Leibniz Universität IT Services

Leibniz Universität Hannover

Virenschutz an der LUH: Bitdefender

LUIS-Sicherheitstage 27.02. & 28.02.2024

Inhalt

- Bitdefender
  - Setup & Lizenz
  - Aktualisierung im/außerhalb des LUH-Netzes
  - Fehler & Lösungen
  - Deinstallation
  - Umgang mit False Positives
  - HTTP-Login blockiert

Bitdefender – Setup & Lizenz

- Setup
  - **Lokal** scannender Security Agent auf Endgeräten
  - Zentrales **Reporting** im LUIS
  - **Aktualisierungen** über Update-Server
  - **Unterstützung** für Windows, macOS und Linux
  - Unterscheidung **Client/Server-Installer** bei Windows/Linux
  - Automatische Installation bei LUIS-**OPSI**-Geräten

- Lizenz**umfang**
  - Für Beschäftigte & universitätseigene Rechner
  - **Nicht** für Studierende und Privatgeräte
    - Stattdessen Empfehlung von **Windows Defender**

Aktualisierung im/außerhalb des LUH-Netzes

- **Innerhalb** des LUH-Netzes
  - Updates über LUIS-**Update**-Server
  - Ereignis-Übertragung zum LUIS-**Management**-Server

- **Außerhalb** des LUH-Netzes
  - Öffentlicher Bitdefender-**Update**-Server
  - Aber: LUIS-**Management**-Server nicht erreichbar
    - keine Lizenz-Updates & Richtlinien-Aktualisierungen
    - Keine Ereignis-Übertragung & Hilfestellung möglich
    - Mögliche dadurch entstehende Fehler:
      - „Lizenzen nicht mehr gültig“
      - „Kommunikation mit Verwaltungskonsole nicht möglich“

Fehler & Lösungen

- Fehler: “-2011“ nach Update des Clients
- **Lösung**: Update neu ausführen

- Fehler: “Verbindung zu Cloud Services fehlgeschlagen“
- Ursache: Client nicht abschließend konfiguriert oder nicht im LUH-Netz
- **Lösung**: Ins LUH-Netz gehen oder Neu-Installation über Support

- Bei anderen Fehlern:
  - LUIS-Support kontaktieren
  - Probleme können ggf. durch ein **„Neu-Konfigurieren“** der Installation behoben werden (dies muss zentral ausgelöst werden)

Bitdefender – Deinstallation

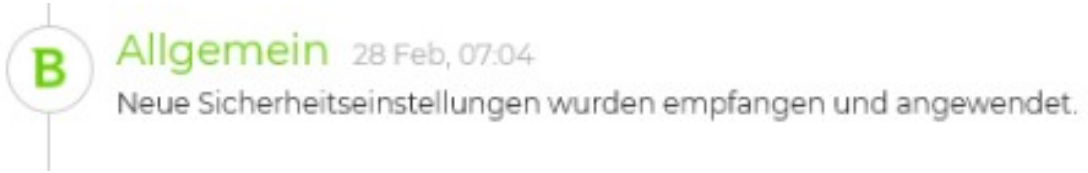
- Deinstallation am Client durch User nicht möglich
- Stattdessen: Zentrale Deinstallation durch LUIS-Sicherheitsteam über **LUIS-Support-Ticket**

- Benötigte Daten:
  - IP + Hostname
  - Begründung für Deinstallation
  - „OK“ per signierter Mail vom zuständigen IT-Beauftragten

- Deinstallations-Aufgabe wird nach Prüfung zentral erstellt
- Deinstallation wird ausgeführt, sobald der Bitdefender-Client den Server kontaktiert (**1x/h** oder nach **Neustart**) und die Aufgabe abholt (gleiches Prinzip bei Richtlinien-Änderungen)

Umgang mit False Positives I

- **False-Positives**
  - können auftreten
  - Melden per **Mail an LUIS-Support**
    - Identifizierung des Endgeräts (IP, Hostname)
    - „OK“ per signierter Mail vom zust. IT-Beauftragten
    - Nach erfolgreicher Prüfung: Erweiterung der **Allowlist**
  - Selbstständiges (Client-seitige) Freischalten nicht möglich



→ Immer eine Einzelentscheidung

Umgang mit False Positives II

- Mögliche Basis für Freischaltungen:
  - (File-/Zertifikat-) **Hash** → bevorzugt
  - Datei-/Ordnerpfad → selten sinnvoll
  - IP-Adresse → selten sinnvoll
  - Befehlszeile (mit regex) → manchmal hilfreich
  - Prozess → manchmal hilfreich

- Richtlinienänderungen betreffen i.d.R. auch andere Installationen
- Jede Einzelfreischaltung pro Gerät erhöht den Verwaltungsaufwand

- Herausforderung bei **Entwicklungsumgebungen**. Abwägung:
  - Ausschalten von Modulen (Unklare Auswirkungen auf Endpunktschutz)
  - Wechsel auf Windows Defender (Verlust der Vorteile der zentr. AV-Instanz)

    → Am besten: Auslagerung auf Extra-(Build-)System oder VM/System

HTTP-Login blockiert

- Bitdefender blockiert die Eingabe/Übermittlung von Login-Daten über ungesicherte HTTP-Verbindungen
- Beispiel (fiktiv):
  - http://130.75.2.228/login?username=admin&password=topsecret
- Lösung: Auf Serverzertifikate / HTTPS umstellen

Zusammenfassung

- Lizenz für Beschäftigte und universitätseigene Rechner

- Updates inner- und außerhalb des LUH-Netzes
- Management-Server nur aus LUH-Netz erreichbar
- Deinstallation nur über LUIS
- Fehler bei LUIS-Support melden

- Umgang mit False Positives
  - Einzelentscheidung
  - Herausforderung bei Spezialfällen

Fragen?

- Doku / Anleitungen unter https://go.lu-h.de/antivirensoftware