Empfehlung zum Einsatz von Sophos Antivirus an der WWU

IV-Sicherheitsteam, Oktober 2017

https://www.uni-muenster.de/IV-Sicherheit

Einleitung

Der Betrieb des Sophos Antivirus Produktes wird innerhalb der WWU nicht einheitlich umgesetzt. Teilweise wird eine Sophos Enterprise Console (SEC) eingesetzt, teilweise werden die Installationspakete des ZIV ohne SEC mit Standardeinstellungen genutzt. Die Lizenz von Sophos beinhaltet verschiedene Komponenten des Sophos Antivirus Produkts. Diese können alle einzeln aktiviert bzw. deaktiviert, sowie konfiguriert werden. Die Konfigurationsvielfalt führt zum Teil zu Unsicherheit bei den Administratoren der SEC und oft auch zu einem bzgl. Datenschutz problematischen oder IT-Sicherheit nicht optimalen Einsatz von Sophos Antivirus.

In den meisten Unternehmen wird eine zentrale Sophos Enterprise Console mit Basisrichtlinien betrieben und den Organisationseinheiten (IVVen, Fachbereichen) jew. Zugriff und Konfigurationsmöglichkeiten für ihre Bereiche eingerichtet, um eigene Ausnahmen zu pflegen oder Auswertungen durchzuführen. Bei einer Verlängerung des Sophos-Lizenzvertrages sollte die Organisation des Sophos-Einsatzes an der WWU in diese Richtung überdacht werden. Der aktuelle Lizenzvertrag läuft noch bis 30.06.2019.

Im Folgenden wird eine Übersicht der Komponenten und eine Konfigurationsempfehlung gegeben.

- **AntiVirus und HIPS**
  - Klassische Viruserkennung mittels Signaturen
  - Erkennen von schädlichen Webseiten (Web-Schutz)
  - Erkennung mit Live-Protection (Übermitteln von Hashes an Sophos)
  - Erkennen von schädlichem Verhalten
- **Exploit-Abwehr**
  - Neue Komponente durch ein Lizenz-Upgrade. Wird nicht automatisch auf Endpoints aktiviert.
  - Kann Ransomware und unbekannte Schadsoftware, die bekannte Exploits verwendet erkennen
- Application Control
  - Zur Ausführungsverhinderung von Software
- Web Control
  - Ermöglicht Einschränkungen des Webzugriffs anhand von Kategorien, z.B. zum Jugendschutz
- Data Control
  - Ermöglicht Regeln auf Basis von Mustern (z.B. IBAN, Kreditkartennummer), um Datenabfluss zu verhindern oder das Kopieren von Dokumenten auf Datenträger zu verhindern.
- Device Control
  - Ermöglicht Zugriff auf Wechseldatenträger oder andere Schnittstellen (WLAN, Bluetooth) zu verhindern
- Patch Analyse
  - Zur Information bei fehlenden Sicherheitspatches (Windows und viele Third Party Produkte)
- Firewall

Empfehlung

Für einen **optimalen Schutz** sollten die folgenden Komponenten *aktiviert* werden.

- AntiVirus und HIPS sowie Exploit-Abwehr
  - Verhaltensüberwachung
  - Web-Schutz
    - Zum Schutz vor dem Aufruf schädlicher Webseiten oder dem Download von Schadsoftware
  - Live Protection ("Cloud Scan")
    - Überprüfung der Hashes von verdächtigen Dateien oder URLs durch Rückfrage bei Sophos

Aus **Datenschutzgründen** sollten die folgenden Komponenten bzw. Einstellungen *deaktiviert* werden.

- On Access Scan/On Demand Scan
  - Scannen auf Adware und PUA
- Live-Protection
  - Übermitteln von Dateisamples
- Web Control
  - Ermöglicht Überwachen des Surfverhaltens

Weiterhin sollten regelmäßig mit dem Tool PurgeDB[1] **alte Datenbankeinträge gelöscht** werden. Es ist empfohlen, alle Einträge älter als sieben Tage (vgl. [2]) zu löschen: `purgedb –HistoryLengthInDays=7`.

Aus **Stabilitätsgründen** sollten die folgenden Komponenten deaktiviert werden.

- Firewall

Optional können folgende Komponenten für einzelne Bereiche interessant sein:

- Patch Analyse
- Application Control
- Data Control
- Web Control

Sophos Datenschutzerklärung[3]

Die Sophos Firmengruppe ist verpflichtet, die privaten Datenschutzrichtlinien in den gesetzlichen Rahmen zu beachten und durchzuführen, siehe dazu Sophos Group Privacy Policy[4] und Sophos Endnutzerlizenzvertrag[5]. Um einen maximalen Schutz vor Schadcodes und infizierten Webseiten zu erhalten, nutzen die Sophos Produkte die Funktionen „Live-Protection“ und „Web-Control“. Sophos beabsichtigt und bearbeitet die aus diesen Funktionen gewonnen Daten **nicht** zum Erstellen von Nutzerprofilen. Diese Funktionen können von der zentralen Konsole aus deaktiviert werden.

---

[1] https://community.sophos.com/kb/en-us/109884
[2] https://heise.de/-2282242
[3] aus dem Vergabevermerk vom 19.12.2013 für die Landeslizenz Schleswig-Holstein, ausgeführt durch die FH Lübeck
[4] http://www.sophos.com/de-de/legal/sophos-group-privacy-policy.aspx
[5] https://www.sophos.com/de-de/legal/sophos-end-user-license-agreement.aspx