EFFEKTIVE KONTROLLE VERTRAULICHER DATEN UND BEREITSTELLUNG VON INFORMATIONEN FÜR ALLE BENUTZER

Das Krankenhauszentrum Bourges, eines der fünf Gesundheitszentren der GHT18-Gruppe (regionale Krankenhausgruppe in Frankreich), hat sich für die automatisierte Benachrichtigungslösung NetSupport Notify und die von Query Informatique bereitgestellte Datensicherheitslösung DriveLock entschieden. Frank Moussé, CISO und DSB des GHT, nennt die Gründe.

Um die Risiken zu minimieren, die durch die Ausbreitung von Schadcode, aber auch durch den ungesicherten Transfer von vertraulichen persönlichen und gesundheitsbezogenen Daten auf USB-Sticks oder Wechseldatenträgern entstehen, empfiehlt unsere allgemeine Sicherheitsrichtlinie für Informationssysteme im Gesundheitswesen (PGSSIS) die Sperrung von USB-Schnittstellen in allen Einrichtungen.

Flexibilität bei der Sperrung von USB-Anschlüssen

Vor drei Jahren war es noch möglich, jeden beliebigen USB-Stick mit allen Computern im Krankenhauszentrum zu verbinden, was ein kritisches und gefährliches Risiko darstellte. „Zunächst haben wir zur Sicherung der Arbeitsplätze die USB-Schnittstellen vollständig mittels Gruppenrichtlinien-Objekten (GPO=Group Policy Objects) gesperrt. Dies war jedoch nicht geeignet, besonders wenn jemand schnellen Zugriff benötigte", erklärt Franck Moussé. Es musste eine Lösung gefunden werden, die Zeit spart und die Wartung erleichtert. „Vor einem Jahr haben wir uns für DriveLock von Query Informatique entschieden, da es gleich mehrere Vorteile bietet: Erstens konnten wir schnell einen Agenten auf allen Computern installieren, der exklusiv und auf Anfrage die vom Krankenhaus bereitgestellten USB-Sticks autorisiert." Jeder USB-Stick oder Wechseldatenträger wird verschlüsselt, und die Berechtigungen werden von einer Konsole aus verwaltet. „Generell wird ein USB-Stick nur dann auf einem Arbeitsplatz im Unternehmen zugelassen, wenn er in DriveLock autorisiert ist und mit DriveLock Encryption 2-Go oder BitLocker, der Verschlüsselungslösung von Microsoft, verschlüsselt ist." Zweitens ermöglicht DriveLock dem SIS, das Risiko von Viren, unkontrolliertem Datenverlust und Datenschutzverletzungen zu verringern, sollte ein USB-Stick oder eine externe Festplatte mit Gesundheitsdaten verloren gehen. Zudem erlaubt DriveLock das Entsperren von USB-Schnittstellen aus der Ferne (Remote), ohne dass eine Verbindung hergestellt werden muss. „Diese Funktion ist sehr hilfreich, da sie es einem Remote-Benutzer ermöglicht, von außerhalb der Einrichtung auf den Inhalt seines USB-Sticks zuzugreifen." Ein weiterer wichtiger Punkt, den der CISO betont hat, ist die Registrierung der USB-Sticks im System über die IMEI-Herstellernummer. Diese ermöglicht es dank Ausnahmen, einen USB-Port mit einem Dongle zu verwenden sowie, die auf den Sticks und den Medien ausgeführten Aktionen nachzuvollziehen.

Sofortige Verfügbarkeit von Informationen

Bevor NetSupport Notify eingeführt wurde, verschickte die IT-Abteilung Informations- und Warnmeldungen per E-Mail oder über andere indirekte Wege, was jedoch nicht sehr effektiv war. Ab sofort kann sie alle Benutzer oder Benutzergruppen dank der Active Directory-Kopplung mit einem Klick über ein Pop-up auf den Bildschirmen sofort und direkt informieren. So kann beispielsweise der Technische Support bei einer notwendigen Aktualisierung einer Anwendung mitteilen, dass diese zu einem bestimmten Zeitpunkt nicht erreichbar ist, und eine Benachrichtigung senden, sobald sie wieder verfügbar ist. Der Vorgang ist sehr einfach, zumal Notify vorformatierte Infotexte anbietet.

Ein weiterer Anwendungsfall für Notify betrifft Warnmeldungen: Die technisch Verantwortlichen stellten während einer Krisenstabsübung fest, dass sie Schwierigkeiten hatten, die Benutzer zu informieren. „Mit der neuen Notify-Konsole kann der Krisenstab nun vorformatierte Warnmeldungen an alle Arbeitsplätze senden und so jeden erreichen." Der Zugriff auf die Konsole wurde sogar auf den Sicherheits-PC ausgeweitet, der unter bestimmten Umständen die Abteilungen oder das gesamte Krankenhaus über einen unbefugten Zutritts oder das Risiko eines Anschlags informieren muss (Vigipirate, französischer Antiterrorplan). „Die Kommunikationsabteilung kann auch Infomeldungen zu verschiedensten Themen versenden, und ich selbst kann veranlassen, dass man die Geräte vom Netz trennt oder die Kabel abzieht, um ein Cybersicherheitsproblem zu lösen."

Laut Frank Moussé entsprechen diese beiden vollkommen unabhängigen Lösungen vollständig den aktuellen Anforderungen der GHT18. „Von den fünf Einrichtungen wartet nur eine auf die bevorstehende Umstellung auf die NetSupport Notify-Lösung." Insgesamt verlief die Bereitstellung über ein Gruppenrichtlinien-Objekt (GPO) oder über den SCCM (System Center Configuration Manager) sehr schnell und für den Benutzer völlig transparent. „Der Agent kommuniziert entweder mit der Notify-Konsole oder mit der DriveLock-Konsole." Angesichts zunehmender Risiken wird der CISO und Datenschutzbeauftragter des GHT möglicherweise neue Drivelock-Funktionen hinzufügen, z. B. das File Protection-Modul zum Schutz von Dateien.

Krankenhauszentrum Jacques Coeur in Bourges

Quelle: EXPERT CYBER SECURITY, Technologien und Innovationen im Krankenhaus | März 2024