ENDPOINT PROTECTOR | by CoSoSys

NECKARGEMÜND www.neckargemuend.de

Die Stadt Neckargemünd nutzt Endpoint Protector über ein Leasingmodell

CASE STUDY | Stadt Neckargemünd

PROFIL

Branche

Kommunalverwaltung

Die Herausforderung

Vollständige Data Loss Prevention für eine kleinere Kommune finanziell attraktiv umsetzen

Die Lösung

Endpoint Protector

Warum Endpoint Protector?

Ausschlaggebend für die Entscheidung der Stadt Neckargemünd für Endpoint Protector war die Möglichkeit, Komplettschutz für sensible Daten schrittweise, angepasst an spezifische Anforderungen und Arbeitsweisen im Rahmen eines Leasingmodells umzusetzen.

www.**endpointprotector**.de

Über die Stadt Neckargemünd

Die Stadt Neckargemünd ist ein Unterzentrum in der Metropolregion Rhein-Neckar und eine beliebte Wohngemeinde am Rand des Ballungsgebietes Heidelberg-Mannheim. Als Urlaubsort profitiert Neckargemünd von der Nähe zu Heidelberg und der Lage an Neckar und Odenwald sowie zahlreichen Ausflugszielen in der Umgebung. Die Kommune bietet den 13.000 Einwohnern eine moderne städtische Infrastruktur mit zahlreichen sozialen Einrichtungen, einem breiten Spektrum an Schulen und Kinderbetreuungsmöglichkeiten sowie einem lebendigen Freizeit- und Kulturangebot.

Die Herausforderung

Der Umgang mit personenbezogenen Daten gehört zum Kerngeschäft von Verwaltungen. Im Rahmen der Umsetzung der DSGVO plante das Rathaus der Stadt, das Sicherheitsniveau zu verbessern. Eine Lösung für Data Loss Prevention, genauer gesagt Funktionalität für Gerätekontrolle, sollte auf den 70 Arbeitsplatzrechnern der Kommune die Verwendung mobiler Geräte regulieren und Schadcode-Eintrag und Datenverlust verhindern. Der IT-Leasing-Spezialist Econocom Deutschland, mit dem die Kommune für die regelmäßige Modernisierung der IT-Infrastruktur zusammenarbeitet, schlug vor, über die Gerätekontrolle hinaus mit USB-Verschlüsselung für notwendige Datentransporte auf Sticks und der Überwachung browserbasierter Schnittstellen für einen Komplettschutz der sensiblen Daten zu sorgen. Als Lösung empfahl er Endpoint Protector und bot eine Vorfinanzierung der Beschaffungskosten auf Grundlage einer Leasing-Vereinbarung an.

"Wir sind sehr zufrieden mit Endpoint Protector. Die Lösung lässt sich sehr einfach einrichten und verwalten, und infolge des Finanzierungsmodells können wir den Schutz, den wir als Kommune benötigen, nahtlos ausbauen."

Nico Walschburger,
IuK-Administrator,
Stadt Neckargemünd

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.

ENDPOINT PROTECTOR

Die Lösung

Nico Walschburger und Andreas Weitzell, die IuK-Experten der Stadtverwaltung Neckargemünd, unterzogen Endpoint Protector unter dem Aspekt umfassender DLP einer näheren Prüfung. Modularer Aufbau für eine schrittweise Einführung, einfache Bedienbarkeit, granulare Einstellmöglichkeiten und smarte Features fielen unmittelbar positiv auf – von der technischen Seite und dem Leistungsumfang her passte Endpoint Protector perfekt. Die Möglichkeit, die Beschaffungskosten über das Leasing-Modell mit mehrjähriger Laufzeit aufzubringen, überzeugte auch den Bürgermeister davon, den Komplettschutz anzugehen. Endpoint Protector wurde mit allen Modulen, Device Control, USB-Verschlüsselung, Content Aware Protection und eDiscovery, lizensiert.

Beim Austausch der Server wurde Endpoint Protector als virtuelle Appliance auf einem der neuen Rechner installiert. Walschburger und Weitzell machten sich mit der Management-Konsole und den Einstellmöglichkeiten vertraut; ein Techniker von Endpoint Protector unterstützte sie dabei, als ersten Schritt den Richtlinien-Satz für Device Control den Anforderungen der Kommune entsprechend zusammenzustellen. Er wurde zunächst auf ausgewählten PCs in verschiedenen Abteilungen getestet und nach der Feinabstimmung auf allen Rechnern ausgerollt.

Derzeit blockiert Device Control den Zugriff auf mobile Geräte an den Arbeitsplatzrechnern. Mobiltelefone können aufgeladen, aber nicht für Datenübertragungen genutzt werden. Mitarbeitende, die USB-Sticks verwenden müssen, erhalten von der IT-Administration einen registrierten und mit EasyLock verschlüsselten Stick für den sicheren Datentransport. Sind Ausnahmen von den strengen DC-Richtlinien erforderlich, informieren die Mitarbeitenden den-Administrator, der die Freischaltung konfiguriert. Dank der Finanzierung über das Leasing-Modell kann die Kommune in weiteren Schritten die Module CAP und eDiscovery für den Komplettschutz der personenbezogenen Daten einrichten.

	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	