Endpoint Data Protection

Sichere Endgeräte - Sichere Daten - Höhere Anwenderproduktivität

Herausforderung: Steigender Datendiebstahl und Datenverlust

Wissen Sie, welche Firmendaten Ihr Unternehmen über welche Endgeräte ungeschützt verlassen? Können Sie sicherstellen, dass nur berechtigte Personen vertrauliche Daten verwenden, kopieren und ablegen? Und können Sie proaktiv verhindern, dass wertvolle Daten das Unternehmen nicht verlassen oder fremdgenutzt werden? So wurden 7 von 10 Industrieunternehmen in den vergangenen zwei Jahren Opfer von Sabotage, Datendiebstahl oder Wirtschaftsspionage. Dadurch ist ein Schaden von 43,4 Milliarden Euro entstanden. Bei einem Drittel der Unternehmen (32 Prozent) wurden IT- oder Telekommunikationsgeräte gestohlen. Bei fast einem Viertel (23 Prozent) sind sensible digitale Daten abgeflossen. [1]

Was ist Matrix42 Endpoint Data Protection?

Matrix42 Endpoint Data Protection ist eine Komplettlösung aus Schnittstellenkontrolle, Datenverschlüsselung und verhaltensbasierter Automation von Abwehrmaßnahmen. Die Lösung schützt Ihre Daten auf dem Endgerät vor unberechtigten Zugriffen. Mit dem Monitoring-Tool Insight Analysis lassen sich Verhaltensanalyse durchführen. Auf Basis dieser können Anomalien schnell erkannt und Maßnahmen in Echtzeit eingeleitet werden. Außerdem können Applikationen und Geräte entsprechend der Unternehmensrichtlinien klassifiziert und die Ausführung bzw. Verwendung von nicht freigegebenen Anwendungen oder Geräten in Echtzeit blockiert werden.

Wussten Sie schon?

Endpoint Data Protection SaaS ist jetzt verfügbar. Mit der Cloudlösung profitieren Sie unter anderem von:

- minimalen Implementierungszeiten,
- mmer der neuesten Version der Anwendung
- maximaler Verfügbarkeit (Sie benötigen lediglich einen Internetzugang).

[1] Studie Wirtschaftsschutz in der Industrie, bitkom, (13.09.2018) https://www.bitkom.org/Presse/Presseinformation/Attacken-auf-deutsche-Industrie-verursachten-43-Milliarden-Euro-Schaden.html [03.07.2019]

Ihre Vorteile

Für IT Abteilungen

- Reduzierte Komplexität durch übersichtliche Anwendungs-und Gerätesteuerung.
- Transparente Übersicht über alle Datenbewegungen und möglicher Schwachstellen.
- Höherer Schutz der Daten, bei gleichzeitig weniger Arbeit, dank Automation.
- Einfache Installation und Konfiguration der Software in kurzer Zeit.
- Schnelle Umsetzung von Datenschutzrichtlinien z.B. Datenspeicherung in der Cloud.
- Kein zusätzlicher Aufwand für das Support-Team.

Für Endanwender

- Anwender müssen sich nicht umgewöhnen.
- Keine Benutzerschulungen erforderlich.
- Automatische Ver- und Entschlüsselung von Dateien auf allen Geräten ohne, dass der Endanwender eingreifen muss.

Für Unternehmen

- Einfache Integration in die bestehende IT-Infrastruktur und geringe Hardwareanforderungen.
- Erfüllung der EU-DSGVO-Vorgaben (Artikel 25, 30, 32, 33, 34).
- Berücksichtigung der Mindeststandards des BSI.
- Datenzugriff nur durch berechtigte Personen.
- Weitergabe und Speicherung von Daten nur auf vordefinierte Weise.
- Zuverlässiger Support mit hervorragender SLA Erfüllung.
- Betriebsrats- und datenschutzkonforme Verhaltensanalyse und Auditierung.

3 Gründe für Endpoint Data Protection

1

Rundumschutz Ihrer Endpunkte.
Haben Sie alle notwendigen Abwehrtools zum Schutz Ihrer Endgeräte zur Hand. Daten werden automatisch gegen unbefugte Benutzer verschlüsselt. Unsichere Zugriffe und Anwendungen werden automatisch blockiert. Durch transparente Einblicke in alle Datenströme innerhalb Ihres Unternehmens können Sie Anomalien und Schwachstellen erkennen und verhaltensbasierte Gegenmaßnahmen einleiten.

2

Sicherheit ohne Beeinträchtigung.
Schützt Ihr Unternehmen ohne Ihre Arbeitsweise zu verändern.
Die Arbeitsabläufe der Benutzer werden nicht unterbrochen und Ihr IT-Team wird nicht mit zusätzlichen Schulungen belastet. Das kommt bei den Nutzern gut an und entlastet Ihre Support- und IT-Teams von zusätzlichen Aufgaben. Alles läuft wie bisher, aber auf einem höheren Sicherheitsniveau.

3

Transparente IT-Sicherheit.
Secure Audit ermöglicht eine detaillierte Sichtbarkeit des Datenflusses und zeigt mögliche Schwachstellen in den Schutzeinstellungen auf. IntellAct wertet die von Insight Analysis gesammelten Fakten aus und kann automatisch geeignete Schutzmaßnahmen auslösen.