Leistungsbeschreibung – managed Firewall (01/2024)

Vorbemerkung

Wenn im Folgenden zwischen Basis, Standard und Premium unterschieden wird, gilt eine Sache für ausschließlich das/die genannte(n) Pakete, andernfalls für alle drei Pakete.
Die Anzahl der abgerechneten Firewalls ergibt sich aus der Anzahl der unter dem Punkt „Bestandteile" des zugehörigen managed Service-Vertrages aufgeführten Menge an Firewalls.
Sofern ein managedFirewall Vertrag ohne Hardwareanschaffung gebucht wird, entfallen die unten aufgeführten Punkte "1. Bereitstellung einer Hardware-Firewall", "7. Sicherheitsumfang des bereitgestellten Software-Pakets" und "9. Grundinstallation und Ersteinrichtung der Firewall".
Die Vertragslaufzeit richtet sich nach der aufgedruckten Vertragslaufzeit auf dem zugehörigen managed Service-Vertrages, beträgt mindestens jedoch 12 Monate. Der Vertrag verlängert sich um je zwölf Monate, sollte er nicht mit einer Frist von drei Monaten zum Ablaufdatum schriftlich gekündigt werden.

Voraussetzungen

Die zuverlässige, sichere und kostengünstige Betreuung innerhalb dieses Konzepts basiert auf bestimmten Voraussetzungen der IT-Struktur beim Auftraggeber. Dies umfasst:

- Der Auftraggeber ist für das tägliche Anfertigen von mindestens zwei Voll-Datensicherung sowie einer Archivierung verantwortlich, wobei eine in einem anderen Brandabschnitt aufbewahrt werden muss.
- Für die eingesetzte Hard- und Software ist erforderlich, dass sie über einen gültigen Herstellersupport (bspw. CarePack, Softwarepflegevertrag, Maintenance, Microsoft Lifecycle Support) verfügt.
- Eine Ist-Analyse mit den Komponenten Netzwerkstruktur inkl. IP-Adressliste, externe Provider-Anbindung, Firewall-Konzept, Softwarestände, Hardwareüberblick, Backup-Konzept, Ansprechpartner der involvierten Personen beim Auftraggeber und dessen Softwarelieferanten, Notfallplan ist vorhanden und entspricht der aktuellen Konfiguration.
- Auf Basis der Erkenntnisse der Ist-Analyse ist möglicherweise die Umsetzung eines Maßnahmenplans notwendig.

Für die Bereitstellung der Ziffer 8 ist die Buchung der Managed Server bzw. Managed Client Pakete Standard oder Premium Voraussetzung. Ansonsten verfällt der Anspruch.

1. Bereitstellung einer Hardware-Firewall

Eine nach üblichem Standard gesicherte Hardware-Firewall inkl. Lizenz für den gebuchten Leistungsumfang wird innerhalb der Vertragslaufzeit durch den Auftragnehmer bereitgestellt. Eine Klassifizierung für empfohlene Nutzerzahlen erfolgt durch den Hersteller. Der Auftragnehmer behält sich die Empfehlung einer von dieser Herstellerangabe abweichenden Nutzerzahl im Einzelfall vor. Die VPN-Funktionalität ermöglicht Standortvernetzungen (Site-to-Site-VPN) und den Zugriff entfernter Benutzer (Remote-User-VPN, über SSL oder IPSec). Enhanced Support ist ebenfalls enthalten.

2. Funktionsprüfung / Monitoring

Aus dem internen Netz des Auftraggebers erfolgt eine Prüfung der Verfügbarkeit der Firewall, der Schnittstellen inkl. Internetanbindung, der VPN-Verbindungen, der Firewall-Dienste und des Hochverfügbarkeits-Modus (sofern genutzt). Im Fehlerfall erfolgt eine Alarmierung gemäß Ziffer 3. Die Überprüfung findet dabei im 60- (bei Basic), 30- (bei Standard) bzw. 15-Minuten-Takt (bei Premium) rund um die Uhr statt. Es gilt die Interventionszeit nach Ziffer 4.
Für die Funktionalität wird ein Agent auf einem, durch den Auftragnehmer bestimmten, Servern installiert, der zwingend eine ausgehende SSL-Internetverbindung (Port 443) in ein bestimmtes Zielnetz nach außen benötigt.

3. Alarmierung

Die Alarmierung im Basic-Paket erfolgt an bis zu drei frei wählbare Empfänger des Auftraggebers. Eine Alarmierung des Auftragsnehmers erfolgt hierbei nicht. Sollte es aus Sicht des Auftraggebers notwendig sein, Fehlerlösungsmaßnahmen durch den Auftragnehmer einzuleiten, so wird der Auftraggeber den Auftragnehmer hierzu über folgende Kommunikationskanäle unter Ziffer 4 beauftragen (es gilt die Interventionszeit nach Ziffer 4).

Im Standard- und Premium-Paket erfolgt eine Alarmierung direkt an den Auftragnehmer. Es wird in diesem Fall die Interventionszeit nach Ziffer4 angewendet sowie die Abrechnung nach Ziffer 20 vorgenommen.

4. Reaktions- / Interventionszeit bei unternehmenskritischen Problemen

Vom Auftragnehmer wird ein Problem als kritisch eingestuft, wenn dadurch Arbeitsausfall für mehrere Personen verursacht wird oder wichtige Kernprozesse laut Anlage 1 der Managed Firewall Servicebedingungen erheblich beeinträchtigt sind. Bei kritischen Problemen muss seitens des Auftragnehmers innerhalb des Next-Business-Day (Basic-Paket) bzw. acht Stunden (Standard-Paket) oder vier Stunden (Premium-Paket) während des Servicezeitraums Mo-Fr 8-17 Uhr mit der Problemlösung entweder beim Auftraggeber vor Ort, per telefonischer Hilfestellung oder per Fernwartung begonnen werden. Die Interventionszeit beginnt mit Mitteilung an den Auftragnehmer unter den folgenden Kommunikationskanälen:

- über das Ticket-Portal portal.kunze-ritter.de
- per E-Mail an support.it@kunze-ritter.de
- telefonisch über 0761 45554-77

Der Auftraggeber ist zur Mitwirkung bei der Problemanalyse und -lösung des Auftragnehmers verpflichtet. Bei unkritischen Problemen muss innerhalb von 48 Stunden während des Servicezeitraums Mo-Fr 8-17 Uhr mit der Problemlösung oder Terminierung der Problemlösung begonnen werden.
Der Auftraggeber benennt einen Systemverantwortlichen und einen Stellvertreter.

5. Austausch bei Hardware-Defekt

Ein Hardware-Defekt wird durch den Auftragnehmer nach üblichen Standards analysiert und vom Support des Hardwareherstellers bestätigt. Ab Bestätigung eines Hardware-Defekts durch den Support des Hardwareherstellers gilt eine Frist von 48 Stunden (Basis-Paket), 24 Stunden (Standard- und Premium-Paket) für die Lieferung eines gleich- oder höherwertigen Ersatzgerätes an den Einsatzort des Defektgerätes. Dieser Service ist regional begrenzt verfügbar innerhalb des Festlandes der Bundesrepublik Deutschland (ohne Inseln).

Die Abrechnung von Analysetätigkeiten und Reisekosten wird zu den Konditionen nach Ziffer 20 nach Aufwand vorgenommen. Die Kosten für das Ersatzgerät sowie Versandkosten, der Hardwaretausch innerhalb der Infrastruktur des Auftraggebers, das Einspielen einer Konfiguration oder Wiederherstellen einer Datensicherung auf dem Ersatzgerät sind in der Monatsgebühr der Managed Firewall enthalten.

6. Datensicherung der Konfiguration

Die Datensicherung der auf der Administrationsoberfläche gesetzten Einstellungen/Konfiguration erfolgt monatlich (Basis-Paket), wöchentlich (Standard-Paket) bzw. täglich (Premium-Paket). Die letzten fünf Sicherungen werden im Rechenzentrum des Auftragnehmers für den Auftraggeber vorgehalten.

7. Sicherheitsumfang des bereitgestellten Software-Pakets

- Eindringungsvermeidung (IPS): Eindringungsversuche in gesicherte Netzwerke werden auf Basis von vordefinierten oder eigens anzulegenden Schutzprofilen erkannt, gesperrt und in das Firewall-Protokoll eingetragen.
- Abwehr gezielter Angriffe (ATP): Überwachung und Protokollierung von eingehendem Datenverkehr durch Kumulierung von Gefahrpunkten aus den verschiedenen Sicherheitsmodulen der Firewall.
- Applikations-Filter nach Benutzern, Bandbreite & Zeit: Der Applikations-Filter beinhaltet vordefinierte Applikationen wie bspw. Skype, Dropbox, TeamViewer. Im Zusammenspiel mit dem Managed Client/Endpoint ab Stufe Standard können der Firewall auch unbekannte Applikationen vom Client der Firewall gemeldet und dort dann freigegeben werden. Die Bandbreite kann je nach Applikation reglementiert werden (Mindestbandbreite, Obergrenze für die Bandbreite oder Gewichtung der verfügbaren Bandbreite). Es könnten Zeiträume pro Benutzergruppe definiert werden, in welchen der Datenverkehr zugelassen oder gesperrt wird.
- Gateway Antivirus: Über die Firewall übertragene Daten werden mit Hilfe automatisch aktualisierte Signaturdaten auf Viren überprüft. Dieser Schutz ergänzt die Antivirus-Strategie und sollte in Kombination mit Virenschutz auf Endgeräten wie Notebooks, PCs, Servern betrieben werden.
- Webseiten-Filter: Webseitenzugriffe können a) einzeln nach Namen, b) durch automatische Zuordnung vergleichbarer Inhalte in verwaltete Kategorien oder c) automatisch durch täglich aktualisierte Risikolisten limitiert werden. Die Aufnahme von weiteren zu sperrenden oder freizugebenden Webadressen ist im Monatspreis enthalten.
- Geschützte Zonen für bspw. Abteilungen, Server, WLAN: Die Firewall ermöglicht die Erstellung von getrennten Sicherheitszonen auf Basis von Sub-Netzen und reglementiert den Verkehr zwischen den Zonen.
- Ausfallsicherheit für Breitbandanschlüsse: Bei Verwendung von zwei oder mehr Breitbandinternetanschlüssen kann ein automatisches Umschalten bei Ausfall eines Anschlusses eingerichtet werden.
- Zugriff auf Ressourcen per Web-Browser: Es ist möglich, von außen eine Verbindung auf ein webbasiertes Verzeichnis („Benutzerportal") von internen Ressourcen wie bspw. Windows Remote-Desktop oder NAS-Verwaltungsoberflächen. Die Benutzer können gegen ein Active Directory authentifiziert werden.
- 2-Faktor-Authentifizierung: Das Benutzer-Portal, das Administrations-Portal sowie VPN-Verbindungen können mit einer 2-Faktor-Authentifizierung geschützt werden.
- Priorisierung von IP-Telefonie: Sprachübertragungen können durch Unterstützung von H.323 und SIP erkannt und bevorzugt behandelt werden.

Standard-Paket:
Zusätzlich sind folgende Merkmale im Leistungsumfang enthalten:

- Erkennen von unbekannten Bedrohungen: Es wird eine Verhaltensanalyse der eingehenden Datenpakete vorgenommen. Bei verdächtigem Inhalt werden die Datenpakete in eine Sandbox übertragen.
- „Waschmaschine in der Cloud": Überprüfung von Inhalten in einer cloudbasierten Sandbox: Das Aktivieren der Sandbox fügt eine neue Schutz-Stufe hinzu, indem verdächtige E-Mail-Anhänge an eine Sandbox-Umgebung gesendet werden, um vor komplexen gefährlichen Angriffen zu schützen. Dieser Schutz erfordert zusätzliche Zeit für das Scannen von Dateien (schätzungsweise 5-10 Minuten).

Premium-Paket:
Zusätzlich sind folgende Merkmale im Leistungsumfang enthalten:

- Spam-, Phishing- & Virenschutz für E-Mails: Der Empfang von unerwünschten Emails von durch die Firewall geschützten Mailservern wird von der Firewall erkannt und blockiert. Der Dienst versucht, schadhafte Dateitypen zu erkennen und unterbindet ihre Zustellung. Durch die Kombination von SPF-, DKIM- und DMARC-Authentifizierungstechniken und der Analyse von E-Mail-Header-Anomalien können legitime E-Mails weitestgehend erkannt werden, während Phishing-Mails ausgefiltert werden.
- Absicherung von nach außen bereitgestellten Servern (bspw. Webserver, Exchange Server, NAS) inkl. Virenschutz: Dies erfolgt über eine Reverse-Proxy-Funktionalität und eine sog. Web-Application-Firewall, welche in die Datenpakete hineinschaut, bevor die Datenpakete weitergeleitet werden.

8. Vernetzte Sicherheit zwischen Endpoint und Firewall

Im Standard- und Premiumpaket ist die vernetzte Sicherheit zwischen Endpoint und Firewall enthalten. Das bedeutet, dass der Endpoint der Firewall über seinen Gesundheitszustand in Form eines Ampelsystems Informationen mitteilt. Im weiteren Verlauf kann die Firewall die Datenübertragung zum Endpoint blockieren, um potenziellen Schaden abzuwenden.

9. Grundinstallation und Ersteinrichtung der Firewall

Die bereitgestellte Firewall wird beim Auftragnehmer aufgebaut und überprüft, Software-Updates installiert und Herstellerlizenzen registriert. Eine Ersteinrichtung mit durch den Auftraggeber zu liefernden Daten gemäß durch den Auftragnehmer bereitgestellter Checkliste wird durchgeführt. Bei fehlenden oder unvollständigen Daten wird der Auftragnehmer den Sicherheitsumfang des Software-Pakets gemäß Ziffer 7 aktivieren und nach üblichem Standard konfigurieren. Nacharbeiten zur Optimierung dieser Konfiguration nach Mitteilung durch den Auftraggeber werden innerhalb von 14 Tagen nach abgeschlossener Einrichtung gemäß Abnahmeprotokoll ohne zusätzliche Berechnung erbracht. Darüber hinaus wird gemäß vereinbartem Stundensatz unter Ziffer 20 abgerechnet.

Leistungen ausschließlich im Standard- und Premium-Paket

10. Installation von Software- / Firmwareupdates

Die Prüfung aktuell anstehender Sicherheitsupdates erfolgt täglich automatisiert. Der Auftragnehmer trägt dafür Sorge, dass die Systeme des Auftraggebers immer mit einer durch den Hersteller supporteten Firmware betrieben werden. Während und nach der Installation von Firmwareupdates ist häufig ein kurzzeitiger, geplanter Ausfall mit anschließendem Neustart der Hardware notwendig. Dieser wird nach Absprache auch außerhalb der Arbeitszeit Mo. – Fr. 8-17 Uhr ausgeführt und ist im Preis enthalten.
Die Sicherstellung der erfolgreichen Installation der Firmware- und Sicherheitsupdates erfolgt unmittelbar nach der Durchführung. Der Auftraggeber ist damit einverstanden, dass die vom Hersteller veröffentlichten Firmware- und Sicherheitsupdates ohne vorherige Prüfung auf den Systemen installiert werden. Die Haftung für die Fehlerfreiheit der Sicherheitsupdates, die Sinnhaftigkeit der Risiko-Klassifizierung sowie die Kompatibilitätseinschätzung mit der zu aktualisierenden Software liegt allein beim jeweiligen Hersteller.
Dem Auftraggeber ist bewusst, dass Softwareupdates Veränderungen an der installierten Software vornehmen, um die Sicherheit oder Stabilität zu verbessern. Bei diesen Veränderungen kann es zu Problemen kommen, die die Lauffähigkeit des Systems negativ beeinflussen. Für Folgeschäden aus diesem Umstand übernimmt der Auftragnehmer keine Haftung. Der Auftragnehmer wird die Problemlösung nach üblichen Standards herbeiführen.

11. Regelmäßiges Ändern des Administratorpasswortes

Das Administratorpasswort wird durch den Auftragnehmer jährlich (Standard-Paket) bzw. halbjährlich (Premium-Paket) geändert, um Einbrüche in das System durch Unbefugte zu erschweren.

Leistungen ausschließlich im Premium-Paket

12. Behebung von herstellerseitigen Sicherheitslücken

Bei herstellerseitigen Sicherheitslücken ist die umgehende Aktualisierung der eingesetzten Firmware notwendig. Sollten Sicherheitslücken durch den Hersteller kommuniziert werden, installiert der Auftragnehmer die neue Firmware innerhalb von 7 Tagen auf den Systemen des Auftraggebers. Während und nach der Installation von Firmwareupdates ist häufig ein kurzzeitiger, geplanter Ausfall mit anschließendem Neustart der Hardware notwendig. Dieser wird nach Absprache auch außerhalb der Arbeitszeit Mo. – Fr. 8-17 Uhr ausgeführt und ist im Preis enthalten.

13. Versand eines Sicherheitsberichts

Es erfolgt ein wöchentlicher Versand eines Sicherheitsberichts mit mindestens den folgenden Bestandteilen an bis zu drei E-Mail-Adressen des Auftraggebers: Risiko-User, Risiko-Applikation, geblockte Applikation und Web-Kategorien.

14. Beratungsgespräch über Firewall-Status & -Strategie

Der Auftraggeber erhält bei Buchung des Premium-Pakets ein regelmäßiges Beratungsgespräch über den Firewall-Status und die Firewall-Strategie. Bestandteil ist die Interpretation der erstellten Handlungsempfehlungen und Dokumentation sowie die Ableitung etwaiger Maßnahmen. Des Weiteren werden aktuelle Trends, wie bspw. die aktuelle Gefährdungslage auf die Relevanz für den Auftraggebers gemeinsam überprüft.

Erweiterungen

15. Erweiterung auf Hochverfügbarkeit (aktiv/passiv)

Das im managed Service-Vertrag ausgewählte Firewall-System kann auf Hochverfügbarkeit erweitert werden. Dafür wird ein zweites Firewall-System gleicher Art und Güte bereitgestellt und im Verbund mit dem ersten Firewall-System betrieben. Im Falle eines Ausfalls eines Firewall-Systems, übernimmt das jeweils andere System den Betrieb und die Bereitstellung von Verbindungen sowie Sicherheitsregeln. In der Regel erfolgt diese Übernahme unterbrechungsfrei und ermöglicht den Regelbetrieb, während Maßnahmen zu einer Wiederherstellung oder einem Austausch des ausgefallenen Systems ergriffen werden. Es ist ausschließlich der hochverfügbare Betrieb von zwei Firewall-Systemen gleicher Art und Güte vorgesehen.

16. Erweiterung Rackmountkit für Firewall

Für die Firewall werden die passenden Rackmountkits zum Einbau in einen Server- oder Netzwerkschrank über die Vertragslaufzeit durch den Auftragnehmer ohne Aufpreis bereitgestellt.

17. Erweiterung Bereitstellung Remote Ethernet Devices

Für die Erweiterung der Netzwerk-Konnektivität auf die Remote-Standorte und Zweigstellen des Auftraggebers werden in der gewünschten Menge aus dem managed Service-Vertrag für die Vertragslaufzeit Sophos SD-RED-Geräte durch den Auftragnehmer bereitgestellt.
Alle Daten zwischen der SD-RED und Ihrer Sophos-Firewall werden unter Einhaltung von AES-256-Vorgaben verschlüsselt.

18. Erweiterung Bereitstellung Access Points

Für die Einrichtung einer kabellosen Netzwerk-Infrastruktur werden in der gewünschten Menge aus dem managed Service-Vertrag für die Vertragslaufzeit Sophos Access Points durch den Auftragnehmer bereitgestellt. Die Access Points können lediglich über Power over Ethernet (PoE) angeschlossen und betrieben werden.

19. Quartals-Support-Flatrate

Wurde im managed Service-Vertrag die Option „Quartals-Support-Flatrate" (möglich in Standard- und Premiumpaket) gebucht, so können Supportdienstleistungen, die die gebuchten Bestandteile des Servicevertrags betreffen (z.B. Client, Server, Firewall), zum vergünstigten Stundensatz über den managed Vertrag abgerechnet werden. Die Leistungen werden in der Zeit von Mo-Fr 8-17 Uhr erbracht. Es gilt die Interventionszeit nach Ziffer 4. Die Flatrate für Störungsbeseitigungen und Administrationstätigkeiten bezieht sich auf technische Dienstleistungen, die am Betriebssystem sowie an weiteren Anwendungen & Diensten laut Anlage 1 durchgeführt werden. Weitergehende Tätigkeiten an Softwareprogrammen oder angeschlossenen bzw. verbundenen Geräten wie NAS, SAN-Systeme sind nicht durch die Flatrate abgedeckt.

Die monatlich über die Quartals-Support-Flatrate gebuchten Stunden sind für das jeweilige Quartal gültig. Nach Ablauf eines jeden Quartals wird die tatsächliche monatlich benötige Dienstleistung der vergangenen drei Monate ermittelt. Sofern eine Abweichung von mind. 20% pro Monat besteht, wird die Höhe der Quartals-Flatrate-Stunden automatisch um diese Abweichung zur nächsten vollen Stunde erhöht oder verringert. Eine Nachberechnung oder Nachvergütung erfolgt nicht. Der Auftraggeber erhält jeweils eine Stundenübersicht zur besseren Nachvollziehbarkeit der getätigten Arbeiten. Projektdienstleistungen sind von der Quartals-Support-Flatrate ausgenommen.

Sonstige Informationen

20. Stundensatz für weitere Leistungen

Der Stundensatz für die Erbringung von Dienstleistungen wie technische Hilfestellung, Fehleranalyse, Lösungserarbeitung, Umsetzung und Dokumentation in der Zeit von Mo-Fr 8-17 Uhr gilt gemäß der aktuellen Preisliste. Abgerechnet wird im 15-Minuten-Takt.

Etwaige Fahrtkosten werden mit EUR 0,60 pro Entfernungskilometer berechnet. Fahrtzeiten werden zum Stundensatz abgerechnet.

Ein Fernzugriff auf die Systeme des Auftraggebers erspart diesem die Fahrtkosten, die Zeit wird wie zuvor genannt abgerechnet.

Der Auftraggeber ist damit einverstanden, dass aufgrund von Fehlermeldungen, die sich aus dem Monitoring der Server nach Ziffer 2 ergeben, bis zu einer Stunde pro Monat pro Server die notwendigen technischen Maßnahmen auf Basis der Vergütungsregelung in dieser Ziffer eingeleitet werden.

Außerhalb des Zeitraums werden 50 % Zuschlag (zwischen 18-20 Uhr), 100 % Zuschlag (zwischen 20-07 Uhr), 100 % Zuschlag für Samstagstätigkeiten bzw. 150 % Zuschlag an Sonntag- und Feiertagen berechnet.

21. Preisanpassungen

Kunze & Ritter kann jederzeit ohne eine begründete Erklärung eine Anpassung der Vergütung verlangen. Ab einer Preiserhöhung von mehr als 10 % wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.

22. Gültigkeit Servicebedingungen

Nachrangig zu den Regelungen dieser Leistungsbeschreibung gelten die Servicebedingungen in der jeweils aktuellen Version. Außerdem gelten nachrangig für die eingesetzten Softwareprodukte die Lizenz- und Nutzungsbedingungen der jeweiligen Hersteller.

Anlage 1: Kernprozesse und Flatrate Anwendungen & Dienste

Im Kerngeschäft kann der Auftragnehmer über diesen managed Vertrag die nachfolgenden Anwendungen und Dienste betreuen.

DNS & DHCP	VPN	IPSec	(Reverse) Proxy
SPF	DKIM	DNAT	IPS
ATP	WAF		

Abweichende Drittanbieter Anwendungen werden nur nach expliziter Absprache mitbetreut.