Patch-Management im Unternehmensalltag

Patch-Management und insbesondere Sicherheitsupdates sind entscheidend, um Sicherheitslücken in Software und Betriebssystemen zu schließen, da Sicherheitslücken unter anderem von Cyberkriminellen ausgenutzt werden könnten. Regelmäßige Updates beheben Schwachstellen, verbessern die Leistung und sorgen für Systemstabilität, wodurch das Risiko von Datenverlust, Diebstahl und Ausfallzeiten minimiert wird. Sie sind ein wesentlicher Bestandteil der IT-Sicherheitsstrategie und unterstützen die Einhaltung gesetzlicher und regulatorischer Anforderungen.

Vorbereitung

Zunächst sollte eine **vollständige und aktuelle Übersicht** erstellt werden, in der alle PCs, Notebooks, internen und externen Server, Cloud-basierte Systeme, Smartphones, Tablets und sonstige Endgeräte (im Idealfall samt Betriebssystem und Betriebssystemversion) aufgelistet sind, die im Unternehmen im Einsatz sind.

Um Schwachstellen oder Bedrohungen frühzeitig zu identifizieren, ist es dringend zu empfehlen, entsprechende **Informationsquellen** (z.B. Newsletter oder Webseiten seitens des Herstellers oder von Sicherheitsbehörden) regelmäßig nach relevanten Patches zu prüfen.

Rahmenbedingungen

- **Automatisierung**: Wo immer möglich, sollten Tools zur Automatisierung des Patch-Managements eingesetzt werden, um Effizienz und Konsistenz zu verbessern. Automatisierte Prozesse müssen zudem immer überwacht werden.
- **Richtlinien**: Wenn eine automatisierte Durchführung nicht möglich ist, sollten klare Vorgaben (z.B. durch Richtlinien) gemacht werden, dass die Systeme eigenständig auf dem aktuellen Stand gehalten werden.
- **Verantwortlichkeiten**: Die Verantwortung zur Durchführung und Implementierung der einzelnen Patches sollte klar geregelt und kommuniziert sein.
- **Sensibilisierung**: Das IT-Personal und die Endnutzer sollten über die Bedeutung von Patch-Management regelmäßig geschult und sensibilisiert werden.
- **Priorisierung**: Patches sollten basierend auf der Schwere der Sicherheitslücke und der Relevanz für die Organisation bewertet und priorisiert werden.
- **Zeitrahmen**: Sicherheitsrelevante Patches sollten innerhalb von 72 Stunden eingespielt werden, nicht sicherheitsrelevante Patches innerhalb von 2 Wochen.
- **Kommunikation**: Bevorstehende Patches und begleitende Auswirkungen sollten allen Betroffenen frühzeitig und transparent kommuniziert werden.
- **Dokumentation**: Alle Patch-Management-Aktivitäten sollten zu Auditzwecken und zur Verbesserung der zukünftigen Planung dokumentiert werden.