Microsoft BitLocker-Laufwerksverschlüsselung

Sehr geehrter Geschäftspartner,

aktuelle Ereignisse diverser Datenschutzverstöße führen dazu, dass immer mehr Unternehmer fürchten, Opfer von Datendiebstählen zu werden.
Der Verlust oder gar die unzulässige Veröffentlichung von Unternehmensdaten haben große finanzielle Schäden zur Folge.

Mehr Datensicherheit durch Microsoft BitLocker-Laufwerksverschlüsselung!

Der **BitLocker** ist ein boardeigenes Sicherheitstool von Microsoft mit dem Systemlaufwerke, Festplatten und Wechsellaufwerke sowohl vor Diebstahl als auch vor Offenlegung von Daten geschützt werden können.
Nur wenn Ihre Festplatte komplett verschlüsselt ist, besteht mehr Sicherheit, dass Ihre Daten geschützt sind – auch wenn die Festplatte physisch entfernt und in anderen Systemen ausgelesen wird. Der **Microsoft BitLocker** sorgt dafür, dass nur Daten gelesen und geschrieben werden können, nachdem das erforderliche Kennwort eingegeben wird bzw. die entsprechenden Schlüssel System passen.
Die Verschlüsselung erfolgt durch AES mit einer Schlüssellänge von Standard 128 bzw. 256 Bit.

Welche Voraussetzungen müssen für die BitLocker-Laufwerksverschlüsselung erfüllt sein?

1.) Erforderliches Betriebssystem

Einzusetzen ist der **Microsoft BitLocker** nicht auf allen Betriebssystemen, sondern nur auf:
- Windows Vista
- Windows 7 Enterprise und Ultimate
- Windows 8 Pro
- Windows Server 2008 R2

2.) Datenpartition

Für das Verschlüsseln einer Datenpartition, eines USB-Laufwerks oder einer beliebigen Partition, die nicht das Betriebssystem enthält, gibt es keinerlei Einschränkungen. Die Nutzung eines bestimmten Dateisystems für das Laufwerk ist nicht notwendig.
Microsoft BitLocker verschlüsselt: NTFS, FAT32, FAT16 oder exFAT.

3.) **Systempartition**

Für den **Microsoft BitLocker**-Einsatz auf der Systempartition ist ein TPM-Chip (TPM = Trusted Platform Module) der Version 1.2 oder höher notwendig.
Fehlt dem entsprechenden Rechner der Hardware-Chip, lässst sich über die Gruppenrichtlinie erzwingen (gpedit.msc, Computerkonfiguration, Administrative Vorlagen, Windows-Komponenten, BitLocker-Laufwerksverschlüsselung, Operating System Drives, Require aditional athentication at startup), dass der **BitLocker** den Schlüssel statt auf das TPM auf einen USB-Stick speichert.

Der Microsoft BitLocker im Einsatz

Im laufenden Betrieb ist die transparente **BitLocker**-Laufwerksverschlüsselung, weder bei der Nutzung von Daten noch bei der Systemleistung, zu bemerken.
Lediglich der einmalige Vorgang der Verschlüsselung ist, je nach Größe der Partition, zeitaufwendig.

Bei Verlust des Kennworts oder des, mit dem Kennwort gespeicherten USB-Sticks, ist kein Zugriff auf die Daten mehr möglich. **BitLocker** bietet aber die Option, den Wiederherstellungsschlüssel, für verschlüsselte Laufwerke, in eine Datei zu speichern oder zu drucken. **Datei oder Ausdruck sollten in jedem Fall sicher verwahrt werden!**
Mit Hilfe der 48-stelligen Ziffernfolge kann auf das **BitLocker-**Laufwerk wieder zugegriffen werden.

Aktuell können wir Ihnen folgenden Preis anbieten:

Microsoft Windows 8.1 - OEM/SB 64-bit Deutsch
mit Software Assurance

EUR 195,-

Der Preis gilt zzgl. MwSt. und Frachtkosten.

Der Aufwand für die Einrichtung der Microsoft **BitLocker**-Laufwerksverschlüsselung beträgt pro Gerät (PC oder Notebook) ca. 2 Stunden.

Bei Fragen steht Ihnen das Team der TSO-DATA gerne zur Verfügung!