LEISTUNGSBESCHREIBUNG

Managed Security: Dezentrale Firewall für Geschäftskunden

1 Allgemeines

Die EWE TEL GmbH (im Folgenden Anbieter genannt) erbringt die nachfolgend beschriebene Dienstleistung Managed Security: Dezentrale Firewall (im Folgenden Firewall-Service genannt) 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 des Firewall-Service

Der Firewall-Service umfasst die Bereitstellung, die Konfiguration, die Wartung und das Management einer Hardware-Firewall. Für die Bereitstellung 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. Die Einrichtung oder Bereitstellung eines Internetzugangs ist 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 Konfiguration und Regelwerk des Firewall-Service

Der Anbieter übergibt dem Kunden eine Dokumentation über die Konfiguration und das Regelwerk des Firewall-Service in elektronischer Form. Der Anbieter stellt dem Kunden ein Verfahren zur Verfügung, kostenpflichtige Konfigurations- und Regelwerksänderungen beim Anbieter zu beauftragen. Der Kunde selbst kann keine eigenständige Konfiguration des Firewall-Service vornehmen.

1.4 Wirkungsbereich des Firewall-Service

Der Firewall-Service kann nur solchen Datenverkehr kontrollieren, 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 schadhaften Bedrohungen erreichen kann. Der Firewall-Service kann nicht

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

2 Basisleistungen

Der Firewall-Service besteht aus einer Basisleistung und kostenpflichtigen optionalen Leistungen (s. Abschnitt 3). Mit der Basisleistung werden mögliche Angriffe, die sich auf IP/ICMP (Netzwerk-Layer, OSI-Layer 3) oder TCP/UDP (Transport-Layer, OSI-Layer 4) beziehen, im Rahmen der technischen Möglichkeiten innerhalb des Firewall-Service erkannt und abgewehrt. Dies gilt für Angriffe auf den Firewall-Service selbst und auf die zu schützenden IPNetze. Die Basisleistung des Firewall-Service bietet keinen Schutz vor Angriffen auf Anwendungsebene (OSI-Layer 5 bis 7). Nicht Bestandteil der Basisleistung sind alle in Abschnitt 3 aufgeführten optionalen Leistungen.

2.1 Implementierung des Firewall-Service

Der Firewall-Service wird als Hardware-Firewall zwischen das zu schützende 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. Für die Implementierung des Firewall-Service wird jeweils eine IP-Adresse aus den angeschlossenen IP-Netzen des Kunden für den Firewall-Service bereitgestellt. Soweit nicht anders vereinbart, verfügt die Hardware-Firewall über mindestens vier FastEthernet-Schnittstellen (10/100 BaseT gemäß IEEE802.3) zum Anschluss des IP-Netz des Kunden, des Internets oder einer demilitarisierten Zone.

2.2 Daten-Durchsatz des Firewall-Service

Der Daten-Durchsatz des Firewall-Service entspricht der in dem Auftragsformular vereinbarten Bandbreite. Wenn nicht anders vereinbart ist, verfügt der der Firewall-Service einen Daten-Durchsatz von 6 Mbit/s.

2.3 Network Address Translation/Port Address Translation

Bei Bedarf kann der Firewall-Service an jeder Netzwerkschnittstelle Network Address Translation (NAT) oder Port Address Translation (PAT) einsetzen. NAT und PAT kann für eingehende und ausgehende Verbindungen konfiguriert werden. Es steht statisches und dynamisches NAT zur Verfügung.

2.3.1 Dynamisches Network Address Translation

Dynamisches NAT kann verwendet werden, wenn es sich bei den IPv4-Adressen im IP-Netz des Auftraggebers um private IPv4-Adressen nach RFC-1918 handelt oder die IPv4-Adressen aus dem offiziellen Adressraum des Internets stammen, aber einem anderem Autonomen System (AS) zugeordnet sind, das nicht vom Kunden und/oder dem Anbieter betrieben wird.

2.3.2 Statisches Network Address Translation

Statisches NAT kann verwendet werden, wenn externe IPv4-Adressen auf interne IPv4-Adressen abgebildet werden müssen, um einen Zugriff auf interne Ressourcen des Kunden (z.B. Webserver, Mailserver) zu ermöglichen.

2.3.3 Port Address Translation für ausgehende Datenpakete

Port Address Translation für ausgehende Datenpakete wird in Verbindung mit NAT eingesetzt, wenn mehrere private IPv4-Adressen in einem LAN zu einer öffentlichen IPv4-Adresse übersetzt werden sollen.

2.3.4 Port Address Translation für eingehende Datenpakete

Bei Port Address Translation für eingehende Datenpakete können je nach angesprochenem Port verschiedene IPv4-Adressen über eine öffentliche IPv4-Adresse erreicht werden.

2.4 Firewall-Regelwerk

Der Anbieter führt gemeinsam mit dem Kunden einen Consulting-Termin durch. Soweit nicht ausdrücklich anders vereinbart, findet der Termin telefonisch statt. In diesem Termin werden die gewünschten Firewall-Regeln sowie die gewünschte Konfiguration des Firewall-Service festgelegt und in einem Regelwerk elektronisch dokumentiert. Als Vorbereitung für den Consulting-Termin definiert der Kunde seine Kommunikationsbeziehungen, die durch den Firewall-Service geprüft werden sollen. Der Anbieter wird den Firewall-Service auf Basis des mit dem Kunden abgestimmten Regelwerks konfigurieren. Hierbei gilt ein Limit von 100 Firewall-Regeln je Firewall-Service. Weitere Firewall-Regeln können entsprechend der gültigen Preisliste hinzugekauft werden.

2.5 Abnahme des Firewall-Service

Der Anbieter sendet dem Kunden die beauftragte Hardware-Firewall zu und stellt ein Anschlusskabel für die Spannungsversorgung zur Verfügung. Die Installation der Hardware- Firewall erfolgt, soweit nicht ausdrücklich etwas anders vereinbart ist, durch den Kunden. Der Kunde informiert den Anbieter über die abgeschlossene Installation, sodass der Anbieter den Firewall-Service in Betrieb nehmen kann. Nach Inbetriebnahme des Firewall-Service durch den Anbieter stellt der Anbieter dem Kunden das Regelwerk elektronisch zur Verfügung und fordert 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 Werktragen abgenommen hat, obwohl er dazu verpflichtet ist. Das bereitgestellte Firewall-Regelwerk bildet die Basis für den Betrieb des Firewall-Service. Stellt der Kunden innerhalb von 10 Werktagen nach Inbetriebnahme des Firewall-Service fest, dass die im Rahmen des Consulting-Termins ermittelten Firewall-Regeln (s. Abschnitt 2.4) unvollständig oder fehlerhaft sind, wird der Anbieter die Firewall-Regeln entsprechend erweitern oder korrigieren. Die vorgesehene Frist von 10 Werktagen zur Abnahme verlängert sich hierdurch nicht.

2.6 Management des Firewall-Service

Der Firewall-Service wird durch den Anbieter via Fernzugriff gemanagt und überwacht. Dem Kunden obliegt es, sicherzustellen, dass der Firewall-Service über die Wide Area Network (WAN) Anbindung ständig erreichbar ist. Im Rahmen des Managements des Firewall-Service übernimmt der Anbieter die Funktionsüberwachung, das Backup der Konfiguration sowie die Software- und Hardwarepflege wie z.B. das Einspielen von Patches oder die Durchführung von Reparaturen. Die Einrichtung oder Bereitstellung des WAN-Zuganges für das Management des Firewall-Service ist nicht Bestandteil des Firewall-Service.

2.7 Demilitarisierte Zone

Der Kunde hat die Möglichkeit, über den Firewall-Service ein zweites vom LAN des Kunden getrenntes Netzwerk als eine demilitarisierte Zone (DMZ) anzuschließen. Eine DMZ kann zum Betrieb von Systemen und Diensten (wie z.B. E-Mail-, Web- und DNS-Server), die sowohl aus dem Internet als auch dem LAN des Kunden erreichbar sein sollen, verwendet werden. Im Rahmen ihres Wirkungsbereiches (Abschnitt 1.4) kann der Firewall-Service die in der DMZ aufgestellten Systeme gegen unerwünschte Zugriffe aus dem Internet und dem LAN des Kunden absichern. Mit Hilfe dieser Trennung kann der Kunden z.B. den Zugriff auf seine öffentlich erreichbaren Dienste gestatten und gleichzeitig sein LAN vor unerwünschten Zugriffen aus dem Internet schützen.

3 Optionale Leistungen

Der Anbieter bietet optionale Leistungen für erweiterte Sicherheitsfunktionen des Firewall-Service an. Die optionalen Leistungen sind bei oder nach Beauftragung des Firewall-Service buchbar und gemäß der jeweils gültigen Preisliste

Stand: 11/18 LB_GK_DZFW_s_04_011118

oder, wenn die Leistung in der Preisliste nicht vorgesehen ist, entsprechend des individuellen Angebots zu vergüten. Der Anbieter richtet beauftragte Optionen nach Vorgabe des Kunden und abhängig von den technischen Möglichkeiten ein. Nachfolgende optionale Leistungen stehen hierbei zur Verfügung:

- Unified Threat Management (Abschnitt 3.1),
- Secure Remote Access (Abschnitt 3.2),
- IPSec-VPN (Abschnitt 3.3),
- Bandbreitenmanagement (Abschnitt 3.4),
- Dynamisches Routing (Abschnitt 3.5),
- Erweitertes Firewall-Regelwerk (Abschnitt 3.6),
- Reporting (Abschnitt 3.7),
- Zusätzliche Netzwerksegmente (Abschnitt 3.8) und
- Hochverfügbarkeits-Cluster (Abschnitt 3.9).

3.1.1 Unified Threat Management

Unified Threat Management (UTM) bezeichnet die Vereinigung verschiedener Sicherheitsaufgaben auf einer Plattform. Dazu gehören:

- UTM-Antivirus (Abschnitt 3.1.2),
- UTM-Antispam (Abschnitt 3.1.3),
- UTM-Webfilter (Abschnitt 3.1.4),
- UTM-Contentfilter (Abschnitt 3.1.5) und
- UTM-Intrusion Prevention (Abschnitt 3.1.6).

UTM kann die gewünschten Funktionen nur erfüllen, wenn die im Folgenden aufgeführten UTM-Funktionen durch automatisch eingespielte Updates ständig auf dem neusten Stand gehalten werden. Der Anbieter ist für das Einspielen der Updates verantwortlich und wird diese zeitnah einspielen, sobald der Hersteller der eingesetzten Hardware-Firewall ein Update zur Verfügung stellt. Der Anbieter hat keinerlei Einfluss auf die Bereitstellung von Updates durch den Hersteller.

3.1.2 UTM – Antivirus

Antivirus (AV) bietet die Option, Computerviren auf Dateibasis zu erkennen und vor diesen zu schützen. Die Virenerkennung beschränkt sich dabei auf diejenigen Viren und Dateiformate, die dem in dem Firewall-Service eingesetzten Virenscanner bekannt sind. Für die Erkennung prüft die Firewall den Netzwerkverkehr auf entsprechende Dateiübertragungen. Die Prüfung erfolgt nur innerhalb der Protokolle SMTP, POP3, IMAP, HTTP und FTP. Der Einsatz von AV im Firewall-Service stellt keinen adäquaten Ersatz für eine clientbasierte Desktop-Antiviren-Software dar, sondern ist als Teil einer gesamten Sicherheitsstrategie zu sehen. Die Einrichtung oder Bereitstellung von AV über den Firewall-Service hinaus ist nicht Bestandteil des Firewall-Service.

3.1.2.1 Standard-AV-Scan

Auf Wunsch des Kunden richtet der Anbieter einen Standard-AV-Scan für ein- und/oder ausgehende Verbindungen ein. Mit dieser Einstellung speichert der Firewall-Service bei einer erkannten Dateiübertragung die Datei zwischen und prüft diese auf schadhaften Quellcode (Viren, Trojaner, Rootkits, Keylogger, Spyware, Adware). Durch das Zwischenspeichern der Datei kann es zu Verzögerungen der Datenübertragung kommen. Im Gegenzug bietet der Standard-AV-Scan eine hohe Erkennungsrate von schadhaftem Quellcode. Komprimierte Dateien können bis zur vierten Kompressionsebene entpackt und überprüft werden. Wird schadhafter Quellcode erkannt, unterbricht der Firewall-Service die Dateiübertragung und informiert den Benutzer über die erkannte Bedrohung. Der Firewall-Service kann zwei Dateien gleichzeitig, jedoch keine verschlüsselten oder passwortgeschützten Dateien oder Dateien mit mehr als 4 Kompressionsebenen, überprüfen. Die Anzahl der gleichzeitig prüfbaren Dateien sowie die Dateigröße sind jedoch abhängig von dem verfügbaren Speicher und der verfügbaren CPU-Leistung der Hardware-Firewall. Es obliegt dem Kunden, festzulegen, wie der Firewall-Service mit Dateien umgehen soll, die nicht überprüft werden können.

3.1.2.2 Stream-AV-Scan

Der Anbieter kann, abhängig von der eingesetzten Hardware-Firewall, anstelle des Standard-AV-Scans alternativ ein Stream-Scanning einrichten. Bei dem Stream-AV-Scan wird der Datenstrom während der Dateiübertragung auf schadhaften Quellcode überprüft. Im Vergleich zum Standard-AV-Scan treten geringere Verzögerungen während der Datenübertragung auf. Die Erkennungsrate ist jedoch geringer. Der Firewall-Service kann keine verschlüsselten oder passwortgeschützten Dateien, sowie komprimierte Dateien nur bei Übertragung in den Protokollen POP3 und HTTP und nur bis zur ersten Kompressionsebene überprüfen.

3.1.3 UTM – Antispam

Antispam (AS) bietet die Möglichkeit, unerwünschte E-Mails wie z.B. massenhaft zu Werbezwecken oder in Betrugsabsicht versandte E-Mails oder E-Mails mit schadhaftem Quellcode zu erkennen und daraufhin zu blockieren oder zu markieren. Die Erkennung erfolgt hierbei IPbasiert auf Basis einer Spam Block List (SBL), die vom Hersteller der Hardware-Firewall bereitgestellt wird. Der Anbieter kann nach Vorgabe des Kunden, basierend auf Domänen-Name, E-Mail-Adresse oder IP-Adresse, zusätzlich eine White- und/oder Blacklist einrichten. Sowohl die White- als auch die Blacklist (Erlauben und Verbieten) ist auf 20 Einträge beschränkt. Der Kunde definiert, ob der Firewall-Service eine als Spam erkannte E-Mail blockiert oder markiert werden soll. Eine Markierung erfolgt durch Hinzufügen einer Zeichenkette im Betreff oder Header der Nachricht. Der Kunde definiert die zu verwendende Zeichenkette (z.B. ***SPAM***).

3.1.4 UTM – Webfilter

Mit Hilfe des Webfilters (WF) kann der Zugriff auf bestimmte Internetseiten individuell oder nach Kategorie zugelassen oder unterbunden werden. Der Kunde kann dadurch die Nutzung von Internetseiten auf das für seine betrieblichen oder sonstigen Zwecke erforderliche Maß einschränken. Die Nutzung des WF kann beim Aufruf einer Internetseite zu einer kurzen Verzögerung der Datenübertragung führen, in der der Firewall-Service die angefragte Internetseite kategorisiert. Wird eine Internetseite aufgerufen, die gemäß den Vorgaben nicht erlaubt ist, erhält der Benutzer eine Meldung über den nicht zugelassenen Zugriff. Der Anbieter richtet den WF nach Vorgabe des Kunden ein. Hierbei können White- und/oder Blacklists und/oder Kategorien zur Filterung eingesetzt werden. Bei der Filterung werden White- und Blacklists vorrangig gegenüber Kategorien berücksichtigt. Die Einrichtung von White- und/oder Blacklists beschränkt sich auf zwei Listen (Erlauben und Verbieten) und ist je Liste auf 20 Einträge beschränkt. Die Einträge können auf URL- oder IP-Basis erfolgen. Die Anwendung von Kategorien ist auf die bereitgestellten Kategorien des Herstellers der Hardware-Firewall beschränkt. Der Anbieter hat weder Einfluss auf die vom Hersteller der Hardware-Firewall bereitgestellten Kategorien noch darauf, welche Internetseiten in welche Kategorien eingeteilt werden.

3.1.5 UTM – Contentfilter

Der Contentfilter (CF) erlaubt oder verbietet bestimmte Datenübertragungen, basierend auf den folgenden Kriterien:

- MIME-Typ (z.B. video, image, audio),
- Dateierweiterung (z.B. .exe, .bat),
- Protokollbefehl (z.B. put, get, list) oder
- eingebettetes Objekt (z.B. ActiveX, Java Applet, Cookie).

Dabei ist der CF auf die Protokolle SMTP, POP3, IMAP, HTTP und FTP beschränkt. Für das Protokoll HTTP kann der Anbieter Filter auf Basis der vorgenannten Kriterien einrichten. Bei FTP ist der Filter auf Dateierweiterungen und Protokollbefehle beschränkt. Bei den E-Mail-Protokollen (SMTP, POP3 und IMAP) besteht nur eine begrenzte Filtermöglichkeit basierend auf MIME-Typen, Dateierweiterung und Protokollbefehlen, abhängig davon, wie viele E-Mail-Header eine Nachricht enthält (unterstützt wird nur ein Ebene). Wird eine Datenübertragung basierend auf den Vorgaben blockiert, wird der Benutzer anhand einer Benachrichtigung informiert.

3.1.6 UTM – Intrusion Prevention

Angriffe können Schwachstellen in Computer-Programmen oder Hardware ausnutzen. Solche Angriffe erfolgen i.d.R. auf OSI-Layer 5 bis 7 und werden von einem Firewall-Service ohne UTM nicht erkannt (s. Abschnitt 2). Durch Intrusion Prevention (IPS) werden Angriffe auf OSILayer 5 bis 7 im Rahmen der technischen Möglichkeiten und anhand eines IPS-Regelsatzes erkannt und verhindert. Der Anbieter richtet den IPS-Regelsatz nach Vorgabe des Kunden ein. Der IPS-Regelsatz besteht aus Signaturen, die vom Hersteller der Hardware-Firewall zu Kategorien zusammengefasst werden. Der Anbieter hat keinen Einfluss auf die vom Hersteller der Hardware-Firewall bereitgestellten Signaturen und Kategorien.

3.2 Secure Remote Access

Über Secure Remote Access (SRA) stellt der Firewall-Service mobilen Benutzern einen sicheren Fernzugriff über das Internet auf Ressourcen innerhalb des IP-Netzes des Kunden bereit. Der Fernzugriff erfolgt über einen vom Firewall-Service bereitgestellten Client in Form eines Webinterface. An dem Webinterface können sich berechtigte Benutzer authentifizieren. Der Kunde hat die Möglichkeit, Benutzer in Gruppen gleicher Berechtigungen zusammenzufassen (z.B. Administratoren, Vertrieb). Die Zugriffsrechte können nach Anforderungen der jeweiligen Benutzergruppe über ein Regelwerk definiert werden. Die maximale Anzahl gleichzeitig verbundener Benutzer über SRA wird durch die beauftragte Leistung beschränkt. Der Anbieter legt die Benutzer nach Vorgabe des Kunden auf dem Firewall-Service an und authentifiziert die Benutzer gegen den Firewall-Service. Die Zuweisung einer IP-Adresse (lokal auf einem IP-Pool), DNS-Server-Adresse und/oder WINS-Server-Adresse ist möglich.

3.3 IPSec-VPN

Bei Vernetzung von Standorten über das Internet kann der Anbieter den Firewall-Service nach Vorgabe des Kunden über ein IPSec-VPN im Tunnelmodus mittels IKE/ESP (Site-to-Site) einrichten. Dadurch wird bei der Übertragung von Daten bezüglich Vertraulichkeit, Authentizität und Integrität ein hohes Maß an Sicherheit gewährleistet. Die Gegenstelle bei der Übertragung von Daten kann hierbei vom Anbieter, vom Kunden oder von Dritten bereitgestellt werden. Die Einrichtung oder Bereitstellung von Hard- oder Software auf Seiten der Gegenstelle ist nicht Bestandteil des Firewall-Service.

3.4 Bandbreitenmanagement

Im Rahmen des Bandbreitenmanagements konfiguriert der Anbieter den Firewall-Service nach Vorgabe des Kunden so, dass bestimmte Bandbreiten für vom Kunden definierten Datenverkehr reserviert werden (Traffic-Shaping). Der Anbieter stellt sicher, dass die vom Kunden definierten Einstellungen innerhalb des Firewall-Service Anwendung finden. Für ein durchgängiges Bandbreitenmanagement (Quality of Service) sind jedoch alle an der Übermittlung von IP-Paketen beteiligten aktiven Netztechniken entsprechend vom Kunden einzurichten. Die Einrichtung oder Bereitstellung solcher Netztechniken über den Firewall-Service hinaus ist nicht Bestandteil des Firewall-Service.

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. Der Anbieter kann den Firewall-Service für die Nutzung dynamischer Routing-Protokolle nach Vorgabe des Kunden einrichten. Die verfügbaren Routing-Protokolle sind OSPF, BGP, RIPv1/v2. Die Einrichtung oder Bereitstellung dynamischen Routings über den Firewall-Service hinaus ist nicht Bestandteil des Firewall-Service. 3.6 Erweitertes Firewall-Regelwerk Das erweiterte Firewall-Regelwerk bietet in komplexen Umgebungen die Möglichkeit, über das in Abschnitt 2.4 definierte Limit für Firewall-Regeln hinaus jeweils 50 weitere Regeln zu beauftragen.

3.7 Reporting

Der Kunde kann den Anbieter damit beauftragen, ein Reporting über den beauftragten Firewall-Service bereitzustellen. Der Anbieter wird in diesem Fall wiederholt (in der Regel wöchentlich) einen Report frei wählbaren Personen oder Personenkreisen des Kunden 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. Durch eine Verknüpfung der Inhalte des Reports mit weiteren Daten des Kunden kann ggf. ein Personenbezug hergestellt werden. In diesem Fall obliegt es dem Kunden als verantwortliche Stelle, die sich hieraus ergebenden datenschutzrechtlichen oder mitbestimmungsrechtlichen Pflichten zu beachten.

3.8 Zusätzliche Netzwerksegmente

Neben dem LAN, WAN und der DMZ kann der Firewall-Service vom Anbieter für weitere Netzwerksegmente konfiguriert werden. Diese Anbindung weiterer Netzwerke kann physikalisch oder logisch vorgenommen werden. Die physikalische Anbindung setzt voraus, dass auf der Hardware-Firewall eine entsprechende Anzahl an erforderlichen Ports zur Verfügung steht. Die logische Anbindung an ein Netzwerk erfolgt mittels Virtual Local Area Network (VLAN) gemäß IEEE 802.1q. Für die logische Anbindung aufseiten des Kunden ist ein VLANfähiger Switch erforderlich. Der Switch ist nicht Bestandteil des Firewall-Service. Durch das Anbinden zusätzlicher Netzwerksegmente kann der Daten-Durchsatz durch den Firewall-Service steigen. Es obliegt dem Kunden, einen ausreichenden Daten-Durchsatz (Abschnitt 2.2) zu beauftragen.

3.9 Hochverfügbarkeits-Cluster

Der Anbieter kann den Firewall-Service als Hochverfügbarkeits-Cluster (High Availability, HA) einrichten. Hierzu muss der Kunde zwei Firewall-Services gleichen Typs beauftragen. Der Anbieter stellt den Cluster als Active-/Passive-Cluster bereit. Voraussetzung für ein Cluster ist eine entsprechende Layer-2-Strukur (Switche) auf LAN- und WAN-Seite, sowie ein direkter Link (HA-Link) zwischen den beiden Hardware-Firewalls. Für den HA-Link wird je ein Port auf beiden Hardware-Firewalls benötigt; diese Ports stehen damit nicht mehr für die Anbindung von Netzwerken zur Verfügung. Die Einrichtung oder Bereitstellung entsprechender Layer-2-Strukturen oder Netzwerkkabel für den HA-Link ist nicht Bestandteil des Firewall-Service.

4 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.

5 Konfigurations- und Regelwerksänderungen

Der Kunde kann den Anbieter damit beauftragen, Änderungen an dem Regelwerk und der Konfiguration des Firewall-Service vorzunehmen. Über das hierbei einzuhaltende Verfahren informiert der Anbieter den Kunden. Der Anbieter nimmt Änderungen an Konfiguration oder Regelwerk nur dann vor, wenn sie von den im Regelwerk aufgeführten autorisierten Personen und mit allen erforderlichen Angaben beauftragt wurden. Der Anbieter führt vereinbarte Änderungen an Konfiguration oder Regelwerk innerhalb von zwei Werktagen durch, sofern keine Rücksprache mit dem Kunden notwendig ist; solche Änderungen 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. Ausgenommen hiervon sind Änderungen nach Abschnitt 2.5.

6 Aufstellungsort der Hardware-Firewall

Während der Nutzung des Firewall-Service hat der Auftraggeber folgende Parameter bei der Aufstellung der Hardware-Firewall einzuhalten:

- Sicherstellung einer dauerhaften Spannungsversorgung,
- Vermeidung von direkter Sonneneinstrahlung und übermäßiger Staubentwicklung,
- Verhinderung von Wärmeentwicklung durch Heizkörper oder andere wärmeentwickelnden Geräte,
- Sicherung der Hardware-Firewall gegen Blitzschlag und Überspannung mittels geeigneter technischer Einrichtungen,
- Raumlufttemperatur von 10-30° Celsius,
- rel. Luftfeuchtigkeit von 10-90%, nicht kondensierend,
- Spannungsversorgung von 230V, 50-60 Hz und
- maximale Leistungsaufnahme von 60 bis 150 Watt (abhängig von der eingesetzten Hardware-Firewall).

7 Störungen

Treten im Betrieb des Firewall-Service Störungen auf, obliegt es dem Kunden, dem Anbieter diese Störungen unverzüglich mitzuteilen.

7.1 Entstörfrist

Die Entstörfrist 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 Entstörfrist überschritten werden. Verzögerungen durch mangelnde Mitwirkung des Kunden werden auf die Entstörfrist nicht angerechnet.

7.2 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.

7.3 Eigenverschulden

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.

8 Wartungsarbeiten

Wartungsarbeiten des Anbieters können eine geplante Unterbrechung der vertraglichen Dienstleistung 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.

9 Verfügbarkeit

Der Firewall-Service hat eine Verfügbarkeit von 98,5% im Jahresmittel. Durch Bildung eines Hochverfügbarkeits-Clusters (Abschnitt 3.9) kann die Verfügbarkeit auf 99,5% erhöht werden. Folgende Zeiten und Ausfälle werden in der Verfügbarkeitsberechnung nicht berücksichtigt:

- Die Entstörfrist (Abschnitt 7.1),
- 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 oder des Kunden und
- Zeitverluste, die nicht vom Anbieter verschuldet sind.

10 Sicherheit der Daten

Der Anbieter unternimmt alle angemessenen und zumutbaren Schritte, um größtmögliche Datensicherheit zu gewährleisten und den Zugriff von unberechtigten Dritten zu unterbinden, soweit es im Rahmen der gängigen Methoden technisch möglich ist. Der Anbieter kann jedoch nicht für Fehler haftbar gemacht werden, die vom Kunden oder von Dritten verursacht wurden.

Stand: 01.11.2018

Stand: 11/18 LB_GK_DZFW_s_04_011118