DriveLock
securing your digital tomorrow

CASE STUDY
DriveLock Device Control in der Klinikumgebung

Patientendaten gehören zu den sensibelsten Daten überhaupt und müssen geschützt werden. Für große Krankenhäuser, sogenannte kritische Infrastrukturen, bilden DSGVO und IT-Sicherheitsgesetz die rechtliche Grundlage. Aber durch welche Maßnahmen gestaltet man diesen Schutz aus? Cyber-Angriffe werden immer trickreicher, gleichzeitig steigt die Zahl von Schadsoftware-Varianten. Die Case Study zeigt am Beispiel eines großen Krankenhauses, wie Sie mit DriveLock Lösungen Cybergefahren entgegenwirken und rechtssicher sind.

Die Landesschutzbeauftragen ermittelten bei einem Großkrankenhaus in Deutschland Verbesserungsbedarf bei der Einhaltung der **gesetzlichen Vorgaben** zu IT-Sicherheit und Datenschutz:

- Das **IT-Sicherheitsgesetz** verpflichtet Betreiber kritischer Infrastrukturen (KRITIS) zum Einsatz von Security Software.
- Die **DSGVO** beinhaltet strenge Datenschutzanforderungen mit Dokumentationspflichten, insbesondere auch im Hinblick auf Patientendaten.
- Bei Auftreten von datenschutzrelevanten Vorfällen (z. B. Datenabfluss) muss jederzeit transparent nachvollzogen und nachgewiesen werden können, wohin diese Daten abgeflossen sind und durch wen es veranlasst wurde.

Probleme & Schwachstellen

+ **MANGELNDE EINHALTUNG GESETZLICHER VORGABEN**
+ **FEHLEN VON ZENTRALEN RICHTLINIEN BEI DER NUTZUNG VON PCS UND DATENTRÄGERN**
+ **GEFAHR DES UNKONTROLLIERTEN ABFLUSSES VON DATEN BEIM EINSATZ VON USB-STICKS UND ANDEREN EXTERNEN SPEICHERMEDIEN**

DriveLock
securing your digital tomorrow

Ausgangssituation

Das Großkrankenhaus war aufgrund von Meldungen des BSI zunehmend für die Risiken von Cyber-Angriffen und Datenverlust sensibilisiert. Eine besondere Herausforderung war die historisch gewachsene Vielfalt von Benutzerberechtigungen bei der Nutzung von IT-Systemen und -Geräten. So verfügten beispielsweise einzelne Nutzer über lokale Administrationsrechte an PCs.

Die IT-Leitung verfolgte die Umsetzung zentraler Richtlinien zur Nutzung von PCs und Datenträgern. Diese Richtlinien sah das Klinikpersonal (u. a. Ärzte und Ärztinnen) zunächst kritisch, insbesondere vor dem Hintergrund, dass z. B. bei Geräten in der Intensivmedizin nach Aufspielen von Security Software ein Garantieverlust drohte.

Rahmenbedingungen im Gesundheitswesen

- **IT-SICHERHEITSGESETZ**
- **BRANCHENSPEZIFISCHE SICHERHEITS-STANDARDS B3S/KRITIS**
- **DSGVO**
- **PATIENTENRECHTEGESETZ**

Zielsetzung des Projektes

Es sollte eine Lösung zum Schutz und zur Nachvollziehbarkeit der Nutzung externer Medien gefunden werden, um den unkontrollierten Datenabfluss von Patientendaten zu verhindern.

Lösung: Schnittstellenkontrolle, Prozesse & IT-Sensibilisierung

Um die Ziele zu erreichen, wurde das Modul Schnittstellenkontrolle, DriveLock Device Control, bei ca. 15.000 Endgeräten eingeführt. Dieses umfasst die Mediennutzungskontrolle für externe Festplatten und USB Geräte. Zugleich wurde der Zugriff auf externe Medien an einen Genehmigungsprozess mit zentralen Richtlinien gekoppelt:
Die Genehmigung zur Nutzung externer Medien muss zunächst bei der Abteilungsleitung, z. B. Oberarzt oder Oberärztin, Chefarzt oder Chefärztin angefragt werden. Im 4-Augen-Prinzip genehmigt anschließend die IT-Abteilung, die daraufhin das Sicherheitsprofil für entsprechenden User modifiziert. Mit der Lösung verbunden sind IT-Sensibilisierungskampagnen mit dem DriveLock Security Education-Modul zur Schärfung des Sicherheitsbewusstseins.

DriveLock
securing your digital tomorrow

Device Control im Detail

DriveLock Device Control verhindert, dass sensible Daten auf externe Speichermedien gelangen oder externe Datenträger einfach angeschlossen und ausgelesen werden können. Die Lösungen kontrolliert externe Datenträger und Datenfluss. Jedes angeschlossene Gerät wird geprüft und ggfs. ausgesperrt. Schließt ein Mitarbeiter ein Gerät an den USB-Port an, so erkennt der Rechner, ob es sich um eine externe Festplatte, einen USB-Stick oder Ähnliches handelt. Via DriveLock lässt sich folglich regulieren, welche USB-Medien überhaupt zulässig sind. Eine andere Regel könnte vorsehen, dass das Anschließen von USB-Geräten zwar erlaubt ist – der Nutzer jedoch keinerlei Dateien auf das Gerät schreiben, sondern die Daten darauf nur lesen darf. DriveLock unterstützt neben der vollständigen Überprüfung der Nutzung externer Medien und die Protokollierung des Datenflusses die Erstellung von Schattenkopien. Die erzwungene Verschlüsselung von Daten, die auf externe Medien geschrieben werden, ist ebenfalls erhältlich.

Ausblick

Die Verschlüsselung von externen Medien wird derzeit nicht großflächig eingesetzt, im Rahmen einer konsequenten Sicherheitsstrategie sollte man dies überdenken. Die Einführung einer Applikationskontrolle gegen die Ausführung unbekannter Programme und dateiloser Malware steht aus. Erstellung von Schattenkopien. Die erzwungene Verschlüsselung von Daten, die auf externe Medien geschrieben werden, ist ebenfalls erhältlich.

DriveLock Device Control Features

- + NUR GEWÜNSCHTE GERÄTE UND EXTERNE LAUFWERKE WERDEN ZUGELASSEN.
- + PROAKTIVES UNTERBINDEN VON CD/DVD-BRENNERN
- + VERHINDERT DATEITRANSFER ÜBER UNVERSCHLÜSSELTE ODER NICHT ZUGELASSENE MEDIEN.
- + ERMÖGLICHT KONTROLLE, WER WELCHE DATEI AUF WELCHES MEDIUM KOPIERT HAT.
- + EINFACHE KONFIGURATION INTEGRIERTER GERÄTE DURCH MACHINE LEARNING
- + VERSCHLÜSSELT EXTERNE USB-DATENTRÄGER AUF WUNSCH.
- + SCHULT MITARBEITER IM SICHEREN UMGANG MIT DATEN UND EXTERNEN DATENTRÄGERN.
- + FORENSISCHE ANALYSE & REPORTING

DriveLock: Experte für IT- und Datensicherheit seit mehr als 20 Jahren

Das deutsche Unternehmen DriveLock SE wurde 1999 gegründet und ist inzwischen einer der international führenden Spezialisten für cloud-basierte Endpoint-und Datensicherheit. Die Lösungen umfassen Maßnahmen der Prävention wie auch zur Erkennung und Eindämmung von Angreifern im System.

DriveLock ist Made in Germany mit Entwicklung und technischem Support aus Deutschland.