HIN ENDPOINT SECURITY SERVICE UND HIN ENDPOINT SECURITY TOOL-SUITE

Leistungsbeschreibung

Einleitung und Anwendungsbereich

Gegenstand dieser Leistungsbeschreibung sind die beiden Services «HIN Endpoint Security Service» und «HIN Endpoint Security Tool-Suite».
Diese Leistungsbeschreibung dient als integraler Bestandteil sowie als Ergänzung der Leistungsbeschreibung des HIN Abo respektive der HIN Gateway.

1. Beratung

Unterstützung und Beratung durch Spezialisten erfolgt ohne Gewähr und nach einem «Best Effort»-Ansatz. Die Unterstützung und Beratung erfolgt per Telefon, E-Mail oder Remote. Einsätze vor Ort erfolgen nur in Ausnahmefällen und nur gegen separate Entschädigung. Es besteht kein Anrecht auf eine bestimmte Dauer oder Umfang der Beratung oder Unterstützung. In gegenseitiger Absprache kann jedoch die Unterstützung durch eine Kostenübernahme durch den Kunden ausgeweitet werden.

2. Systemanforderungen

Der Einsatz des Endpoint Security Services ist an eine Reihe von Systemanforderungen und technische sowie organisatorische Rahmenbedingungen geknüpft. HIN behält sich vor, einzelnen Geräten, Organisationen oder Personen den Service vorzuenthalten. Weitere Voraussetzung sind der Webpage zu entnehmen.

3. Aufschaltung

HIN verpflichtet sich, dem Kunden den Service innerhalb von zwei Wochen zur Aufschaltung zur Verfügung zu stellen. Die Aufschaltung muss der Kunde dann selbstständig durchführen.

4. Alertierung, Reaktionszeit

Die Alertierung erfolgt zu HIN Servicezeiten (Montag bis Freitag, 08.00 bis 18.00 Uhr). Die Reaktionszeit erfolgt in der Regel innerhalb 2 Stunden («Best Effort») per Telefon, via Schutzsoftware oder per E-Mail.

5. Erkennung, Verhinderung und Desinfektion von Schadsoftware

HIN übernimmt keine Gewähr für (i) die Richtigkeit, Vollständigkeit, Aktualität oder Zuverlässigkeit der Inhalte der im Rahmen der Warndienste und Schadsoftware-Erkennungssoftware bereitgestellten Daten oder (ii) die zeitliche Koordinierung oder Verfügbarkeit der Warndienste.
HIN und seine Lizenzgeber und Lieferanten geben keine Garantien, Auflagen, Zusagen oder Zusicherungen jeglicher Art, weder ausdrücklich noch impliziert, gesetzlich vorgeschrieben oder anderweitig in Bezug auf den Service oder irgendwelche Software Dritter ab. HIN und seine Lizenzgeber und Lieferanten garantieren
insbesondere nicht, dass der Service alle Bedrohungen (schädliche oder sonstige), Anwendungen oder sonstige Komponenten erkennen und/oder korrekt identifizieren und desinfizieren kann.

6. Beschränkungen

Der Lizenznehmer respektive Kunde des Service darf den Service nicht mit oder in Verbindung mit sicherheitskritischen Anwendungen verwenden, wenn Grund zur Annahme besteht, dass ein Versagen des Produkts zu einer wesentlichen Körperverletzung, Verlust von Eigentum oder Leben führen kann. Alle Arten dieser Verwendung finden ausschliesslich auf Risiko des Lizenznehmers statt und der Lizenznehmer bestätigt, dass er HIN von allen Ansprüchen oder Schäden in Bezug auf eine derartige, unbefugte Verwendung schadlos hält.
Der Lizenznehmer respektive Kunde des Service darf den Service und die damit verbundenen Produkte nicht modifizieren und nicht durch Reverse Engineering analysieren.
Zugang zum Service und die damit verbundenen Produkte an Dritte zu übertragen oder zu gewähren, ist nicht erlaubt.

7. Sicherung der Daten

Der Lizenznehmer erkennt an und erklärt sich damit einverstanden, dass ausschliesslich der Lizenznehmer für die Sicherung aller seiner Daten verantwortlich ist und die entsprechenden Massnahmen treffen muss, um diese Daten zu schützen. HIN und ihre Drittlizenzgeber übernehmen keinerlei Haftung oder Verantwortung für verlorengegangene oder beschädigte Daten.

8. Datenspeicherung

HIN erfasst nur eine sehr geringe Anzahl personenbezogener Daten zusätzlich zu den im Rahmen der elektronischen Identität von HIN erfassten Daten. Diese Daten werden benötigt, um den Schutz des Endpoints, die Durchsetzung von Sicherheitsrichtlinien und die Bereitstellung von Reports zu ermöglichen. Folgende Daten werden erfasst:

- Richtlinieninformationen – Einstellungen (abhängig von Richtlinienkomponenten) oder Beispielausnahmen
- Geräteinformationen – Gerätename, letzter Benutzer, Informationen zum Betriebssystem, Status
- Ereignisse – Typ, z. B. Web, Gerät, Malware, Geräteinformationen (Datei- und Pfadnamen, Netzwerkorte, Logins usw.)
- HIN speichert nicht den gesamten Browserverlauf der Endbenutzer; nur Webereignisse für blockierte Webseiten und für Webseiten, vor denen gewarnt wurde, werden zu Reporting-Zwecken gespeichert.

Die Daten werden geschützt in der Sophos Cloud in Frankfurt, Deutschland gespeichert. Unter dem folgenden Link ist die Datenschutzerklärung von SOPHOS Central ersichtlich: https://www.avanet.com/assets/pdf/sophos-central-datenschutz.pdf

HEALTH INFO NET AG
November 2018