Neue Antivirenlösung

Wechsel von Sophos Central zu Cisco Secure Endpoint

IT Center | RWTH AACHEN UNIVERSITY

Agenda

- aktueller Stand
- Weiterer organisatorischer Ablauf
- Technische Umstellung bestehender Systeme
- Praktische Hinweise zum Betrieb
- Demo

Bisherige Antivirenlösung

- NRW Vertrag Sophos
  - Nutzung von Sophos Central (Cloud-Lösung)
  - Nutzung über NRW Landeslizenz
  - Bisher vollständige Förderung über NRW
  - Vertragsende 13.September 2024 => verlängert bis 13.12.2024 (Eigenkosten RWTH)

- Ausschreibung
  - Weitere NRW Lösung angestrebt
  - Herstelleroffene Ausschreibung durch Universität Bochum
  - Teilfinanzierung durch MKW

- Neuer Vertrag
  - Zuschlag an Cisco mit dem Produkt Cisco Secure Endpoint
  - Lizenzumfang: Cisco Secure Endpoint Essentials
  - Vertragslaufzeit 01.10.2024 – 30.09.2029

Umsetzung Cisco Secure Endpoint

- Zeitliche Verzögerung
  - Verzögerungen im Beschaffungsprozess und bei der Bereitstellung
  - Verlängerung der Sophos Lizenzen der RWTH bis zum 13.12.2024
  - Bereitstellung der RWTH Instanz zum 30.09.24
  - Überarbeitetes DPA erst zum 07.10.2024 verfügbar

- Änderungen
  - keine Lizenz für Studierende und Privatgeräte von Mitarbeitenden in der NRW Lizenz enthalten
  - Support-Tickets müssen zentral über das IT Center eröffnet werden

- Technische Realisierung ähnlich zu Sophos Central
  - RWTH hat als Organisation eine Cloud-Instanz, die zentral vom IT Center organisiert wird
  - Alle Einrichtungen, die das Produkt nutzen möchten, bekommen eine eigene Unter-Instanz

- Cisco Secure Client
  - bereits bekannt durch den VPN-Client
  - Cisco Secure Endpoint integriert sich als Plugin
  - Installation VPN/Secure Endpoint erfolgt unabhängig

Aktueller Stand

- Datenschutz
  - DPA von der RWTH geprüft und unterschrieben
  - TOM, Nutzungsbedingungen, VVT, Datenschutzhinweise erstellt
  - Stellungnahme DSB erfolgt
  - Mitbestimmungsprozess angestoßen

- Dokumentation
  - ab sofort auf *https://help.itc.rwth-aachen.de* *-> IT-Basis-Infrastruktur -> IT-Sicherheit -> Antivirenschutz RWTH* verfügbar

- Technisch können Instanzen können bereitgestellt werden

Weiterer organisatorischer Ablauf

- Bereitstellung der Unter-Instanzen kann erst nach Mitbestimmung erfolgen
  - Bitte senden Sie uns bei Interesse eine E-Mail an servicedesk@itc.rwth-aachen.de mit folgenden Angaben
    - OrgID der Einrichtung(en)
    - Bei mehreren: 1 Tenant für alle, oder einzeln

- Umstellung aller Geräte bis 13.12.24 notwendig, ab dann gilt:

  - vorhandene Endpoints werden nicht mehr aktualisiert
  - neue Endpoints können nicht mehr geschützt werden
  - es können keine Richtlinien mehr aktualisiert werden
  - Zugriff zu Sophos Central ist maximal für weitere 30 Tage möglich (Manipulationsschutz!!)

Technische Umstellung bestehender Systeme

- Vorbereitung von Cisco Secure Endpoint
  - Prüfen und ggf. Anpassung der vorhandenen Gruppenstruktur und Richtlinien
  - Einpflegen von Exceptions
  - Generieren der Installer

- Notwendige Schritte:

1. Sophos Manipulationsschutz deaktivieren
   - geht pro Gerät oder global
   - es kann ein paar Minuten dauern, bis die Änderung den Client erreicht

2. Sophos deinstallieren
   - benötigt Reboot

3. Cisco Secure Client installieren
   - benötigt Reboot

allgemeine Hinweise (1)

- Default Gruppen und Richtlinien

Name	Zweck
Audit	„nur“ Überwachung, keine Aktionen
Protect	Settings für Standardclients
Server	Settings für allgemeine Serversysteme
Domain Controller	optimiert für Domain Controller
Triage	„schärfere“ Policy für verdächtige Systeme
Default Network	Netzwerkkomponenten, wird nicht benötigt

- Neue Richtlinien
  - Können blank erzeugt werden, oder per „Duplicate“
  - bei neuen Windows Richtlinien ist die Benutzerbenachrichtigung deaktiviert!

allgemeine Hinweise (2)

- Produktupdates
  - Passieren **nicht** automatisch!
  - Steuerung der eingesetzten Version entweder per Richtlinie oder per Installer
  - Benachrichtigung bei neuer Version möglich (*Account Settings -> Announcement Preferences*)
  - Reboots sollten nicht notwendig sein, ggf. wird bei Einstellung der Richtlinie gewarnt

- Systeme ohne Internetanbindung
  - Verwendung eines HTTP Proxies möglich per Richtlinienkonfiguration
  - IT Center bietet zentrales System an: *cseproxy.itc.rwth-aachen.de*
    - Nur innerhalb des RWTH-Netzes erreichbar
    - leitet ausschließlich Requests an Cisco Cloud weiter
  - Bitte nur für diese Kategorie von Systemen verwenden

allgemeine Hinweise (3)

- IPv6 Unterstützung
  - Keine Unterstützung für IPv6-Only Systeme
  - Network Block & Allow Lists unterstützen nur IPv4 Adressen
  - Network Isolation funktioniert aber zuverlässig
- „fremde“ Nutzer / API-Keys im Tenant
  - API-Key *ITC_Mgmt_DO_NOT_DELETE* bitte nicht löschen!
  - IT Center Adminaccounts werden automatisch angelegt bei Generierung des Tenants, oder später bei Zugriff auf den Tenant durch das ITC bspw. zu Supportzwecken
  - ITC-Benutzeraccounts können gefahrlos gelöscht werden
- File Analysis
  - Feature zum (händischen) Upload von Dateien zur automatisierten Analyse in einer virtuellen Umgebung
  - Hochgeladene Dateien können nicht händisch gelöscht werden!
  - bis zu 24 Monate sicht- und wieder herunterladbar
  - Upload nur nach Zustimmung des betroffenen, bestimmte Kategorien **nicht** zulässig

    ➡ Beachten Sie die **Nutzungsbedingungen** im IT Center Help!

Fragen

Vielen Dank
für Ihre Aufmerksamkeit