



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

Immer auf Stand – 5 Kniffe für effizientes Update Management

Ungepatchte Schwachstellen sind nach Phishing die häufigste Methode, über die IT-Systeme kompromittiert werden. Auch wenn die Zahl der Schwachstellen täglich zunimmt, kann man dieses Problem mit den richtigen Werkzeugen und 5 einfachen Kniffen leicht lösen.

✓ Kritische Hard- und Software identifizieren

Bevor es los geht, müssen ein paar Fragen geklärt werden: Welche Endgeräte sind besonders kritisch für den gesamten Betrieb und welche Softwareanwendungen sind besonders gefährdet/wichtig. Dementsprechend müssen Prioritäten beim Patchen gesetzt werden.

✓ Updates testen

Tragischerweise können auch Updates Fehler enthalten. Daher sollten sie erst auf einigen Geräten getestet werden. Wenn sichergestellt ist, dass die Updates nicht zu größeren Problemen führen als sie lösen, dürfen die Updates großflächig ausgerollt werden.

✓ Ring-Konzept umsetzen

Nicht alle Endpoints können und sollen zur selben Zeit mit denselben Updates versorgt werden. Geräte, welche ein Update zur selben Zeit erhalten, sollten in einem sog. Ring zusammengefasst werden. Die Ringe mit den wichtigsten Endgeräten erhalten dann als erstes das Update.

✓ Security Automation

Händische Verteilung von Updates ist nicht nur zeitaufwendig, sondern auch sehr fehleranfällig. Besser ist es sie per Endgeräte Management zu automatisieren und so zeitnahe, einwandfreie Installationen sicherzustellen. In diesem Zuge kann auch gleich das Auffinden der Schwachstellen an die Software delegiert werden. Ebenfalls helfen vorkapertierte Software-Updates, den Arbeitsaufwand zu reduzieren.

✓ Risikomanagement

Vorsicht: Nicht immer ist ein Softwareupdate möglich oder wünschenswert. Von defekten oder inkompatiblen Updates einmal abgesehen, gibt es Legacy-Systeme, die nicht oder nur schwer verändert werden können. Hier muss eine Abwägung stattfinden und ggf. das entsprechende Gerät vom Netz getrennt oder durch externe Schutzmaßnahmen gegen Angriffe gesichert werden

Kurz gesagt: Effizientes Update Management ist entscheidend, um ungepatchte Schwachstellen zu vermeiden. Identifikation kritischer Systeme, Testen von Updates, das Ring-Konzept, Security Automation und abgewogenes Risikomanagement sind zentrale Strategien, die durch die **baramundi Management Suite verlässlich umgesetzt werden können.**

ALLE ENDPOINTS IM GRIFF

Mithilfe der baramundi Management Suite verwalten Sie über LAN oder Internet beliebig viele Geräte – egal, wo Sie sich befinden. Erfahren Sie mehr zu Unified Endpoint Management mit baramundi unter www.baramundi.com.