Leistungsbeschreibung Tech-Prax Hardware Firewall (auf Basis Securepoint Black Dwarf as A Service)

1. Einleitung

Die Tech-Prax GmbH stellt dem Kunden über Securepoint die Firewall Securepoint Black Dwarf as A Service zur Verfügung. Der Firewall-Service ist beschrieben in §1.4 Sicherheitspaket Firewall – Black Dwarf Black Dwarf as A Service. Telefonsupport ist dabei kostenpflichtig. Für die Standardkonfiguration ist Grundlage die von Tech-Prax definierte Grundkonfiguration (siehe 4.2), sowie die vom Kunden beauftragten individuellen Regeln, gemäß vom Kunden übersendeter Regeln.
Der Umfang der insgesamt vertraglich vereinbarten Leistungen ergibt sich aus dieser Leistungsbeschreibung und ggfs. weiteren Leistungsbeschreibungen der vom Auftraggeber bestellten Leistungen sowie aus den Allgemeinen Geschäftsbedingungen der Tech-Prax GmbH.

2. Zuständigkeiten

Bei Erteilung des Auftrags wird definiert, wer zukünftig Ansprechpartner für den Kunden ist. Dabei wird zwischen Tech-Prax und einem von Tech-Prax zertifizierten Vertriebs- und Servicepartner unterschieden. Es ist zu beachten, dass hierdurch Unterschiede in den Preislisten entstehen können. Gültig ist jeweils die aktuelle Preisliste des im Auftrag definierten Ansprechpartners. Tech-Prax behält sich zudem das Recht vor, externe Dienstleister mit Service und Support zu beauftragen. Diese sind an die jeweils gültige Fassung der Tech-Prax Preisliste gebunden.

3. Funktionsumfang der Firewall

Der Funktionsumfang der Firewall (u. a. DPI, IPSec, Antivirus, Antispam, Contentfilter) ist über die Herstellerwebsite von Securepoint (https://www.securepoint.de/produkte/utm-firewalls/funktionsumfang.html) einzusehen und ist abhängig von dem eingesetzten Modell (Black Dwarf UTM as A Service). Tech-Prax gibt keine Garantie für die Verwendung und Funktionstüchtigkeit einzelner Komponenten. Die Firewall wird von Securepoint eingesetzt und unterliegt daher den Bestimmungen der Securepoint GmbH (https://www.securepoint.de/fileadmin/securepoint/downloads/leistungsbeschreibungen/securepoint-black-dwarf-aas-leistungsbeschreibung.pdf).

Auszug:

Leistungselemente
Die folgenden Leistungen sind während der gesamten Vertragslaufzeit Teil von Securepoint Black Dwarf as A Service.

Securepoint NextGen UTM-Firewall
Das Paket umfasst die Securepoint NextGen UTM-Firewall Software inkl. notwendigen Infinity-Lizenzen. Der Leistungsumfang der Securepoint NextGen UTM Firewall Software ist auf der Homepage des Herstellers www.securepoint.de zu finden und bezieht sich auf die jeweils gültige neueste Softwareversion. Die Black Dwarf as a Service Firewall ist für Netzwerke mit bis zu 10 Benutzern geeignet.

Weitere Leistungsinformationen finden Sie hier: https://securepoint.de/utm-features

Die Benutzung alter Programmversionen ist nicht möglich und wird nicht unterstützt.

Securepoint Black Dwarf Hardware

- Firewall-Hardware zur Ausbringung an den im Vertrag benannten Endkunden. Die Firewall-Hardware hat mindestens folgende Leistungsmerkmale:
- Firewall Durchsatz: >500Mbit
- Ethernet (RJ45) Anschlüsse: 2x Ethernet RJ45 mit 1 GBit
- Wireless-LAN: WLAN 802.11ac
- Monitoranschluss: HDMI/VGA
- USB: vorhanden
- Formfaktor: Mini-Desktop
- Geeignet für Netzwerke bis zu 10 Benutzer.
- Die Hardware bleibt Eigentum der Securepoint GmbH und muss nach Vertragsende auf eigene Kosten

zurückgeschickt werden (inkl. Zubehör und Originalverpackung).

Securepoint Vorabaustausch-Service PLUS (VAT+)

Bei defekten wird dem Partner eine Austauschhardware zum Tausch beim Endkunden zur Verfügung gestellt. Den Austausch der Hardware übernimmt der Reseller bei seinem Endkunden selbständig.

Die genauen VAT+ Vertragsbedingungen sind in der Servicekarte für VAT+ benannt.

Securepoint behält sich vor proaktiv zu tauschen. Der Vorteil für den Kunden ist eine kürzere und geplante Ausfallzeit, als sie beim Tausch wegen eines Defekts auftreten würde. Der Tausch wird vorab mit dem Kunden besprochen.

4. Bereitstellung: Installation und PolicyKonfiguration

4.1 Basisinstallation

Die Basisinstallation findet nach Absprache Werktags zwischen 8 und 18 Uhr statt. Außerhalb dieses Zeitfensters wird ein Aufschlag berechnet. Der Installationstermin muss dabei, seitens des Kunden, so gewählt / abgestimmt werden, dass der ausführende Techniker seine Tätigkeiten unterbrechungsfrei durchführen kann. Eine Garantie für die Umsetzung von Terminwünschen kann nicht zugesprochen werden, allerdings ist Tech-Prax stets bemüht, auf die Wünsche des Auftraggebers einzugehen. Im Vorfeld der Installation wird es ggfs. zu einer Kontaktaufnahme durch den Installationsdienstleister kommen, um eine Vorqualifikation mit dem Kunden durchzuführen. Diese dient dem Zweck den Betriebsablauf am Tag der eigentlichen Installation, möglichst wenig zu stören, indem mittels der durch den Auftraggeber bekanntgegebenen Informationen eine Vorkonfigurierung der Hardware erfolgt. Bestandteile der Basisinstallation sind die Anfahrt innerhalb des deutschen Festlands, sowie Einbindung und Inbetriebnahme der Firewall in das Netzwerk des Kunden. Anschließend wird eine Grundkonfiguration, sowie das Installieren der notwendigen Sicherheitszertifikate durchgeführt. Um diese Sicherheitszertifikate einspielen zu können, muss dem Techniker Zugang zu den Clients gewährt werden. Für den Fall, dass es dabei zu, durch den Kunden verschuldeten, Verzögerungen kommt, behält Tech-Prax, bzw. der zertifizierte Vertriebs- und Servicepartner, sich das Recht vor, die Mehraufwände gemäß Preisliste zu fakturieren. Die Einrichtung der Firewall als Einwahlrouter für den Online-Zugang ist nicht Bestandteil. Seitens des Auftraggebers muss sichergestellt sein, dass die Voraussetzungen für den Betrieb der Firewall erfüllt sind. Für die Basisinstallation steht ein vordefiniertes Zeitkontingent zur Verfügung, welches dem jeweils zugrundeliegenden Teilnahmeantrag zu entnehmen ist. Ist dies nicht der Fall, behält Tech-Prax bzw. der zertifizierte Vertriebs- und Servicepartner sich das Recht vor, die Installation abzubrechen und in Rechnung zu stellen. Nach erfolgter Einrichtung wird stichprobenartig eine Kontrolle der FirewallPolicy durchgeführt.

4.2 Grundkonfiguration

Die Grundkonfiguration beinhaltet den Anschluss der Firewall im Netzwerk des Kunden in Reihenschaltung (zzgl. Materialien wie LAN Kabel oder Switch). Folgende Firewallregeln werden dabei standardmäßig konfiguriert:

Firewallregeln [Gruppen + Protokolle] internal-network -> Internet

1. Telematik
   - HTTPS-alt (TCP 8443)
   - LDAPS (TCP-636)

2. Default-internet
   - domain-UDP (UDP-53)
   - FTP (TCP-21)
   - HTTP (TCP-80)
   - HTTPS (TCP-443)
   - ICMP-echo-req (ICMP-8)

3. DNS
   - domain-TCP (TCP-53)
   - domain-UDP (UDP-53)

4. network-time
   - NTP-TCP (TCP-123)
   - NTP-UDP (UDP-123)

5. IPsec
    - isakmp (UDP-500)
    - NAT-traversal (UDP-4500)
    - ESP

6. Mail
    - IMAP-SSL (TCP-993)
    - SMTPS (TCP-465)
    - POP3S (TCP-995)
    - submission (TCP-587)

7. Teamviewer
    - Teamviewer_TCP (TCP-5938)
    - Teamviewer_UDP (UDP-5938)

Firewallregeln [Gruppen + Protokolle] internal-network -> internal-interface

- Proxy
- domain-TCP (TCP-53)
- domain-UDP (UDP-53)
- webcache (TCP-8080)
- HTTP-transparent (TCP-2411)
- ICMP-echo-req (ICMP-8)
- POP3Proxy (TCP-8110)
- Proxy-URLshortener (TCP-8081)
- HTTPS-transparenter (TCP-2412)

Content-Filter

1. Blacklist-Kategorien
    - Hacking
    - Threat Intelligence Feed
    - Proxy
    - Porno und Erotik
    - Werbe Dienste
    - Tracking strict
    - SPAM domains

Über einen Content-Filter wird der Zugriff auf Seiten mit Hacking -Inhalten beschränkt. Weitere Filter können im Rahmen der Basisinstallation, oder durch nachträgliche Konfigurationsänderungen individuell aktiviert werden, je nach Wunsch des Auftraggebers.

Geoblocking
Für ausgehenden als auch für eingehenden Datenverkehr werden jegliche Dienste und Websites aus den folgenden Ländern geblockt:

Afghanistan, Bangladesh, China, India, Iran, North Korea, South Korea, Nepal, Pakistan, Taiwan, Vietnam, Nigeria, Belarus, Hungary, Romania, Russian Federation, Turkey, Brazil

4.3 Individuelle Konfiguration

Basierend auf einer vom Kunden erstellten Firewall-Policy kann, im Rahmen der Basisinstallation, eine weitergehende individuelle Konfiguration erfolgen. Sofern zwecks Vorqualifizierung eine telefonische Kontaktaufnahme durch einen Installationsdienstleister oder zertifizierten Vertriebs- und Servicepartner erfolgt, hat der Kunde diesen über die individuellen Regeln in Kenntnis zu setzen, um den Aufwand am Tag der Installation möglichst gering zu halten. Die Individuelle Konfiguration wird, sofern Sie nicht im Rahmen der Leistungen, gemäß Punkt 4.1 dieser Leistungsbeschreibung, abbildbar ist, anhand der jeweils gültigen Preisliste in Rechnung gestellt.

Individuelle Konfigurationen, welche nicht im Rahmen der Basisinstallation stattfinden, gelten als Standard Konfigurationsänderungen (siehe Punkt 4.1).

4.4 Mitwirkungspflichten des Kunden

Im Anschluss an die Inbetriebnahme der Firewall erhält der Kunde ein Installationsprotokoll. Mit seiner Unterschrift auf diesem Protokoll, bestätigt der Auftraggeber, dass alle individuellen Regeln auf Funktion geprüft wurden. Gleiches gilt auch für Geräte und Dienste, welche bereits vor der Installation durch den Auftraggeber genutzt wurden. Wird eine Einschränkung erst zu einem späteren Zeitpunkt festgestellt, so hat der Auftraggeber kein Recht auf Nachbesserung vor Ort. Die Nachbesserung erfolgt im Rahmen des, im Teilnahmeantrag definierten, Supportes, wenn dieser bestellt wurde. TECH-PRAX behält sich vor, Mehraufwände, welche auf eine nicht ausreichende Funktionsprüfung, seitens des Auftraggebers,

zurückzuführen sind, gemäß Preisliste in Rechnung zu stellen.

Es gelten die folgenden Voraussetzungen und Mitwirkungspflichten (seitens Securepoint):

- Es besteht eine aktive Internetverbindung (hierdurch können weitere Kosten entstehen).
- Der Vertragspartner hat logischen und physischen Zugriff auf die Infrastruktur, in der die Leistungen aus diesem Vertrag eingesetzt werden.
- Auf Verlangen der Securepoint GmbH richtet der Vertragspartner eine Fernwartungsmöglichkeit auf die Infrastruktur bzw. definierte Geräte ein. Dabei wird ein von der Securepoint GmbH vorgegebenes Tool verwendet.
- Der Vertragspartner hat die für die Einrichtung / Administration erforderlichen Daten zur Verfügung gestellt.
- Der Vertragspartner stellt einen kompetenten und entscheidungsbefugten Ansprechpartner zur Verfügung.
- Der Vertragspartner trägt die Verantwortung für die Datenqualität der zur Verfügung gestellten Personen- und Organisationsdaten.
- Der Vertragspartner stellt sicher, dass die Rufnummern von den Anwendern inkl. Durchwahl übertragen wird.
- Trifft eine der hier beschriebenen Voraussetzungen nicht zu, ist die Securepoint GmbH nicht verpflichtet, den beschriebenen Service mit den vereinbarten Service-Leveln zu erbringen.

Diese Mitwirkungspflichten werden grundsätzlich in einer Qualität erbracht, die es der Securepoint GmbH erlaubt, ohne Mehraufwand die vertraglichen Verpflichtungen zu erfüllen. Verzögerungen der Leistungserbringung und/oder Verletzungen der vereinbarten Service-Level, die auf die Nichterfüllung der Mitwirkungspflichten durch den Vertragspartner zurückzuführen sind oder die nicht von der Securepoint GmbH zu vertreten sind, gehen nicht zu Lasten der Securepoint GmbH.

4.5 Router

Bei Routern von Vodafone (Vodafone Station) kann es zu Beeinträchtigungen beim Service kommen, da nicht remote auf die Firewall zugegriffen werden kann. Hier können z. B. nicht automatisiert Updates installiert werden. Wir empfehlen hier den Einsatz einer FritzBox. Diese ist nicht Bestandteil der Einrichtung / des Vertrages.

5. Reportings

Der Auftraggeber erhält einen wöchentlichen/monatlichen Report über die Aktivitäten seiner Firewall. Der Inhalt des Reports kann über die Website des Herstellers Securepoint eingesehen werden (https://www.securepoint.de/produkte/unified-security-report.html). Dieser Report wird an die, vom Auftraggeber auf dem Teilnahmeantrag festgelegte, E-Mail-Adresse versandt.

6. Service-Level-Agreement (SLA)

Die Meldung und Bearbeitung von Servicebeeinträchtigungen erfolgt über den im Auftrag definierten Ansprechpartner. Beachten Sie, dass der von Tech-Prax zertifizierte Vertriebs- und Servicepartner ggfs. abweichende Zeiten für die Servicebereitschaft und Servicewiederherstellung benennt.

6.1 Definition von Servicebeeinträchtigungen im Rahmen der Managed Firewall Services

Eine Servicebeeinträchtigungen liegt immer dann vor, wenn die Firewall als Ganzes ausfällt oder einzelne Leistungsmerkmale trotz korrekter Konfiguration / Installation nicht mehr funktionieren. Beeinträchtigungen, die im Zusammenhang mit verhinderten Gegebenheiten, die abweichend der Grundkonfiguration auftreten, wie z. B. die Nicht-Erreichbarkeit einer bestimmten Homepage / Applikation /Port oder neue Hardware im Kundennetzwerk, die nicht richtig mit dem Internet kommunizieren kann, gelten nicht als

Servicebeeinträchtigungen und werden gesondert berechnet.

6.2 Meldung von Servicebeeinträchtigungen und Servicebereitschaft

Servicebeeinträchtigungen meldet der Kunde unter Nennung aller zur Servicewiederherstellung erforderlichen Daten, insbesondere seiner Kundennummer grundsätzlich per Telefon, Fax oder E-Mail. Um eine schnelle Diagnose sicherzustellen, ist der Auftraggeber angehalten, die Symptome der Servicebeeinträchtigungen möglichst genau zu beschreiben. Liegen Tech-Prax alle notwendigen Informationen vor, beginnt die Wiederherstellung des Services. Die Bearbeitung von Servicebeeinträchtigungen durch die Servicebereitschaft erfolgt werktags - ausgenommen samstags - in der Zeit zwischen 09:00 Uhr und 16:00 Uhr. Meldungen von Servicebeeinträchtigungen, die nachts in der Zeit zwischen 16:00 Uhr und 09:00 Uhr, samstags, sonntags oder an gesetzlichen Feiertagen eingehen, beginnt die Wiederherstellungsfrist am folgenden Werktag um 09:00 Uhr. Fällt das Ende der Wiederherstellungsfrist auf einen Zeitpunkt zwischen 16:00 Uhr und 08:00 Uhr, auf einen Samstag, Sonntag oder gesetzlichen Feiertag, wird die Wiederherstellungsfrist ausgesetzt und am folgenden Werktag um 09:00 Uhr fortgesetzt.

6.3 Servicebeeinträchtigung- und wiederherstellung

Tech-Prax beseitigt Servicebeeinträchtigungen, welche im Einflussbereich von Tech-Prax liegen, innerhalb von 7 Tage während der angegebenen Servicebereitschaftszeiten. Die Wiederherstellungszeit beginnt, ab Meldung durch den Auftraggeber und gilt als eingehalten, wenn der Service nach dieser Zeit wieder vollständig zur Verfügung steht. Die Wiederherstellungszeit wird während der Reparatur und ggf. Austausch der eingesetzten Endgeräte ausgesetzt, unabhängig davon ob diese von Tech-Prax oder einem zertifizierten Vertriebs- und Servicepartner bezogen wurde. Ebenso wird die Wiederherstellungszeit ausgesetzt bis alle vom Auftraggeber geschuldeten Informationen zu der Servicebeeinträchtigung vorliegen. Beeinträchtigungen, welche durch Updates / Neuanschaffungen von Auftraggeber eigener Hard- und Software auftreten, stellen keine Servicebeeinträchtigung im Sinne dieser Leistungsbeschreibung dar, da diese nicht im Einflussbereich von Tech-Prax liegen. In diesen Fällen muss der Auftraggeber TECH-PRAX eine Standardkonfigurationsänderung, gemäß Punkt 4.1, mitteilen.

6.4 Kosten

Für die Servicewiederherstellung, sowie den ggfs. notwendigen Tausch von, durch Tech-Prax bezogener, Hardware, im Rahmen der Gewährleistung, entstehen dem Kunden keine Kosten, wenn diese Wiederherstellung im Rahmen des Zeitkontigentes erfolgt (wenn gebucht), es sei denn, im Verlauf der Servicewiederherstellung wird festgestellt, dass die Servicebeeinträchtigung durch den Kunden verschuldet ist oder dass gar keine Servicebeeinträchtigungen vorliegt. In diesen Fällen ist Tech-Prax oder der von Tech-Prax zertifizierte Vertriebs- und Servicepartner dazu berechtigt, den Aufwand gemäß der jeweils gültigen Preisliste in Rechnung zu stellen.

6.5 Erbringung kostenloser Leistungen

Eine derzeitige oder zukünftige, kostenlose Erbringung von Leistungen durch die Tech-Prax oder von Tech-Prax zertifizierten Vertriebs- und Servicepartnern gegenüber dem Auftraggeber begründet keinen Erfüllungsanspruch. Tech-Prax kann derartige vergütungsfrei zur Verfügung gestellten Leistungen künftig auch gegen Entgelt anbieten. In einem solchen Fall wird Tech-Prax den Auftraggeber unverzüglich informieren.

6.6 Wartungsarbeiten

Wartungsarbeiten können zu einer geplanten Unterbrechung der Dienste führen. Geplante Updates werden automatischen Werktages in der Zeit zwischen 08:00 – 16:00 Uhr installiert.