sind, gezielt an einen zentralen Ort zurückzuspielen. Im Zweifelsfall gilt die Verschlüsselung dieser Daten als ein probates Mittel, um sicherzustellen, dass im Fall eines Computerverlustes oder Diebstahls diese Informationen nicht in böswillige oder sorglose Hände gelangen.

Device-Zugriffe schützen Daten rigoros

Ein wesentlicher Bestandteil eines DLP-Konzepts ist "Device Control", da nicht selten größere Datenmengen per externer USB-Festplatte oder USB-Thumbdrive auf die Reise gehen – da stellen Wechselda-

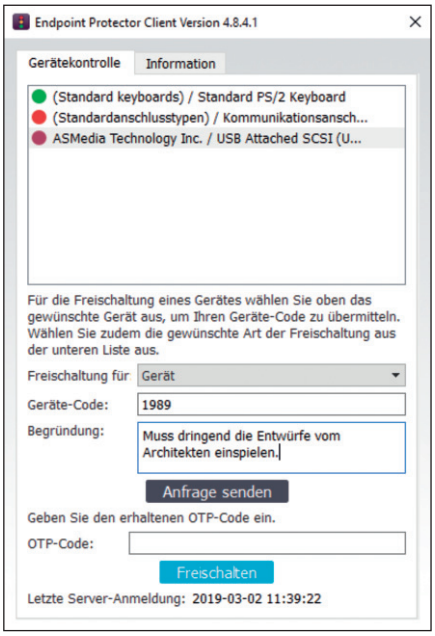

Bild 3: Benötigt ein Anwender einen USB-Device-Zugriff, kann er diesen Wunsch automatisiert per E-Mail an den Administrator senden.

tenträgersysteme auch keine Ausnahme dar. Jeder Administrator weiß, dass mitunter ganze virtuelle Maschinen in wenigen Minuten auf einen solchen Datenträger kopiert sind. Ohne dass die IT-Abteilung die Kontrolle über Wechseldatenträger jeglicher Art gewinnt, ist eine Sicherstellung, dass keine Daten unerwünscht abfließen, gar nicht möglich.

Die Gerätekontrolle im Endpoint Protector umfasst die Prüfung auf austauschbare Datenträger mit einer recht feinen Zugriffssteuerung und einer Ad-Hoc-Freigabeanforderung per E-Mail. Praktischerweise gilt dies nicht nur für Windows-basierte Computer, sondern auch für Apple-Systeme mit USB-, FireWire- oder Thunderbold-Datenaustausch. In unserem Test zeigte sich die Software auf unseren Clientsystemen äußerst robust und rigoros. Glücklicherweise ist der Einsatz von Tastaturen und Mäusen von Haus aus zulässig, während die unkoordinierte Zusammenarbeit mit USB-Datenträgern, Kartenlesern oder Bluetooth-Geräten konsequent untersagt blieb.

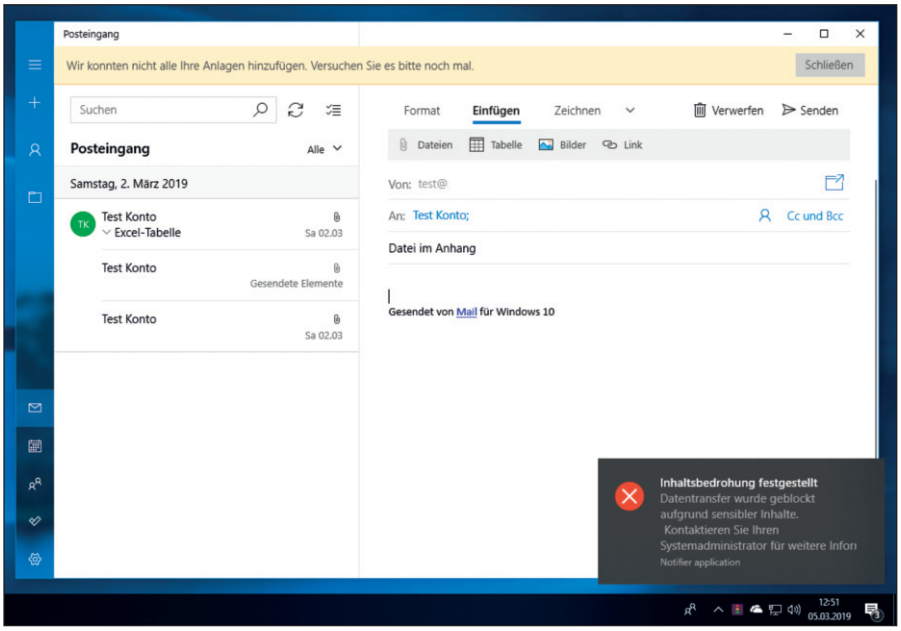

Bild 4: Endpoint Protector verhindert die Verbreitung schützenswerter Dokumente über alle erdenklichen Wege, darunter Wechseldatenträger, Cloudspeicherdienste oder wie hier per E-Mail.

Sensible Daten zuverlässig geschützt

An dieser Stelle begegneten wir den für das eDiscovery angelegten Richtlinien gleich noch einmal. In den Richtlinien für die "Content Aware Protection" (CAP) konnten wir die Prüf- und Suchroutine der Inhalts- und Metadatenprüfung noch einmal verwenden. Der Clientagent überwacht, je nach Einstellungen der Systemverantwortlichen, das Geschehen sehr genau. Solange ein Mitarbeiter nur lokal mit den relevanten Dateien arbeitet, greift die Software nicht ein und an sich bemerkt niemand, dass im Hintergrund jede Aktivität noch einmal einer Prüfung unterzogen wird.

Versucht der Mitarbeiter jedoch, Dateien oder Ordner, die als sensibel definiert wurden, an einen anderen Ort zu verschieben, greift die Software beherzt ein und unterbindet die Transaktion. Der E-Mail-Versand von Dateien war uns so nicht möglich – erst nachdem wir den betreffenden Anhang entfernt hatten, konnten wir unsere E-Mails verschicken. Der Schutz ist dabei nicht nur auf Applikationen wie Outlook, Apple Mail, Thunderbird oder den Windows-Mailer beschränkt – selbst der im Browser gestartete Webmailer blockierte, sofern wir versuchten, auf den "Sende"-Button zu klicken.

Entsprechend umfangreich ist die Richtliniengestaltung in diesem Bereich – unter "Browser" finden sich die üblichen Platzhirsche wie Chrome, Firefox, Safari, Edge, Internet Explorer, aber auch Varianten wie der FrontMotion FireFox oder Maxthon oder der Tor-Browser. Alle bekannten Instant-Messaging-Programme, Clouddienste oder E-Mail-Applikationen und -Services sind ebenfalls zu finden. Letztendlich blockierte die Software sogar den Datenaustausch per WinSCP-SFTP-Transfer sowie den Upload in ein persönliches OneDrive-Konto bei Microsoft.

Fazit

CoSoSys Endpoint Protector ist eine leistungsfähige Lösung, um Dateizugriffe und Dokumentenaustauschvorgänge per DLP-Vorstellungen zu sichern. Die einfache Inbetriebnahme und die Flexibilität im Regelwerk konnten im Test in jedem Fall überzeugen. Dass die im Internet angebotene Testversion des "MyEndpoint Protector" nicht über den entsprechenden Release-Stand – immerhin fünf Monate nach Ankündigung auf der it-sa – der On-Premises-Version verfügt, wundert dann schon ein wenig. Wer sich erstmalig mit DLP auseinandersetzt und die ansonsten übliche Komplexität der notwendigen Betriebslandschaft scheut, ist mit der virtuellen oder physischen Appliance von CoSoSys gut beraten. *(jp)* IT

So urteilt IT-Administrator

Gerätesicherheit	8
Richtliniensätze	8
Datei-Erkennung	7
Schutz vor Datenabfluss	8
OS-Unterstützung	8

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

Dieses Produkt eignet sich

optimal für KMUs, die eine Dokumentenüberwachungen auf verschiedenen Plattformen benötigen.

bedingt für Firmen die vorgefertigte deutschsprachige Richtliniensätze benötigen.

nicht für Firmen, die keine schützenswerten Dokumente vorhalten oder in denen eine solch enge Überwachung von Mitarbeitern unzulässig wäre.