Virtuelles Patchen

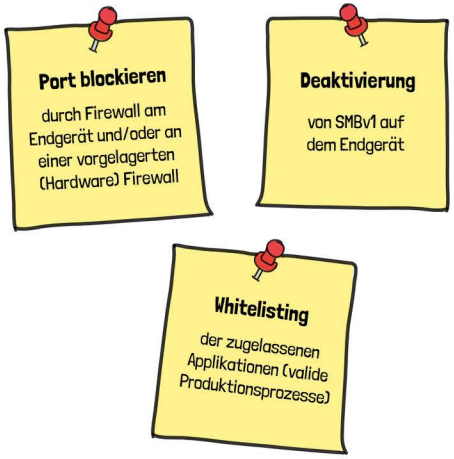
Bei einem **virtuellen Patch** wird nicht die eigentlich fehlerhafte Anwendung repariert, sondern ein Sicherheitsmechanismus etabliert, welcher die Ausnutzung einer Verwundbarkeit verhindern soll.

Im Gegensatz dazu werden mit **„klassischen" Patches** Fehler in Programmen korrigiert oder Sicherheitslücken geschlossen.

Kurz gesagt: **Ein virtueller Patch behebt nicht die eigentliche Ursache, sondern nur die Symptome.**

Umsetzung

anhand des Beispiels: „WannaCry"-Ransomware auf Windows (XP) Systemen in der Produktion durch Blockierung des SMBv1 Traffics



Vor- und Nachteile

des virtuellen Patchens

Vorteile

- **Geschwindigkeit**
  Sofortige Reaktion auf Sicherheitslücken möglich
- **Ungehinderter Rollout**
  Installation erfolgt meist ohne Störung des laufenden Arbeitsbetriebs z.B. System-Neustart

Nachteile

- **Kein nachhaltiger Schutz der Systeme**
  Lediglich als Übergangsmaßnahme sinnvoll
- **Einschränkungen im Funktionsumfang**
  Gegebenenfalls Zugriffssperrung auf Funktionen oder Endpunkte notwendig

Virtuelles vs. klassisches Patchen?

Sowohl klassische als auch virtuelle Patches stellen effektive Security-Maßnahmen dar, welche in ihrem jeweiligen Anwendungsfall genutzt werden können.

Grundsätzlich gilt:

Ein virtueller Patch ist kein Ersatz für die eigentliche Behebung der Lücken über klassische Patches.

Wählen Sie Ihren Patch-Typ mit Bedacht und ziehen Sie eine Beratung durch Experten in Betracht!