ENDPOINT PROTECTOR

GEMEINDE WEYHE

Die Gemeinde Weyhe hat mit Endpoint Protector alle Datenbewegungen im Griff

CASE STUDY | Gemeinde Weyhe

PROFIL

Branche

Kommunalverwaltung

Die Herausforderung

Abfluss sensibler Daten verhindern; die Verwendung von Devices und den Upload von Dateien regulieren

Die Lösung

Endpoint Protector Device Control und Content Aware Protection

Warum Endpoint Protector?

- granulare Einstellmöglichkeiten
- umfassende Protokollierung
- günstiges Preis-Leistungs-Verhältnis

www.**endpointprotector**.de

Über die Gemeinde Weyhe

Die Gemeinde Weyhe mit ihren neun Ortsteilen liegt vor den Toren von Bremen mitten im Grünen. Sie verbindet eine ländliche Umgebung mit der guten Erreichbarkeit großstädtischer Angebote und wird als Lebensmittelpunkt besonders von Familien sehr geschätzt. Die Gemeindeverwaltung beschäftigt mehr als 500 Mitarbeiter, davon 150 an IT-Arbeitsplätzen im Rathaus, und bietet ihren 30.000 Einwohnern ein breites Spektrum an Dienstleistungen. Darüber hinaus betreibt sie Einrichtungen wie Bibliotheken, Kinderbetreuungsstätten, ein Freibad und ein Fahrradparkhaus am Bahnhof.

Die Herausforderung

Aus Gründen des Datenschutzes setzt die Gemeindeverwaltung bereits seit Jahren eine Lösung für Data Loss Prevention ein. Neben Geräte- und Inhaltskontrolle zum Schutz personenbezogener Daten ist es wichtig, dass Bildmaterial nur von berechtigten Mitarbeitern ins Netzwerk geladen werden kann. Diese Bilder werden von Außendienstmitarbeitern mit Digitalkameras oder Smartphones zur Dokumentation von Zuständen beispielsweise von kommunalen Gebäuden erstellt und sind Arbeitsgrundlage für Fachabteilungen wie Bau und Liegenschaften. Nach der Migration auf Windows 10 zeigte sich, dass die bestehende Lösung die Erkennung mancher Geräte nicht mehr unterstützt und daher abgelöst werden muss.

"Wir sind sehr zufrieden mit Endpoint Protector. Dank der Lösung haben wir die volle Kontrolle über sämtliche Datenbewegungen und können maximalen Schutz mit wesentlich weniger Arbeitsaufwand umsetzen."

Ralf Eggers,
IT-Leiter,
und Roberto Petrocelli,
IT-Administrator, Gemeinde Weyhe

Über Endpoint Protector

Endpoint Protector schützt Windows-, Mac- und Linux-Rechner vor Datenverlust, Datendiebstahl und Datenlecks, indem alle Datentransfers zu cloudbasierten Diensten und Anwendungen wie Webbrowser, E-Mail, Skype überwacht und gegebenenfalls blockiert werden. Die Lösung überwacht auch den Einsatz tragbarer Speichermedien wie USB-Sticks, CDs / DVDs, HDDs, Speicherkarten an Endpoints mit den Betriebssystemen Windows, macOS und Linux. Starke Sicherheitsrichtlinien verhindern, dass Daten unrechtmäßig oder aus Versehen das Unternehmen verlassen.

Die Lösung

Die Gemeinde entschied sich für Endpoint Protector, da die Lösung durch vielseitige Konfigurationsmöglichkeiten, umfassende Protokollierung und ein günstiges Preis-Leistungs-Verhältnis überzeugte. Für die 150 IT-Arbeitsplätze im Rathaus wurden die Module Device Control (DC) und Content Aware Protection (CAP) lizensiert.

Die neue DLP-Lösung ließ sich schnell und einfach installieren und in Betrieb nehmen; bei den Begrifflichkeiten des GUI mussten die IT-Mitarbeiter punktuell umlernen. Da die Mitarbeiter mit der Einschränkung des Datentransfers durch eine DLP-Lösung vertraut sind, gestaltete sich die Einführung der neuen Lösung ebenfalls problemlos. Nach dem Rollout des Clients auf die Rechner konnte dank der in Endpoint Protector voreingestellten Richtlinien der Basisschutz für personenbezogene Daten und für die Verwendung von mobilen Geräten unverzüglich aktiviert werden. Scanner-Geräte, die im Rahmen der Digitalisierung im öffentlichen Bereich an den Arbeitsplätzen installiert wurden, werden via Custom Classes freigegeben.

„Die granularen Einstellmöglichkeiten von Endpoint Pprotector bringen uns spürbare zeitliche Entlastung", sagt Roberto Petrocelli, IT-Administrator der Gemeinde Weyhe. „Früher mussten die Mitarbeiter, die JPG-Dateien ins Netzwerk übertragen wollten, uns für jeden Vorgang kontaktieren und sich eine Art Active-Directory-naher Richtlinie anlegen lassen." Jetzt ist dauerhaft geregelt, dass sie ihre freigegebenen Geräte am Rechner verwenden und Bildmaterial hochladen können."

Die Protokollierung der Mitarbeiter-Aktivitäten hat für die Gemeinde höchste Bedeutung, da Verstöße gegen Richtlinien sowie Datenlecks oder potentielle Datenlecks frühzeitig sichtbar werden. „Einmal pro Woche sichten wir mit überschaubarem Zeitaufwand die Logs nach dem Vier-Augen-Prinzip und können gegebenenfalls unmittelbar aktiv werden und beispielsweise Richtlinien anpassen", sagt Ralf Eggers, IT-Leiter der Gemeinde Weyhe.

ENDPOINT PROTECTOR

	Endpoint Protector GmbH	CoSoSys Ltd.	CoSoSys USA
E-Mail	info@endpointprotector.de	sales@cososys.com	sales.us@cososys.com
Tel	+49 7541 978 26730	+40 264 593 110	+1-888-271-9349
Fax	+49 7541 978 26279	+40 264 593 113	