Leistungsbeschreibung

Managed Security: Zentrale & Dezentrale Firewall für Geschäftskundschaft

Inhaltsverzeichnis

1 Allgemeines

Die EWE TEL GmbH (im Folgenden Anbieter genannt) erbringt die nachfolgend beschriebene Dienstleistung EWE Managed Security: Zentrale & Dezentrale Firewall (im Folgenden: „Firewall-Service“) auf Basis der Vereinbarungen im Auftragsformular und der AGB des Anbieters für Telekommunikations- und Online- sowie Datendienstleistungen (Geschäftskunden) (im Folgenden: „AGB“).

1.1 Funktionsweise des Firewall-Service

Der Firewall-Service arbeitet als Filter zwischen IP-Netzen wie z. B. dem Internet und dem zu schützenden IP-Netz des Kunden. Der Firewall-Service verfügt über ein Regelwerk, das Kommunikationsbeziehungen zwischen IP-Netzen gemäß den Vorgaben des Kunden abbildet. Kommunikationsbeziehungen definieren die Zugriffsmöglichkeiten auf Ressourcen aus dem IP-Netz des Kunden in das Internet und umgekehrt.

1.2 Umfang und Modalität des Firewall-Service

Die vertragsgegenständliche Dienstleistung umfasst die Bereitstellung, die Konfiguration, das Management und die Wartung des Firewall-Service gemäß dieser Leistungsbeschreibung. Der Anbieter erbringt Firewall-Service, je nach Vereinbarung mit dem Kunden, zentral oder dezentral:

- Soweit eine Zentrale Firewall vereinbart ist, erbringt der Anbieter den Firewall-Service auf einem eigenen System in seinen eigenen Räumlichkeiten.

- Soweit eine Dezentrale Firewall vereinbart ist, erbringt der Anbieter den Firewall-Service mittels einer Hardware-Firewall, die in den Räumlichkeiten des Kunden aufgestellt wird. Die besonderen Vereinbarungen, die nur im Falle der Vereinbarung eine Dezentralen Firewall gelten, sind in Abschnitt 3 enthalten.

Die Einrichtung oder Bereitstellung eines Internetzugangs sind nicht Bestandteil des Firewall-Service. Ebenso wenig ist es Bestandteil des Firewall-Service, die notwendigen technischen Voraussetzungen beim Kunden, insbesondere die erforderliche technische Infrastruktur, zu schaffen oder bei deren Beschaffung zu unterstützen.

1.3 Wirkungsbereich des Firewall-Service

Der Firewall-Service kann nur denjenigen Datenverkehr prüfen, der durch sie transportiert wird. Für die volle Funktionalität des Firewall-Service muss der Kunde sicherstellen, dass keine sonstigen Verbindungen zwischen den durch den Firewall-Service getrennten IP-Netzen aufgebaut werden und dass keine Änderungen durchgeführt werden, die den Firewall-Service in seiner Funktion beeinflussen. Der Anbieter kann nicht gewährleisten, dass das IP-Netz des Kunden sicher ist. Der Anbieter stellt vielmehr einen Sicherheitsmechanismus zur Verfügung, mit dessen Hilfe der Kunde ein hohes Maß an Absicherung vor unerwünschten Zugriffen und potenziell schadensverursachenden Angriffen erreichen kann. Der Firewall-Service kann nicht

- vor unbekannten Angriffen schützen,
- verschlüsselte oder mehrfach komprimierte Dateien auf schadensverursachende Inhalte hin untersuchen.

2 Basisleistung

Im Rahmen des Firewall-Service erbringt der Anbieter in jedem Fall die nachfolgend beschriebene Basisleistung. Der Kunden kann zusätzlich die in Abschnitt 3 beschriebenen kostenpflichtigen optionalen Leistungen bestellen.

Im Rahmen der Basisleistung werden, abhängig vom Regelwerk (Abschnitt 2.4), Zugriffe, die sich auf IP/ICMP (Netzwerk-Layer, OSI-Layer 3) oder TCP/UDP (Transport-Layer, OSI-Layer 4) beziehen, nur dann zugelassen, wenn sie explizit erlaubt sind. Dies gilt für Zugriffe auf den Firewall-Service selbst und auf die zu schützenden IP-Netze. Die Basisleistung des Firewall-Service bietet, soweit kein Unified Threat Protection (UTP, Abschnitt 3.1) vereinbart ist, keinen Schutz vor Angriffen auf Anwendungsebene (OSI-Layer 5 bis 7).

2.1 Implementierung des Firewall-Service

Der Firewall-Service wird zwischen dem zu schützenden IP-Netz des Kunden (z. B. Local Area Network, LAN) und dem Internet eingesetzt und bietet Funktionen, um unerwünschten Netzwerkverkehr zwischen diesen IP-Netzen zu unterbinden. Die Implementierung des Firewall-Service erfolgt auf Basis des TCP/IP-Protokolls. Im Zuge der Implementierung des Firewall-Service richtet der Anbieter eine IP-Adresse aus den angeschlossenen IP-Netzen des Kunden innerhalb des Firewall-Service ein; dem Kunden obliegt es, dem Anbieter rechtzeitig eine geeignete IP-Adresse mitzuteilen.

2.2 Daten-Durchsatz des Firewall-Service

Mit welcher Geschwindigkeit die Daten von dem Firewall-Service verarbeitet werden (Daten-Durchsatz) ergibt sich aus den Vereinbarungen in dem Auftragsformular und der Preisliste.

2.3 Hardware-Firewall

Soweit eine **Dezentrale** Firewall vereinbart ist, gilt:

Der Anbieter überlässt dem Kunden während der Laufzeit des Vertrages über den Firewall-Service eine Hardware-Firewall. Für die Überlassung gelten insbesondere die besonderen Bestimmungen der AGB für die zeitweise Überlassung von Hardware. Der Kunde hat keinen Anspruch auf einen bestimmten Hersteller oder ein bestimmtes Modell der Hardware-Firewall. Der Anbieter wird die Hardware-Firewall an dem vereinbarten Aufstellungsort aufstellen, es sei denn, der Kunde wünscht ausdrücklich die Versendung der Hardware-Firewall.

2.4 Regelwerk

In dem Regelwerk ist festgelegt, welche Kommunikationsbeziehungen zwischen IP-Netzen innerhalb des Firewall-Service berücksichtigt werden. Eine Kommunikationsbeziehung besteht, wenn eine Ressource aus dem IP-Netz des Kunden Daten in das Internet sendet und/oder in umgekehrter Richtung Daten aus dem Internet empfängt.

Das Regelwerk wird ausschließlich in einem elektronischen Format geführt. Der Kunde kann während des Betriebs des Firewall-Service den aktuellen Stand des Regelwerks einsehen.

2.5 Mitwirkung des Kunden vor der Bereitstellung

Der Anbieter kann den Firewall-Service erst implementieren und bereitstellen, nachdem der Kunde ihm die hierfür erforderlichen Informationen gegeben hat. Zu diesen Informationen zählen insbesondere diejenigen Kommunikationsbeziehungen, die von dem Firewall-Service berücksichtigt werden sollen.

Der Kunde ist verpflichtet, diese Informationen unverzüglich nach Vertragsschluss, spätestens jedoch binnen einer Frist von vier Wochen an den Anbieter zu übermitteln. Dies kann auch im Rahmen eines Consulting-Termins mit dem Kunden und dem Anbieter stattfinden, der telefonisch durchgeführt wird.

Liegen dem Anbieter die Informationen, die für die Bereitstellung erforderlich sind, binnen der Frist von vier Wochen nicht oder nicht vollständig vor, wird er dem Kunden auffordern, diese Informationen binnen einer Frist von zwei Wochen an den Anbieter zu übermitteln. Verläuft auch diese zweite Frist fruchtlos, wird der Anbieter dem Kunden das vereinbarte monatliche Entgelt in Rechnung stellen.

2.6 Bereitstellung

Im Zuge der Bereitstellung konfiguriert der Anbieter den Firewall-Service und richtet das Regelwerk entsprechend den Festlegungen im Consulting-Termin ein.

Stellt der Kunden binnen einer Frist von 10 Werktagen nach der Bereitstellung des Firewall-Service fest, dass das im Rahmen des Consulting-Termins festgelegte Regelwerk unvollständig oder fehlerhaft ist und informiert den Anbieter hierüber binnen der 10-Tages-Frist, wird der Anbieter die Firewall-Regeln entsprechend erweitern oder korrigieren. Die Frist zur Abnahme des Firewall-Service (Abschnitt 2.7) bleibt hiervon unberührt.

Soweit eine **Dezentrale** Firewall vereinbart ist, gilt Folgendes:

Der Anbieter installiert die Hardware-Firewall an dem hierfür mit dem Kunden vereinbarten Standort. Wahlweise kann der Kunde die Installation selbst vornehmen; in diesem Fall informiert der Kunde den Anbieter, nachdem er die Installation erfolgreich abgeschlossen hat.

2.7 Abnahme

Nach der Bereitstellung des Firewall-Service fordert der Anbieter den Kunden zur Abnahme des Firewall-Service auf. Die Abnahme kann nicht auf Grund unwesentlicher Mängel verweigert werden. Der Abnahme steht es gleich, wenn der Kunde den Firewall-Service nicht binnen einer Frist von 10 Werktagen abgenommen hat, obwohl er dazu verpflichtet ist.

2.8 Betrieb des Firewall-Service

Der Anbieter betreibt den Firewall-Service via Fernzugriff. Voraussetzung hierfür ist, dass die vom Kunden beizustellende Anbindung an sein Wide Area Network (WAN) (Abschnitt 6) besteht und funktionstüchtig ist. Im Rahmen des Betriebs des Firewall-Service überwacht der Anbieter deren Funktion, fertigt Backups der Konfiguration an und führt die Software- und Hardwarepflege durch, z. B., indem er Patches einspielt oder Reparaturen durchführt. Die Einrichtung oder Bereitstellung des WAN-Zuganges für das Management des Firewall-Service ist nicht Bestandteil des Firewall-Service.

3 Optionale Leistungen

Der Kunde kann die nachfolgend beschriebenen optionalen Leistungen für erweiterte Sicherheitsfunktionen des Firewall-Service bei dem Anbieter bestellen.

3.1 Unified Threat Protection

Unified Threat Protection (UTP) ist eine Vereinigung verschiedener Sicherheitsfunktionen auf einer Plattform. Zu diesen Sicherheitsfunktionen gehören die folgenden, nachfolgend beschriebenen Funktionen:

- UTP – Antivirus & Anti-Malware,
- UTP – Webfilter,
- UTP – Intrusion Prevention,
- UTP - Application Control,
- UTP – GeoIP-Blocking & Botnet-Blocking.

3.1.1 UTP – Antivirus & Anti-Malware

Antivirus (AV) erkennt und schützt vor Computerviren auf Dateibasis, beschränkt sich jedoch auf bekannte Viren und Dateiformate, die nicht passwortgeschützt, verschlüsselt oder komprimiert sind. Anti-Malware erkennt Malware, die dem für diese Funktionen verwendeten System bekannt sind, filtert zuvor erkannte Malware aus den Datenströmen, die über die Firewall laufen, heraus und verhindert so, dass sie in die Systeme des Kunden übertragen wird.

3.1.2 UTP – Webfilter

Der Webfilter (WF) erlaubt es dem Kunden, den Zugriff auf Internetseiten durch individuelle oder kategoriebasierte Regeln zu steuern. Dabei können White-/Blacklists oder fest vorgegebene Kategorien verwendet werden. Der Webfilter kann kurzzeitig die Datenübertragung verzögern, um die angefragte Seite zu kategorisieren, und blockiert eine von den Regeln als unzulässig eingestufte Seiten, indem es statt der aufgerufenen Seite eine Meldung über die erfolgte Blockade anzeigt.

3.1.3 UTP – Intrusion Prevention

Intrusion Prevention (IPS) erkennt und verhindert, soweit es technisch möglich ist, Angriffe auf OSI-Layer 5 bis 7 anhand eines Regelsatzes mit Signaturen, die vom Hersteller der Hardware-Firewall bereitgestellt werden (IPS-Regelsatz). Der Anbieter richtet den IPS-Regelsatz entsprechend den Vorgaben des Kunden ein, hat jedoch keinen Einfluss auf die Signaturen oder Kategorien des Herstellers.

3.1.4 UTP – Application Control

Mit Application Control kann der Anbieter auf Wunsch des Kunden Richtlinien für den Firewall-Service erstellen, mit deren Hilfe der Zugriff auf Anwendungen oder auf bestimmte Kategorien von Anwendungen erlaubt, verweigert oder eingeschränkt werden kann.

3.1.5 UTP – GeoIP-Blocking & Botnet-Blocking

Der Firewall-Hersteller bietet Feeds an, die der Anbieter innerhalb des Firewall-Service verwenden werden kann, um auf Wunsch des Kunden z.B. geografische Einschränkungen zu implementieren. Außerdem können Botnetze (C&C) blockiert werden.

3.2 Secure Remote Access

Über Secure Remote Access (SRA) stellt der Firewall-Service mobilen Benutzern des Kunden einen sicheren Fernzugriff über das Internet auf Ressourcen innerhalb des IP-Netzes des Kunden bereit. Der Fernzugriff erfolgt über einen im Rahmen des Firewall-Service bereitgestellte Software-Clients Die maximale Anzahl gleichzeitig verbundener Benutzer über SRA ergibt sich aus dem Auftragsformular.

3.3 IPSec-VPN

Bei Vernetzung von Standorten über das Internet richtet der Anbieter im Rahmen dieser Option ein IPSec-VPN (Site-to-Site) nach Vorgabe des Kunden ein. Die bei der Übertragung solcher Daten zum Einsatz kommende Gegenstelle kann hierbei auf Grundlage eines separaten Vertrages vom Anbieter oder alternativ von dem Kunden sowie von Dritten bereitgestellt werden. Die Einrichtung oder Bereitstellung von Hard- oder Software auf Seiten der Gegenstelle ist nicht Bestandteil der Option IPSec-VPN.

3.4 Bandbreitenmanagement

Im Rahmen der Option Bandbreitenmanagement konfiguriert der Anbieter den Firewall-Service nach Vorgabe des Kunden so, dass bestimmte Bandbreiten für einem vom Kunden vorab festgelegten Datenverkehr reserviert werden (Traffic-Shaping). Der Anbieter stellt sicher, dass die vom Kunden vorab festgelegten Einstellungen innerhalb des Firewall-Service Anwendung finden. Für ein durchgängiges Bandbreitenmanagement (Quality of Service) ist mindestens Voraussetzung, dass der Kunde alle an der Übermittlung von IP-Paketen beteiligten aktiven Netztechniken in hierfür geeigneter Art und Weise einrichtet. Die Einrichtung oder Bereitstellung solcher Netztechniken über den Firewall-Service hinaus ist nicht Bestandteil der Option Bandbreitenmanagement.

3.5 Dynamisches Routing

In großen Netzwerken tragen dynamische Routing-Protokolle dazu bei, im Falle von Topologie-Änderungen ohne manuelles Eingreifen aktuelle Routing-Informationen zu verteilen. Im Rahmen der Option Dynamisches

Routing richtet der Anbieter den Firewall-Service für die Nutzung dynamischer Routing-Protokolle nach Vorgabe des Kunden ein. Die verfügbaren Routing-Protokolle sind OSPF, BGP, RIPv1/v2. Die Einrichtung oder Bereitstellung dynamischen Routings über die Option Dynamisches Routing hinaus ist nicht Bestandteil des Firewall-Service.

3.6 Reporting

Der Kunde kann den Anbieter mittels der Option Reporting damit beauftragen, ein Reporting über den beauftragten Firewall-Service bereitzustellen. Der Anbieter wird in diesem Fall wiederholt (in der Regel wöchentlich) einen solchen Report an zuvor vom Kunden hierfür benannte Personen auf elektronischem Wege bereitstellen. Der Report basiert auf einer vom Anbieter festgelegten Vorlage. Der Kunde kann Anpassungen der Vorlage gegen das hierfür in der einschlägigen Preisliste vereinbarte Entgelt beauftragen.

3.7 Firewall-Redundanz (Hochverfügbarkeits-Cluster)

Soweit eine Dezentrale Firewall vereinbart ist, kann der Kunde die Option Firewall-Redundanz (Hochverfügbarkeits-Cluster) beim dem Anbieter bestellen.

Im Rahmen dieser Option wird der Anbieter den Firewall-Service als redundanten Systemaufbau (Hochverfügbarkeits-Cluster, High Availability-Cluster, HA-Cluster) einrichten. Hierzu muss der Kunde zweimal das Produkt Dezentrale Firewall desselben Typs beauftragen. Der Anbieter stellt den Hochverfügbarkeits-Cluster als Active-/Passive-Cluster bereit. Ein Hochverfügbarkeits-Cluster setzt voraus, dass

- eine entsprechende Layer-2-Struktur (Switches) auf LAN- und WAN-Seite, sowie
- eine direkte Verbindung (Link) zwischen den beiden Hardware-Firewalls vorhanden ist.

Es obliegt dem Kunden, sicherzustellen, dass diese beiden Voraussetzungen erfüllt sind.

3.8 FortiAnalyzer Threatmanagement

Im Rahmen des Produktes FortiAnalyzer Threatmanagement stellt der Anbieter dem Kunden die zentrale Plattform Plattform FortiAnalyzer zur Anbindung an Fortigate Firewalls zur Verfügung. Innerhalb des Produkts FortiAnalyzer Threatmanagement kann der Kunde die folgenden Optionen für eine Integration von Dezentralen Firewalls bestellen:

Firewall Intergration S	Dezentrale Firewalls Typ 1-3
Firewall Intergration M	Dezentrale Firewalls Typ 4
Firewall Intergration L	Dezentrale Firewalls Typ 5

FortiAnalyzer analysiert und verarbeitet Log-Daten von Fortigate Firewalls, um Sicherheitsvorfälle zentral zu erkennen, zu bewerten und zu reagieren. FortiAnalyzer aggregiert dabei Daten, erkennt Anomalien durch Verhaltens- und Regelanalysen und nutzt global ermittelte Bedrohungsinformationen wie den Indicators of Compromise (IOC) Feed des Herstellers Fortinet, um Systeme des Kunden als kompromittiert zu identifizieren.

Integrierte Funktionen wie Outbreak Detection zeigen neue, identifizierte Bedrohungen auf, und liefern weitere Informationen wie betroffene Software und Systeme, etwa. Etwa im Hinblick auf Zero-Day-Exploits. FortiAnalyzer kann relevante Ereignisse an ein SIEM weiterleiten.

Das Produkt FortiAnalyzer Threatmanagement umfasst ein Reviewmeeting pro Quartal. Die Parteien können abweichende Intervalle vereinbaren. Im Reviewmeeting informiert der Anbieter den Kunden über den aktuellen Status des FortiAnalyzer Threatmanagements und der daran angebundenen Firewalls, die seit dem letzten Reviewmeeting als Bedrohung qualifizierten Zugriffe und mögliche Optimierungen.

4 Konfigurations- und Regelwerksänderungen

Der Kunde kann den Anbieter damit beauftragen, Änderungen an dem Regelwerk und der Konfiguration des Firewall-Services vorzunehmen. Über das hierbei einzuhaltende Verfahren informiert der Anbieter den Kunden. Im Übrigen gilt für vereinbarte Änderungen an dem Regelwerk und der Konfiguration des Firewall-Services Folgendes:

- Der Anbieter nimmt Konfigurations- und Regelwerksänderungen nur dann vor, wenn sie von den im Regelwerk aufgeführten autorisierten Personen und mit allen erforderlichen Angaben beauftragt wurden. Der Anbieter führt die vereinbarten Konfigurations- und Regelwerksänderungen während der Servicezeit (Abschnitt 9) durch.
- Aufträge über einfache Konfigurations- und Regelwerksänderungen (wie z. B. eine Anpassung einer bestehenden Regel oder Erstellung einer neuen Regel), die dem Anbieter innerhalb der Servicezeit (Abschnitt 9) vor 11 Uhr zugehen, bearbeitet der Anbieter noch am selben Tag bearbeitet.
- Vereinbarte Konfigurations- und Regelwerksänderungen stellen keine Wartung dar.
- Der Kunde hat die Durchführung der Änderung an Konfiguration oder Regelwerk gemäß der jeweils gültigen Preisliste oder, wenn die Leistung in der Preisliste nicht vorgesehen ist, nach Aufwand zu vergüten.

5 Sonstige zusätzliche Leistungen

Erbringt der Anbieter auftragsmäßig neben den vertraglich geschuldeten Leistungen weitere Leistungen, so sind diese vom Kunden gemäß der jeweils gültigen Preisliste oder, wenn die Leistung in der Preisliste nicht vorgesehen ist, nach Aufwand zu vergüten, falls nicht ausdrücklich eine entgegenstehende Vereinbarung getroffen worden ist.

6 Mitwirkungspflichten des Kunden

Der Kunden ist verpflichtet, während der Vertragslaufzeit die folgenden Voraussetzungen einzuhalten:

- Soweit eine Dezentrale Firewall vereinbart ist: Es sind sämtliche Vorgaben des Herstellers zur Aufstellung der Hardware-Firewall (wie z.B. geeignete Aufstellungsorte, Anforderungen an die Umgebung, Stromversorgung usw.) einzuhalten.
- Für die Nutzung des Firewall-Service ist ein Internetanschluss erforderlich. Dieser ist vom Kunden beizustellen. Dem Kunden obliegt es, dafür zu sorgen, dass vorgeschaltete Geräte wie z.B. Router so eingerichtet und konfiguriert sind, dass die Funktion des Firewall-Services jederzeit gewährleistet ist.

7 Verfügbarkeit

Die Zentrale Firewall und die Dezentrale Firewall sind nicht verfügbar, wenn eine Störung vorliegt.

Die Zentrale Firewall hat eine Verfügbarkeit von 99,9% im Jahresmittel. Die Dezentrale Firewall hat eine Verfügbarkeit von 98,5% im Jahresmittel. Soweit die Option Firewall-Redundanz (Hochverfügbarkeits-Cluster) vereinbart ist (Abschnitt 3.7), beträgt die Verfügbarkeit der Dezentralen Firewall 99,5%.

Bei der Berechnung der Verfügbarkeit werden die folgenden Zeiten und Ausfälle nicht berücksichtigt:

- Ausfälle durch Fehler, die im Verantwortungsbereich des Kunden liegen,
- unvermeidliche Unterbrechungen auf Grund von Änderungswünschen des Kunden,
- Ausfälle, die durch höhere Gewalt verursacht wurden,
- Ausfälle in Folge des ausdrücklichen Wunsches des Kunden, die Störung nicht zu beheben,
- Ausfälle auf Grund geplanter oder vereinbarter Unterbrechungen in Folge von Wartungsarbeiten des Anbieters und
- Zeitverluste, die nicht vom Anbieter verschuldet sind.

8 Servicezeit

Die Servicezeit verläuft von Montag bis Freitag (gesetzliche Feiertage am Sitz des Anbieters ausgenommen), jeweils von 8 bis 17 Uhr.

9 Störungen

Treten im Betrieb des Firewall-Service Störungen auf, obliegt es dem Kunden, dem Anbieter diese Störungen unverzüglich mitzuteilen. Der Anbieter nimmt Störungsmeldungen täglich rund um die Uhr entgegen. Über einen durch den Anbieter verursachten Ausfall informiert der Anbieter den Kunden unverzüglich.

9.1 Entstörzeit

Die Entstörzeit beträgt 24 Stunden nach Meldung der Störung durch den Kunden, soweit Technik des Anbieters betroffen ist. Im Fall höherer Gewalt oder bei Störungen, die von Zulieferern des Anbieters verursacht werden, kann die Entstörzeit überschritten werden. Verzögerungen durch mangelnde Mitwirkung des Kunden werden auf die Entstörzeit nicht angerechnet.

9.2 Behebung von Störungen

Die Störung gilt als behoben, wenn der Anbieter sie gegenüber dem Kunden abgemeldet hat oder wenn die Funktionalität wieder hergestellt ist und der Kunde die vertragliche Dienstleistung wieder nutzen kann.

9.3 Vom Kunden zu vertretende oder nicht vorhandene Störungen

Hat der Kunde die Störung zu vertreten oder liegt eine vom Kunden gemeldete Störung nicht vor, ist der Anbieter berechtigt, dem Kunden die ihm durch die Entstörung bzw. den Entstörversuch entstandenen Kosten gemäß der jeweils gültigen Preisliste oder, wenn die Leistung in der Preisliste nicht vorgesehen ist, nach Aufwand in Rechnung zu stellen.

10 Wartungsarbeiten

Der Anbieter führt nach eigenem Ermessen Wartungen durch.

Wartungsarbeiten des Anbieters können eine geplante Unterbrechung des Firewall-Service bewirken. Der Anbieter wird den Kunden rechtzeitig im Voraus über Wartungsarbeiten informieren. In dringenden Fällen kann eine ungeplante Wartung ohne vorherige Information des Kunden notwendig sein.

Soweit eine **Dezentrale** Firewall vereinbart ist, gilt:

Die Dezentrale Firewall unterstützt automatische Updates. Kleinere Fehlerkorrekturen und Sicherheitsupdates werden automatisch und ohne manuellen Eingriff eingespielt. Die automatischen Updates erfolgen ohne Ankündigung ausschließlich nachts, um den laufenden Betrieb so wenig wie möglich zu beeinträchtigen. Der Kunde hat die Möglichkeit, diese Funktion auf Anfrage deaktivieren zu lassen (Opt-Out für automatische Updates).

Stand: 20. März 2025