baramundi

BARAMUNDI CHECKLISTEN liefern praxisorientierte Step-by-Step Anleitungen für komplexe Fragen und Probleme – kompakt und unkompliziert. Mehr davon finden Sie hier: **www.baramundi.com/checklisten**

Bitlocker-Verschlüsselung in 7 Schritten einführen und konfigurieren

Der Bitlocker ist eine proprietäre Festplattenverschlüsselung von Microsoft und ein unverzichtbarer Schutz für Business-Endgeräte, um sensible Unternehmensdaten zu sichern. Diese Checkliste erklärt Ihnen in 7 Schritten, wie Sie den Bitlocker sinnvoll einführen und passgenau für Ihre Anforderungen konfigurieren.

Hardware prüfen und Richtlinien festlegen

Überprüfen Sie, ob die Hardware der Endgeräte die erforderlichen Bitlocker-Anforderungen erfüllt. Definieren Sie klare Richtlinien für die Bitlocker-Nutzung im Unternehmen, welche Geräte verschlüsselt werden müssen (z.B. Notebooks).

Schrittweise Einführung und Testläufe

Als nächstes erfolgt ein Aktionsplan für die schrittweise Einführung und Testläufe auf einzelnen Geräten. Erst wenn sichergestellt ist, dass die Nutzer zuverlässig auf ihre Geräte zugreifen können und keine Inkompatibilitäten vorliegen, führen Sie den Bitlocker auf allen relevanten Geräten ein.

Zentrale Aktivierung bei OS-Installation

Am besten implementieren Sie, dass die Festplattenverschlüsselung bereits während der Betriebssysteminstallation zentral aktiviert wird. Das spart Zeit bei der Verschlüsselung und erleichtert eine flächendeckende Umsetzung.

Hindernisse bei Softwareverteilung

Bedenken Sie, dass der Bitlocker eventuell die Verteilung bestimmter Spezial-Software (z.B. Virtualisierungslösungen) hemmt. Bei Bedarf müssen Sie den Bitlocker-Schutz pausieren können.

Network-Unlock implementieren

Aktivieren Sie die Network-Unlock-Funktion. Dann bootet das System automatisch ohne Bitlocker-Pin-Abfrage, sobald es sich in dem eigenen und sicheren Unternehmensnetzwerk befindet. Ein echter Mehrwert für die User-Zufriedenheit.

Wiederherstellungsschlüssel

Gewährleisten Sie einen zentralen, sicheren, für das zuständige IT-Team leicht zugänglichen Speicherort für Bitlocker-Wiederherstellungsschlüssel, um den Mitarbeitern bei vergessenen Passwörtern oder Hardwareänderungen schnell wieder Zugang zu gewähren.

Schulungen der Belegschaft

Informieren Sie alle End User über die Bitlocker-Einführung und ihre Vorteile. Sie müssen sich außerdem eventuell darauf einstellen, dass sich Anmeldevorgänge ändern. Richten Sie einen Support-Mechanismus ein, um Benutzern bei Problemen oder Fragen zum Bitlocker zu helfen.

Kurz gesagt: Die erfolgreiche Einführung und Aktivierung von Bitlocker trägt maßgeblich zur Sicherheit der Unternehmensdaten bei. Die obenstehende Checkliste sowie das baramundi-Modul Defense Control unterstützen Sie dabei, den Prozess effizient und effektiv durchzuführen.