

# Recherche im IT-Grundschutzkompendium

## Aufgabenstellung

Ich wurde in den letzten Wochen beauftragt, veraltete Softwareversion auf den Clients der Benutzer zu aktualisieren. Dafür nutze ich das «Microsoft Defender Portal» welches mir alle Informationen über die veraltete Software liefert.

## Informationen aus dem IT-Grundschutzkompendium

[DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle](#)

### Bedrohungen

Unvollständige Bereinigung: Nicht aktualisierte Software können weiterhin als Angriffsziel genutzt werden.

Datenverlust: Bei veralteter Software gibt es die Gefahr, dass es zu einem Datenverlust auf dem System kommen kann.

### Checkliste / Basisanforderungen

Leitungsgremium einrichten. Ein Team, welches die Massnahmen und Aufgaben plant und koordiniert.

Bereinigungsstrategie festlegen. Eine Strategie, wie mit welchen Fällen umgegangen werden soll. Diese Strategie wird vom Leitungsgremium genutzt.

Isolierung des betroffenen Netzabschnitt.

Zugangsdaten ändern/sperren.