Leistungsbeschreibung – Managed Endpoint Security

Zielsetzung

Das Ziel des Managed Endpoint Security Services ist es, den umfassenden Schutz von Workstations und Servern des Kunden gegen Viren, Malware und andere Cyber-Bedrohungen sicherzustellen. Durch die Bereitstellung und regelmäßige Aktualisierung von Antivirus-Software streben wir an, die Sicherheit der IT-Infrastruktur zu maximieren und die Integrität der Daten zu bewahren.

Leistungsumfang

1. Bereitstellung von Lizenzen

Inklusion von Wartungs- und Updatepaketen für den optimalen Schutz von Workstations und Servern.

2. Regelmäßige Überprüfung:

Tägliche Kontrolle der Aktualität der Antivirus-Signaturen, um sicherzustellen, dass die Systeme mit dem neuesten Schutz ausgestattet sind.

3. Alarmierung und Anpassung:

Benachrichtigung bei veralteten Antivirus-Signaturen und Anpassung der Richtlinien bei Systemstörungen oder Konflikten mit anderer Software.

4. Umfassender Schutz:

- AntiVirus-Engine: Virenscanner arbeiten mit Signaturen. Hier finden Sie die Hersteller der Datenbanken – bei der Endpoint Security arbeiten zwei perfekt aufeinander abgestimmte Engines gleichzeitig.
- Persisten Footholts: Der Persistens Footholt analysiert, wie sich schädliche Dateien verhalten und findet dadurch sogar unbekannte Viren.
- Webschutz: Der Webschutz überprüft schon beim Surfen alle Internetinhalte auf Infektionen. Schädliche Webseiten werden nicht angezeigt.
- 24/7 Security Operations Center: Kontinuierliche Analyse der Vorgehensweise von Hackern zur Beseitigung von Cyber-Bedrohungen.

Leistungserbringung

Die Überprüfung erfolgt kontinuierlich, um die Sicherheit der IT-Infrastruktur des Kunden zu gewährleisten. Leistungen der Ihre Helden GmbH werden von Montag bis Freitag von 8.00 Uhr bis 17.00 Uhr erbracht, ausgenommen sind bundesweit geltende Feiertage. Bei Notwendigkeit eines Systemneustarts erfolgt dies nach Absprache.

Weitere enthaltene und nicht enthaltene Leistungen

Der Service umfasst nicht die Beseitigung eines Virenbefalls und dessen Folgen; diese Leistungen werden separat angeboten und abgerechnet.

Haftung und Verantwortung

Während die Ihre Helden GmbH nach besten Kräften und Standards zum Schutz der Workstations und Server beiträgt, ist ein 100%iger Schutz vor Viren und Malware nicht möglich.
Die Verantwortung für den umsichtigen Umgang mit IT-Ressourcen bleibt beim Kunden, insbesondere im Hinblick auf das Verhalten der Endnutzer und die Zeitspanne zwischen dem Bekanntwerden neuer Schadsoftware und der Verfügbarkeit entsprechender Schutzmaßnahmen durch den Softwarehersteller.

Mitwirkungspflicht des Kunden

Der Kunde verpflichtet sich, den von der "Ihre Helden GmbH" bereitgestellten Hinweisen und Anweisungen, welche über das System oder per E-Mail übermittelt werden, aktiv nachzukommen. Diese Anweisungen können, ohne darauf beschränkt zu sein, Updates der Software, Änderungen an den Konfigurationseinstellungen oder Empfehlungen zur Verbesserung der Nutzererfahrung umfassen.

Sollte der Kunde diesen Mitwirkungspflichten nicht nachkommen, werden bereits unternommene Kontaktversuche und erbrachte Leistungen seitens der "Ihre Helden GmbH" als vollständig und ordnungsgemäß erachtet. In einem solchen Fall erlischt der Anspruch des Kunden auf die Funktionalität der bereitgestellten Dienste oder Produkte.

Um die Rechte und Pflichten beider Parteien zu wahren, empfehlen wir dem Kunden dringend, bei Erhalt solcher Kommunikationen zeitnah zu reagieren. Eine ausbleibende oder verzögerte Reaktion kann dazu führen, dass die Funktionalität der Dienste oder Produkte beeinträchtigt wird.

Diese Bestimmung zielt darauf ab, eine reibungslose Zusammenarbeit und die höchstmögliche Qualität der Dienstleistung zu gewährleisten. Bei Fragen oder Unsicherheiten bezüglich der empfangenen Anweisungen bittet Ihre Helden GmbH um umgehende Kontaktaufnahme, um Unterstützung anzubieten.

Die Sensibilisierung der Mitarbeiter im Umgang mit IT-Ressourcen ist entscheidend für die Cybersicherheit. Mitarbeiter sollten regelmäßig über sichere Online-Praktiken informiert werden, z.B. das Erkennen von Phishing-Versuchen, die Bedeutung regelmäßiger Passwortänderungen und den vorsichtigen Umgang mit unbekannten E-Mails und Anhängen. Eine proaktive Schulung kann wesentlich dazu beitragen, Risiken zu minimieren.