Leistungsbeschreibung für A1 IT Security Services (LB A1 IT Security)

Allgemeines

Diese Leistungsbeschreibung gilt ab 4. Mai 2020 für neue Bestellungen. Die am 1. Oktober 2018 veröffentlichte LB A1 IT Security wird ab diesem Zeitpunkt nicht mehr angewendet. A1 Telekom Austria AG (A1) erbringt im Rahmen ihrer technischen und betrieblichen Möglichkeiten A1 IT Security Services nach den Bestimmungen des Telekommunikationsgesetzes (TKG 2003), den Allgemeinen Geschäftsbedingungen für Solutions von A1 (AGB Solutions) in der jeweils geltenden Fassung, sowie nach den für dieses Produkt maßgeblichen Leistungsbeschreibungen und Entgeltbestimmungen in der jeweils geltenden Fassung, insoweit keine von diesen abweichende oder ergänzende Regelungen getroffen werden, samt allfälligen schriftlichen Individualvereinbarungen.

Bei diesem Produkt handelt es sich um dem Kunden zur Verfügung gestellte Dienstleistungen von A1, die aus verschiedenen Schutzmaßnahmen vor Angriffen an das Kundennetz aus dem Internet samt Überprüfungen bestehender IT-Sicherheitseinrichtungen am Kundenstandort bestehen. Das Produkt setzt sich aus Firewall & VPN-, Content Security- und Endpoint Security Services zusammen:

- Firewall & VPN Services beinhalten Dedicated Firewall, A1 Professional Secure und A1 Central Firewall. Sie dienen zum Schutz vor externen und internen unbefugten Zugriffsversuchen auf Ressourcen im geschützten Netzwerkbereich sowie zur gesicherten Datenübertragung in öffentlichen Netzen.
  A1 Professional Secure kann ab 4. Mai 2020 nicht mehr neu bestellt werden.
- Content Security Services bestehen aus Dedicated Content Security, A1 Mail Security und A1 Web Security. Sie dienen der Filterung von E-Mails bzw. Web-Verkehr unerwünschten Inhalts und der Abwehr von Viren, Würmern oder Trojanern, die firmeneigenen Ressourcen sehr hohen Schaden zufügen können.
  A1 Mail Security und A1 Web Security können ab 4. Mai 2020 nicht mehr bestellt werden.
- Endpoint Security Services besteht aus dem Produkt A1 Desktop Security und beinhaltet grundlegende Technologien wie Antivirus & Antispyware, Firewall, Intrusion Prevention sowie einen proaktiven Bedrohungsschutz zur Endgerätesicherheit.
  A1 Desktop Security wird mit 06. Juli 2020 eingestellt.

A1 bietet im Rahmen des Produktes A1 IT Security Services gem. Punkt 1.4 weitere IT Security-Komponenten (Optionen) an.

Das Produkt A1 IT Security Services gliedert sich in 6 Ausprägungen, die Firewall & VPN-, Content Security- und Endpoint Security Services in verschiedenem Ausmaß einsetzen. Die Produktnamen sind

1. Dedicated Firewall und Dedicated Content Security,
2. A1 Professional Secure
   A1 Professional Secure kann ab 4. Mai 2020 nicht mehr neu bestellt werden.
3. A1 Central Firewall,
4. A1 Mail Security
   A1 Mail Security kann ab 4. Mai 2020 nicht mehr neu bestellt werden.
5. A1 Web Security
   A1 Web Security kann ab 4. Mai 2020 nicht mehr neu bestellt werden.
6. A1 Desktop Security.
   A1 Desktop Security wird mit 06. Juli 2020 eingestellt.

A1 lädt den Kunden nach erfolgter Realisierung der gewünschten A1 IT Security Services zur Abnahme ein. Nimmt die Erfüllung des Auftrags aufgrund der Größe oder Komplexität der Leistung mehrere Monate in Anspruch, ist A1 berechtigt, Teilabnahmen zu verlangen. Die Abnahme erfolgt durch Unterzeichnung eines Abnahmeprotokolls. Nach der Abnahme (Teilabnahme) erfolgt die Fakturierung der Leistung gem. EB A1 IT Security. Bei Verzögerungen, die nicht durch A1 zu vertreten sind, beginnt die Fakturierung mit der Bereitstellung der Leistung.

1 Dedicated Firewall und Dedicated Content Security

1.1 Produktbeschreibung mit Hardware und Software

A1 implementiert spezielle IT Security-Lösungen wie Firewalls oder Content Security-Systeme, die entsprechend den Anforderungen des Kunden gemeinsam erarbeitet werden.

Dabei können spezielle Komponenten von Firmen wie z.B. Check Point, Cisco, Hewlett-Packard, Barracuda Networks oder Radware verwendet werden. Die Wahl der einzusetzenden Hard- und Software wird von A1 nach Überprüfung der technischen oder betrieblichen Erfordernisse getroffen.

Hinsichtlich der benötigten Hard- und Software hat der Kunde entweder eine Kauf- oder eine Überlassungsoption. Soweit der Kunde sich für die Überlassungsvariante entscheidet, ist die Inanspruchnahme des Wartungsdienstes gem. Punkt 1.3.1 unbedingt erforderlich.

Dem Kunden wird das Recht eingeräumt, eine Sicherungskopie zu Zwecken der Datensicherung sowie einer Installationskopie auf einer Festplatte des verwendeten Rechners zu erstellen. Die Sicherungskopie ist vom Kunden mit einem Hinweis auf das Urheberrecht zu versehen. In Netzwerken darf das Programm nur auf einem Rechner des Netzwerkes zur selben Zeit eingesetzt werden. Sofern die Software in der Überlassungsvariante in Anspruch genommen wird, sind sämtliche angefertigte Kopien vom Kunden bei Vertragsbeendigung an A1 zu retournieren.

Die Software darf vom Kunden insbesondere weder abgeändert, zurückentwickelt, weiterentwickelt oder übersetzt werden. Das schriftliche Material darf weiters insbesondere weder vervielfältigt noch dürfen aus dem Benutzerhandbuch abgeleitete Werke hergestellt werden.

Der Kunde hat das Recht, die Software zur Herstellung der Interoperabilität mit einem anderen Programm im notwendigen Umfang zu entschlüsseln. Dabei hat er die Grenzen des Urheberrechtsgesetzes einzuhalten.

Da Dedicated Firewall und Dedicated Content Security speziell auf die Bedürfnisse des Kunden abgestimmt und sowohl einmalige als auch laufende Entgelte vom Ausmaß des Umfanges der Leistung abhängig sind, erfolgt die Festlegung der Entgelte von A1 im Zuge der Projektplanung.

1.2 Einmalige Dienstleistungen

1.2.1 Installation von Hardware und Software

A1 implementiert die gem. Punkt 1.1 beschriebenen Komponenten und führt einen Test im Kundennetz durch. A1 kann die Installation ausschließlich bei Vorhandensein von

insbesondere eines funktionierenden Internet-Zugangs und einer funktionierenden Stromversorgung durchführen. Bei nicht von A1 betriebenen Sicherheits-Systemen kann auf Anfrage des Kunden und gegen gesondertes Entgelt gem. Punkt 1.4.3 während oder nach der Installation eine Einweisung des Kunden durchgeführt werden.

1.2.2 Support

Bei Nicht-Inanspruchnahme des Wartungs- oder des Managementdienstes gem. Punkt 1.3 bietet A1 Dienstleistungen wie die Installation von Software-Updates, Major Release-Wechsel (z.B. Software-Versionswechsel von 2.0 auf 3.0) und Änderungen an der System-Konfiguration auf Anfrage und gegen gesondertes Entgelt. Die Verrechnung erfolgt nach Aufwand im Nachhinein oder auf Kundenwunsch im Vorhinein mit Bereitstellung eines Stunden-Pools. Die hierzu erforderlichen Arbeiten erfolgen werktags (Montag bis Freitag von 8:00 bis 17:00 Uhr, ausgenommen 24.12. und 31.12.) in Absprache mit dem Kunden. Dabei ist A1 zur Außerbetriebnahme des Systems berechtigt. Die im Punkt 1.3 garantierten Leistungsmerkmale kommen hier nicht zur Anwendung.

1.3 Laufende Dienstleistungen

A1 führt auf Anfrage des Kunden die in diesem Punkt genannten laufenden Dienstleistungen durch.

A1 ist ausschließlich bei von ihr gewarteten Geräten verpflichtet, die u.a. Zeiten (z.B. Reaktions- oder Lösungszeiten) einzuhalten. Weiters ist der Kunde verpflichtet, bevor er eine Störungsmeldung im Bereich einer Firewall, einer VPN-Verbindung oder eines Content Security-Systems an A1 übermittelt, zu überprüfen, ob die Internet Connectivity und die Stromversorgung funktioniert.

1.3.1 Wartung für Hardware (DHS) oder Hard- und Software (DCS)

A1 bietet Wartungsdienstleistungen in zwei Varianten:

- Data Hardware Service (DHS): nur Hardware-Wartung bei Störung,
- Data Comprehensive Service (DCS): zusätzlich Software-Wartung inklusive Updates.

A1 wird bei Inanspruchnahme des Wartungsdienstes die Fehlerbehebung der Hardware (DHS) und/oder von Hard- und Software (DCS) auch vor Ort – an Standorten von A1 und Standorte des Kunden laut Standort-Verzeichnis im Angebot – übernehmen.

Der Wartungsdienst umfasst die Inspektion und die Instandsetzung des IT Security-Systems, soweit die auftretenden Störungen bei ordnungsgemäßem Gebrauch entstanden sind. Die Instandsetzung erstreckt sich auch auf die Erneuerung der gekauften Komponenten, die auf Dauer unbrauchbar geworden sind. Während der Arbeiten ist A1 berechtigt, das System außer Betrieb zu setzen. In der Regel erfolgt die Instandsetzung durch Austausch der Hardware- und/oder Hard- und Software-Komponenten.

Änderungen wie Umkonfigurierungen an Hard- und Software dürfen nur von A1 durchgeführt werden. Eingriffe durch IT-Administratoren des Kunden bedürfen der Zustimmung durch A1; die Verantwortung für ordnungsgemäße Datensicherung – Backup der zur Wiederherstellung der System-Funktionalität benötigten Daten – liegt dann ausschließlich beim Kunden, weiters meldet der Kunde Außerbetriebnahmen und Änderungen der Erreichbarkeit (IP-Adresse) des Systems an A1 einen Werktag zuvor.

1.3.1.1 Service Level Agreement (SLA) Fehlerbehebung

A1 nimmt Störungsmeldungen des Kunden unter einer, bei Vertragsabschluss dem Kunden bekannt gegebenen Service-Rufnummer entgegen.

Beginn der Fehlerbehebung ist die qualifizierte Störungsmeldung durch berechtigte Mitarbeiter des Kunden. Bei telefonischer Meldung beginnt die Fehlerbehebung mit Abschluss des Anrufes. Wird die Störung mittels E-Mail eingemeldet, antwortet A1 innerhalb der Fehlerrückmeldezeit nach interner Prüfung mit der Annahme der Fehlermeldung; die Fehlerbehebung beginnt mit der Annahme.

Der Kunde nominiert kompetente Ansprechpartner für die Fehlerbehebung. Kontaktdaten dieser Ansprechpartner und allfällige Änderungen der Ansprechpartner oder Kontakte gibt der Kunde A1 schriftlich bekannt. Die Ansprechpartner des Kunden verfügen über ausreichende Sprachkenntnisse in Deutsch oder Englisch.

Die Fehlerbehebung erfolgt gemäß den unten angeführten Serviceklassen je nach der vom Kunden gewählten Ausprägung:

Qualitäts-parameter	**Serviceklasse Classic**	**Serviceklasse Comfort**	**Serviceklasse Professional**	**Serviceklasse Premium**
Störungs-annahme	Mo–So, 0–24 Uhr			
Servicezeiten	Mo–Fr, 8–17 Uhr werktags	Mo–Fr, 7–19 und Sa, 7–12 Uhr werktags	Mo–Sa, 7–19 Uhr werktags	Mo–So, 0–24 Uhr
Fehlerrück-meldezeit	0,5 h			
Reaktionszeit	nächster Werktag	nächster Werktag	2 h	1 h
Terminfenster Zutritt	4 h	2 h	1 h	1 h
Techniker-vor-Ort	übernächster Werktag	nächster Werktag	8 h	6 h
Lösungszeit	übernächster Werktag	nächster Werktag	8 h	6 h

A1 misst die Fehlerbehebung über ihr Trouble Ticket System auf Basis der erfassten Störungstickets. Im Trouble Ticket System erfasst A1 Störungsgeschäftsfälle auf Grund der Störungsmeldung des Kunden.

Fremdverzögerungen während der Fehlerbehebung werden nicht in der Berechnung von Reaktionszeiten, Techniker-vor-Ort Zeiten oder Lösungszeiten berücksichtigt.

A1 führt die Fehlerbehebung innerhalb der Servicezeit der vereinbarten Serviceklasse durch. Wenn die Servicezeit eines Arbeitstages endet, unterbricht A1 die Tätigkeiten zur Fehlerbehebung und setzt sie mit Beginn der Servicezeit des nächsten Arbeitstages fort. Als Lösungszeit berücksichtigt A1 nur Zeiten innerhalb der Servicezeit.

Mitarbeiter von A1 und/oder durch A1 beauftragte Subunternehmer müssen für den Betrieb des Service innerhalb der Nutzungszeit (Montag bis Sonntag von 0:00 bis 24:00 Uhr) kostenlosen Zugang zu den technischen Einrichtungen am Kundenstandort haben, die zur Service Bereitstellung erforderlich sind. Wird der Zugang nicht gewährt, ist A1 berechtigt, die Kosten eines neuerlichen Einsatzes gesondert zu verrechnen.

1.3.1.2 Begriffsdefinitionen im SLA Fehlerbehebung

Fremdverzögerungen sind Zeiträume, in denen die Leistungserbringung aus nicht von A1 zu vertretenden Gründen unterbleibt.

Werktags umfasst die angegebenen Wochentage exklusive Sonntage, österreichische gesetzliche Feiertage sowie 24.12. und 31.12.

Störungsmeldung ist die Mitteilung des Kunden an eine von A1 im Angebot bekannt gegebene Stelle unter exakter Angabe des Fehlerbildes.

Bei Proaktiver Störungserkennung durch A1 wird ein Fehler unabhängig von einer Störungsmeldung des Kunden erkannt und bearbeitet.

Bestätigung der Fehlerannahme ist der Zeitpunkt zu dem A1 dem Kunden den Erhalt der Störungsmeldung bestätigt und dem Kunden die Fehler-Ticketnummer bekannt gibt.

Fehlerrückmeldezeit ist die maximale Frist zwischen dem Eingang einer Störungsmeldung und der Bestätigung der Fehlerannahme durch A1 unter Angabe der Fehler-Ticketnummer.

Reaktionszeit ist der Zeitraum zwischen Beginn der Lösungszeit und einer qualifizierten Rückmeldung an den Kunden.

Eine qualifizierte Rückmeldung liegt vor, wenn A1 dem Kunden eine erste Diagnose der Problemursache und den weiteren Lösungsweg mitteilt.

Techniker-vor-Ort ist der Zeitraum zwischen Beginn der Lösungszeit und dem Eintreffen eines Technikers vor Ort.

Lösung ist der Zeitpunkt, zu dem die Störung behoben ist. Die Funktionalität des Systems wiederhergestellt ist oder dem Kunden ein adäquater Ersatz zur Verfügung gestellt wurde.

Lösungszeit ist der Zeitraum zwischen Bestätigung der Fehlerannahme oder proaktiver Störungserkennung und der Lösung.

Gutmeldung ist eine Information über die erfolgte Lösung.

1.3.2 Betrieb und Management des IT Security-Systems aus dem Network Operation Center (NOC)

Darüber hinaus betreibt A1 IT Security Management-Systeme, die auf einem von ihr erstellten Konzept und einer von ihr formulierten IT-Sicherheitspolitik basieren, im Rahmen von abgestuften „Managed Security Paketen“.

Voraussetzung für die Inanspruchnahme dieser Pakete ist der Bezug von Hard- und Software-Wartung (DCS) gem. Punkt 1.3.1. Im Trouble Ticket System erfasst A1 Störungsgeschäftsfälle

- proaktiv durch Störungserkennung mit dem IT Security Management-System und
- reaktiv auf Grund der Störungsmeldung des Kunden.

Es werden folgende Managed Security Pakete angeboten:

1.3.2.1 Managed Security bei Cisco ASA und Barracuda NG Firewalls

1.3.2.1.1 Überwachung und Betrieb

A1 überwacht und betreibt das IT Security-System über einen Internet-Zugang oder das Corporate Network des Kunden täglich von 0:00 bis 24:00 Uhr. Der Internet-Zugang ist nicht Gegenstand dieses Vertrages, ist aber Voraussetzung zur Erbringung der gegenständlichen Leistungen.

1.3.2.1.2 Reaktionen auf Alarme

Durch Überwachen der Erreichbarkeit des IT Security-Systems werden kritische Ereignisse erkannt. Bei Eintritt eines kritischen Ereignisses wird das A1 Network Operation Center (NOC) automatisch alarmiert. Eine Analyse der Alarmsituation wird innerhalb der vereinbarten Zeiten durchgeführt und der Normalzustand wieder hergestellt. Eine Auswertung der vom Hersteller als gefährlich definierten Angriffe kann mittels eines zusätzlichen Intrusion Prevention Systems auf Kundenwunsch gegen gesondertes Entgelt zur Verfügung gestellt werden.

1.3.2.1.3 Backup

A1 erstellt periodisch sowie nach jeder Änderung eine Sicherheitskopie der zur Wiederherstellung der System-Funktionalität benötigten Daten.

1.3.2.1.4 Updates, Patches und Fixes

In Absprache mit dem Kunden führt A1 Anpassungen der Security- und Betriebssystem-Software an den aktuellen Entwicklungsstand des Herstellers durch. Die hierzu erforderlichen Arbeiten erfolgen werktags (Montag bis Freitag von 8:00 bis 17:00 Uhr, ausgenommen 24.12. und 31.12.). Dabei ist A1 zur Außerbetriebnahme des IT Security-Systems berechtigt.

1.3.2.1.5 Verschlüsselter Datenaustausch (VPN-Client, Site-to-Site-VPN, SSL-Web-VPN)

Mittels verschlüsselten Datenaustauschs ist es möglich, dass Mobile- und Home User auf Ressourcen im Firmennetzwerk zugreifen können. Das kann mittels Remote Access (VPN-Client) oder SSL-Web-VPNs ermöglicht werden. Ebenso ist es möglich, durch A1 Firewalls gesicherte Außenstellen über Site-to-Site-VPNs an die Zentrale anzubinden. Die Konfiguration auf der Firewall wird durch A1 durchgeführt.

1.3.2.1.6 Änderungen an der System-Konfiguration

In Absprache mit dem Kunden können Standard-Änderungen an der System-Konfiguration pro Monat bis zu zwei Stunden werktags (Montag bis Freitag von 8:00 bis 17:00 Uhr, ausgenommen 24.12. und 31.12.) vorgenommen werden. Die Änderungsaufträge werden zwischen A1 und autorisierten Mitarbeitern des Kunden vereinbart und nach ihrer

Ausführung dokumentiert. Änderungswünsche, die bis 11:00 Uhr eingehen, werden am gleichen Tag bearbeitet.

1.3.2.2 Managed Security bei Check Point Firewalls

Die Leistungen des Managements beim Hersteller Check Point beinhalten die im Punkt 1.3.2.1 angeführten Merkmale inklusive der Überwachung des Firewall-Prozesses samt einem umfassenden Reporting.

1.3.2.2.1 Reporting

A1 stellt autorisierten Mitarbeitern des Kunden bei Bedarf Reports bereit. Die kundenindividuellen Reports werden mittels zentralen Check Point SmartReporter automatisiert erstellt und in regelmäßigen Abständen (täglich, wöchentlich oder monatlich) dem Kunden per E-Mail übermittelt. Die Reports sind einfach zu lesen, graphisch aufbereitet und bieten einen umfassenden Überblick der betriebenen Firewall. Eine Auswertung der vom Hersteller als gefährlich definierten Angriffe kann mittels eines zusätzlichen Intrusion Prevention Systems auf Kundenwunsch gegen gesondertes Entgelt zur Verfügung gestellt werden.

Die Leistungen des Managements werden in folgenden Ausprägungen angeboten:

1.3.2.2.2 Management Small

- Einpflegen und Ändern von Regeln und Rechten sowie von Netzobjekten;
- Anpassungen der Regelbasis aufgrund von Änderungen in der Adressinfrastruktur;
- Arbeiten im Zusammenhang mit der Implementierung neuer Netzstränge im Kundennetz;
- Anpassen der Routing-Tabelle an die Erfordernisse des Kunden.

1.3.2.2.3 Management Medium (zusätzlich zu Management Small)

- Ergänzungen des Regelwerkes und Freischalten von Services, die über die jeweils gültigen Standard-Dienste der eingesetzten Firewall-Software hinausgehen;
- Anpassungen der Firewall bei der Einrichtung von Site-to-Site-VPNs;
- Verhinderung des Zugriffs auf nicht freigegebene Web-Sites mittels URL-Filtering nach bestimmten Kategorien und Themengruppen.

1.3.2.2.4 Management Large (zusätzlich zu Management Medium)

- Inbetriebnahme neuer Interfaces sowie Anpassung der Regelbasis ohne zusätzlicher neuer Hardware;
- Anpassungen der Firewall zum Betreiben einer Remote Access-Lösung;
- Einrichten einer separaten Authentifizierungs-Lösung;
- Anlegen neuer und Löschen bestehender User bzw. User-Gruppen aus dem Firewall-Regelwerk;
- Check Point Management Portal (Web-basierender Zugang zum Firewall Management-System).

1.3.2.3 Managed Security bei Cisco IronPort Content Security Appliances

Die Leistungen des Managements sind grundsätzlich die gleichen wie unter Punkt 1.3.2.1 beschrieben. Ausgenommen sind VPN-Verbindungen Punkt 1.3.2.1.5 und Änderungen an der System-Konfiguration Punkt 1.3.2.1.6. Änderungen oder Erweiterungen an der System-Konfiguration sind vom Kunden selbst mittels einer Web-Oberfläche vorzunehmen. Dazu steht dem IT-Administrator des Kunden ein Service Desk im Ausmaß von einmalig zwei Stunden und laufend ein Mal pro Woche bis zu 15 Minuten werktags (Montag bis Freitag von 8:00 bis 17:00 Uhr, ausgenommen 24.12. und 31.12.) für Support-Anfragen zur Verfügung.

1.3.2.4 Virus Prevention Management

Bei Inanspruchnahme von Managed Security gemäß 1.3.2.1 oder 1.3.2.2 ermöglicht A1 mit Virus Prevention, eingehende Daten in Firewall-gesicherten Netzwerken auf Virusbefall zu überprüfen. Virus Prevention kann als Proxy-Server eingesetzt oder über entsprechende Hardware-Module (bei Cisco) bzw. Software-Module (bei Check Point und Barracuda) angesprochen werden. A1 liefert, installiert und betreibt die für Virus Prevention benötigte Hard- und Software. Zeitpunkt und Modalität der Lieferung und Installation werden in Absprache mit dem Kunden festgelegt. Das Management umfasst folgende Leistungen:

- Updates der Software Releases;
- Regelmäßiges Update der Antiviren-Patterns;
- Backup;
- Reaktion auf Alarme bei gefundenen Viren.

1.3.2.5 Proxy Security Services

A1 ermöglicht mit Proxy Security Services das Scannen des HTTP- und FTP-Verkehrs des Kunden sowie die Verhinderung des Zugriffs auf nicht freigegebene Web-Sites mittels URL-Filtering. A1 implementiert und betreibt die für die Proxy Security Services benötigte Hard- und Software zentral im NOC 7x24 Stunden als dedizierte Instanz für jeden einzelnen Kunden. Folgende Leistungen sind damit verbunden:

- Updates des Betriebssystems;
- Scannen des HTTP- und FTP-Verkehrs des Kunden;
- Scannen und Entfernen von Viren, Trojaner, Malicious Code, Dialer;
- Filterung von unerwünschten Dateitypen und Downloads aus dem Datenverkehr;
- Filterung und Blocken von Web-Sites unerwünschten Inhalts;
- Automatische Updates der Virendatenbanken und URL-Filtering-Datenbanken;
- Einrichtung von Berechtigungsprofilen aufgrund unterschiedlicher offizieller IP-Adressen;
- Backup;
- Reporting.

1.3.2.6 Intrusion Prevention Management

Bei Inanspruchnahme von Managed Security gemäß 1.3.2.1 oder 1.3.2.2 ermöglicht A1 mit Intrusion Prevention, dass der IP-Verkehr in das private Netz des Kunden und/oder auf die zu überwachenden Diensterechner über ein Intrusion Prevention System (IPS) geführt und auf Angriffe oder Anomalien untersucht wird. Erkannte Anomalien werden protokolliert, sodass – falls erforderlich – auch entsprechende Gegenmaßnahmen durchgeführt werden können.

Der zur Verfügung gestellte Dienst Intrusion Prevention entspricht dem derzeit verfügbaren Stand der Technik bei der Überwachung des IP-Verkehrs im Netzwerk auf Unregelmäßigkeiten. Dennoch kann, insbesondere aufgrund der ständigen Neu- und Weiterentwicklung von Angriffstechniken ein 100% Erkennen jeglicher Angriffe oder Anomalien nicht garantiert werden.

Intrusion Prevention kann mit entsprechenden Hardware-Modulen (bei Cisco) bzw. Software-Modulen (bei Check Point und Barracuda) angesprochen oder mittels dedizierten Komponenten (Radware) eingesetzt werden. A1 liefert, installiert und betreibt die für Intrusion Prevention benötigte Hard- und Software. Zeitpunkt und Modalität der Lieferung und Installation werden in Absprache mit dem Kunden festgelegt. Das Management umfasst folgende Leistungen:

- Updates der Software Releases;
- Regelmäßiges Update der IPS-Patterns;
- Backup;
- Reaktion auf Alarme bei Angriffen oder Anomalien.

1.4 Optionen

Da es sich bei Dedicated Firewall und Dedicated Content Security um Lösungen für spezielle Kundenanforderungen handelt, werden verschiedene Optionen zusätzlich angeboten.

1.4.1 IT Security Consulting

1.4.1.1 Workshop

A1 erarbeitet zusammen mit dem Kunden im Rahmen eines Workshops ein Grobkonzept zur sicheren Anbindung seines Netzwerkes über ein IT Security-System an das Internet. Der Workshop wird mittels eines vom Kunden auszufüllenden Fragebogens vorbereitet und in den Räumen des Kunden durchgeführt. Im Rahmen des Workshops werden zusammen mit dem Kunden die möglichen Schwachstellen einer ungeschützten Internet-Anbindung erarbeitet und die vorhandenen Risiken aufgezeigt. Das Ergebnis des Workshops wird dem Kunden spätestens zehn Arbeitstage nach dem Workshop als Protokoll ausgehändigt. Der Workshop umfasst acht Stunden mit zwei Spezialisten für Telekommunikationstechnologie. Inhalte der gemeinsam mit dem Kunden zu ermittelnden Agenda sind grundsätzlich:

- Abklärung des genauen Zwecks und der Absicht der Internet-Nutzung;
- Erklärung der Adress Translation;
- Erklärung der System-Architektur;
- Erklärung des Regelwerks;
- Erklärung des Policy Editors;
- Darstellung der Möglichkeiten des Managements;
- Vorführung der Hardware;
- Vorführung der Software und des Graphical User Interface (GUI);
- Diskussion technischer Details;
- Darlegung des Loggings und zusätzlicher Optionen.

1.4.1.2 Konzeptvorschlag

A1 übermittelt einen auf Basis der Ergebnisse aus dem Workshop und Teilen des Consultings erstellten Konzeptvorschlag.

1.4.1.3 Consulting und Netzdesign

Das Consulting findet in der Zeit nach dem Workshop statt. Consulting- und Netzdesign beinhalten folgende Leistungen:

- Sizing der Hardware für optimierte Durchsatzraten;
- Sizing der Software zur Bestimmung der Größe der Lösung;
- Festlegung der Hardware-Plattformen und der IT Security-Produkte;
- Festlegung der Netzanbindung des IT Security-Systems an das Netzwerk des Kunden;
- Festlegung der Architektur des geeigneten IT Security-Systems;
- Empfehlungen bezüglich eventuell bestehender Sicherheitslücken;
- Festlegung zu schützender Netzbereiche zur Platzierung von Internet-Servern;
- Demilitarized Zone (DMZ) im Detail mit Diensterechnern;
- Festlegung der Anzahl der offiziellen IP-Adressen;
- Dienstekonzepte für die Nutzung der Internet-Dienste Network News Transfer Protocol (NNTP), Domain Name Service (DNS), Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP) und File Transfer Protocol (FTP);
- Konfiguration des IT Security-Systems.

1.4.1.4 IT-Sicherheitspolitik

Die IT-Sicherheitspolitik enthält zusätzlich zum Ergebnis des unter Punkt 1.4.1.2 beschriebenen Konzeptes die Formulierung einer kundenindividuellen IT-Sicherheitspolitik für den zu schützenden Netzübergang. Die Sicherheitspolitik enthält die für einen gesicherten Betrieb erforderlichen Richtlinien, Vorgaben und Konzepte und ist der Organisationsstruktur des Kunden angepasst. Sie deckt die Bereiche Organisation, Umgang mit Daten sowie Systemen, Netzwerk, Kommunikation, Infrastruktur, Dokumentation und Revision ab. Voraussetzung für die Leistungserbringung ist, dass der Kunde einen für alle technischen und organisatorischen Bereiche qualifizierten Ansprechpartner sowie alle erforderlichen Informationen aktuell zur Verfügung stellt. Das Konzept und die Sicherheitspolitik werden dem Kunden in elektronischer Form ausgehändigt und zusätzlich im Rahmen einer Management-Präsentation vorgestellt.

1.4.2 High Availability Pack

Mit dem High Availability Pack wird die Ausfallsicherheit des IT Security-Systems erhöht. Hierzu sind zwei identische IT Security-Systeme (identische Hard- und Software) zur Verfügung gestellt. A1 liefert, installiert und betreibt auf Basis des Konzeptes und der IT-Sicherheitspolitik die für das High Availability Pack benötigte IT Security-Hardware und Software. Zeitpunkt und Modalität der Lieferung und Installation werden in Absprache mit dem Kunden festgelegt.

1.4.3 Schulungen

A1 kann alternativ in ihren Räumen oder Räumen des Kunden eine Schulung für die Komponenten der Firmen Check Point, Cisco oder Barracuda halten.

2 A1 Professional Secure

A1 Professional Secure kann ab 04. Mai 2020 nicht mehr neu bestellt werden.

Speziell für die in Österreich stark ausgeprägten Marktsegmente wurden eigene Security Bundles von A1 entwickelt. A1 implementiert standardmäßig die IT Security-Bundles am Standort des Kunden. Dabei kommen Komponenten von Cisco zum Einsatz.

2.1 Einmalige Dienstleistungen

A1 implementiert die Komponenten der Firewall und führt einen Test im Kundennetz durch. Für die Installation ist ein fixer A1 Business Breitband Internet-Zugang zum Netzwerk des Kunden erforderlich. Die Installationspauschale ist von der Anzahl der Interfaces (bis zu drei Interfaces) und dem Virtual Private Network (VPN) - Gateway abhängig.

2.2 Laufende Dienstleistungen

Es werden die im Punkt 2.3 und 2.4 beschriebene Hardware und Software von A1 bereitgestellt. Weiters ist standardmäßig die Hardware-Wartung von Punkt 1.3.1 mit Fehlerbehebung der Serviceklasse Classic inkludiert. Optional wird die Management-Leistung von Punkt 1.3.2.1 angeboten. Der Kunde ist verpflichtet, bevor er eine Störungsmeldung im Bereich einer Firewall oder einer VPN-Verbindung an A1 übermittelt, zu überprüfen, ob die Internet Connectivity und die Stromversorgung funktioniert. A1 bleibt Eigentümer der bereitgestellten Hardware; hinsichtlich der im Punkt 2.4 beschrieben Software erwirbt der Kunde insbesondere kein Lizenzrecht, sondern nur die Möglichkeit die Applikationen, die für die Funktionalität des Produktes notwendig sind, für die Vertragsdauer zu nutzen.

2.3 Hardware

Die Modelle unterscheiden sich in der Ausprägung der Hardware. Derzeit bietet A1 folgende Funktionen (Änderungen vorbehalten):

- Cisco ASA 5505, In- & Outbound Traffic, 10 User;
- Cisco ASA 5505, In- & Outbound Traffic, Unlimited User;
- Cisco ASA 5510 oder 5512-X, In- & Outbound & DMZ Traffic, Unlimited User.

2.4 Software

Für die Erbringung des Services wird Software von Cisco eingesetzt.

3 A1 Central Firewall

Mit A1 Central Firewall ist es möglich, dedizierte Firewall-Instanzen von einander logisch getrennt auf einer Hardware für verschiedene Kunden zu betreiben. Voraussetzung für die Inanspruchnahme von A1 Central Firewall ist der Bezug einer zentralen Internet Connectivity aus dem A1 NOC, da die Hardware für diesen Dienst nur ein Interface für die Internet Connectivity aufweist.

Ein Intrusion Prevention Management gemäß 1.3.2.6 kann auf Kundenwunsch gegen gesondertes Entgelt zur Verfügung gestellt werden. Dabei wird die zentrale Internet Connectivity der A1 Central Firewall zusätzlich über ein im A1 NOC aufgebautes Intrusion Prevention System geführt.

3.1 Einmalige Dienstleistungen

A1 sorgt dafür, dass der IP-Verkehr aus dem und in das private Netz des Kunden über dessen A1 Central Firewall-Instanz geroutet wird. Dafür ist ein Zugang zum Corporate Network des Kunden erforderlich.

3.2 Laufende Dienstleistungen

Die Infrastruktur wird im NOC aufgebaut. Dadurch entfallen die Dienstleistungen im Zusammenhang mit Übertragung von Daten vom Kundenstandort in das NOC. Es werden die im Punkt 3.3 und 3.4 beschriebene Hardware und Software von A1 verwendet. A1 bleibt Eigentümer der bereitgestellten Hardware; hinsichtlich der im Punkt 3.4 beschriebenen Software, erwirbt der Kunde insbesondere kein Lizenzrecht, sondern nur die Möglichkeit die Applikationen, die für die Funktionalität des Produktes notwendig sind für die Vertragsdauer zu nutzen.

Die Leistungen des Managements der Firewall-Instanzen sind weiters inkludiert und sind grundsätzlich die gleichen wie unter Punkt 1.3.2.2 beschrieben. Ausgenommen sind Updates, Patches und Fixes wie unter Punkt 1.3.2.1.4 beschrieben. Dafür gibt es ein Wartungsfenster, werktags, jeden Donnerstag bis Freitag, 21:00 bis 2:00 Uhr, ausgenommen 24.12. und 31.12. In Notfällen werden Fixes umgehend eingespielt. Weiters ausgenommen ist der Punkt „Inbetriebnahme neuer Interfaces sowie Anpassung der Regelbasis“ unter 1.3.2.2.4.

3.3 Hardware

Die Hardware ist entsprechend des Traffic-Aufkommens der verschiedenen Kunden sehr leistungsfähig und skalierbar. Der Internet-Zugang eines einzelnen Kunden sollte eine Bandbreite von 50 Mbit/s nicht übersteigen. A1 Central Firewall für eine darüber hinaus gehende Bandbreite ist auf Anfrage und gegen gesondertes Entgelt möglich.

3.4 Software

Durch die Virtualisierungstechnologie von Check Point ist es möglich, jedem einzelnen Kunden eine eigene Firewall-Instanz zuzuweisen und diese in übersichtlicher Form zu administrieren. Die Features der Software sind folgende (Änderungen der Software vorbehalten):

- Virtualized Security GatewayVLAN Trunking-Fähigkeit;
- Zentrales Management;
- Remote VPN Access;
- URL-Filtering.

4 A1 Mail Security

A1 Mail Security kann ab 04. Mai 2020 nicht mehr neu bestellt werden.

Mit einer mandantenfähigen (vom Kunden selbst individuell einstellbaren) Antispam- und Virenschutz-Lösung wird der E-Mail-Verkehr des Kunden, bevor er in die E-Mail Boxen der User gelangt, zentral auf Spam und einen eventuellen Virenbefall untersucht. Voraussetzung für die Inanspruchnahme von A1 Mail Security ist der Bezug eines fixen A1 Business Breitband Internet-Zugangs.

A1 Mail Security schützt vor E-Mails unerwünschten Inhalts und eventuell schädlichen Programmen wie zum Beispiel Viren, Würmern oder Trojaner. Dazu wird der MX- (Mail Exchange) Eintrag geändert. Es handelt sich somit um einen Mail Relayer mit Mail Scanning-Funktion. Dabei ist es möglich, den einzelnen Domains des Kunden verschiedene Regeln zuzuweisen, nach denen der E-Mail-Verkehr gescannt werden soll. Über eine Web-Oberfläche gelangt der Kunde oder sein IT-Administrator mittels Username und Password zu den kundenspezifischen Konfigurationen. Unterschiedlich, je nach ein- oder ausgehendem E-Mail-Verkehr, kann der Empfänger über einen Virenvorfall informiert werden. Ebenso kann festgelegt werden, wie mit einem vireninfizierten E-Mail verfahren wird. Darauf aufbauend werden Sicherheitsprofile definiert.

Der Kunde erklärt sich ausdrücklich damit einverstanden, dass E-Mails anhand der vom Kunden individuell festzulegenden Parameter auf Spam und Viren untersucht werden. Die Konfiguration liegt in der alleinigen Verantwortung des Kunden. Der weitere Umgang mit als Spam klassifizierten oder vireninfizierten E-Mails obliegt dem Kunden. Der Kunde ist verpflichtet, bestehende rechtliche, insbesondere arbeits- und datenschutzrechtliche Bestimmungen einzuhalten.

4.1 Einmalige Dienstleistungen

A1 Mail Security wird nach Vorkonfiguration durch A1, nachfolgender Einstellungen durch den Kunden und entsprechender Verständigung des A1 Service Desk aktiviert. Nach dieser Mitteilung des Kunden sorgt A1 dafür, dass der eingehende – und im Falle voriger Konfiguration durch den Kunden abgehende – E-Mail-Verkehr gescannt wird. Dafür wird der Verkehr über die A1 Mail Security Infrastruktur geroutet, was über eine Änderung des MX-Eintrags passiert.

4.2 Laufende Dienstleistungen

Die Infrastruktur wird im A1 NOC aufgebaut. Es werden die im Punkt 4.3 und 4.4 beschriebene Hardware und Software von A1 verwendet. A1 bleibt Eigentümer der bereitgestellten Hardware; hinsichtlich der im Punkt 4.4 beschriebenen Software, erwirbt der Kunde insbesondere kein Lizenzrecht, sondern nur die Möglichkeit die Applikationen, die für die Funktionalität des Produktes notwendig sind, für die Vertragsdauer zu nutzen.

Der zur Verfügung gestellte Dienst A1 Mail Security entspricht dem verfügbaren Stand der Technik bei der Bekämpfung von Spam E-Mails sowie Computerviren. Dennoch kann, insbesondere aufgrund der ständigen Neu- und Weiterentwicklung von Spam E-Mails und Software-Viren deren Mutationen oder die Entwicklung neuer, virenähnlicher Programme, ein vollständiger und absoluter Schutz (100%) vor Spam E-Mails sowie Virenbefall seitens A1 nicht ermöglicht werden. A1 übernimmt für etwaige daraus dem Kunden entstandene Schäden sowie für den Inhalt des durch den Kunden, z.B. in Form einer Werbezeile, beigefügten Text keinerlei Verantwortung, Gewähr oder sonstige Haftung. Haftungsansprüche etc. gegen A1, die insbesondere durch Spamming, Virenbefall oder

Kundeninhalte verursacht wurden, sind, soweit es gesetzlich zulässig ist, ausdrücklich ausgeschlossen. Der Kunde hält weiters A1 hinsichtlich sämtlicher von Dritter Seite erhobenen Ansprüche aufgrund Gewährleistung, Schadenersatz oder sonstig mit den Kundeninhalten in Zusammenhang stehend auf erstes Anfordern und in vollem Umfang schad- und klaglos.

4.2.1 Antivirus Services

Folgende Antivirus Leistungen werden dem Kunden bei A1 Mail Security zur Verfügung gestellt:

- Das Scannen des gesamten SMTP-Verkehrs auf einen eventuellen Virenbefall bekannter Viren mit Hilfe von verschiedenen Scan-Technologien.
- Das Erkennen von Viren in Dateien mit verschiedenen Packalgorithmen.
- Das Entfernen von E-Mails mit aufgefundenen Computerviren in E-Mails und Attachments. Bei entsprechender Konfiguration durch den Kunden wird jedoch das infizierte E-Mail zugestellt und auf dessen Gefahr hingewiesen.
- Die Information an den Kunden-IT-Administrator über Vorfälle.
- Das Blocken von definierten Dateien.
- Das selbständige Konfigurieren der Antivirus-Einstellungen über eine Web-Oberfläche.
- Das selbständige, individuelle Einfügen von Texten, z.B. einer Werbezeile für das Kundenunternehmen, über eine Web-Oberfläche.
- Das Konvertieren von E-Mails im HTML-Format auf Text-Format, z.B. gegen Password Fishing (Phishing), über eine Web-Oberfläche.
- Automatische Updates der Antiviren-Patterns.
- Statistiken und Reporting:
  - Information über Anzahl der verschickten E-Mails;
  - Information über das E-Mail-Aufkommen insgesamt;
  - Information über die Anzahl der gefundenen Viren;
  - Information über die Top 5 Viren;
  - Zugriff auf Informationsdatenbank über Computerviren für Beschreibung der Auswirkung der verschiedenen Viren;
  - Die Darstellung der Statistik kann vom Kunden aufgrund vorhandener Parameter individuell zusammengestellt werden.

Bei A1 Mail Security wird der E-Mail-Verkehr des Kunden auf einen eventuellen Virenbefall bekannter Viren geprüft, vireninfizierte E-Mails werden je nach Einstellung des Kunden zugestellt, entfernt oder gelöscht. Es werden Settings definiert, nach denen die Software auf den A1 Servern die ein- und ausgehenden E-Mails scannt. Kunden, die über mehrere Domains bei A1 verfügen und den darüber laufenden E-Mail-Verkehr auf Viren prüfen wollen, ist es frei gestellt, für jede Domain eigene beliebige Settings zu definieren.

Bei Kunden mit eigenen Mail-Servern, die auch den ausgehenden E-Mail-Verkehr scannen lassen, steht die Funktion „E-Mail-Umleitung“ nur eingeschränkt zur Verfügung. Die Funktion „Extern E-Mails empfangen und an externe Adresse umleiten“ wird nicht unterstützt. Möchte ein Kunde „E-Mail-Umleitung“ verwenden, so kann der gesamte ausgehende E-Mail-Verkehr nicht gescannt werden.

4.2.2 Antispam Services

Folgende Leistungen sind bei A1 Mail Security beinhaltet:

- Spam E-Mail-Prüfung des eingehenden E-Mail-Verkehr des Kunden aufgrund regelbasierender Technologien. Der Kunden-IT-Administrator kann Einstellungen

mittels zweier Regler treffen, der E-Mails als „Spam“, „Possible Spam“, „Regular Mail“ mittels eines Zählsystems klassifiziert.
- Klassifizierung und Bezeichnung aller Spam E-Mails durch Hinzufügen des Subject-Texts mit „Spam“ oder „Possible Spam“ und default-mäßige Zustellung an alle User oder Umleiten dieser klassifizierten E-Mails auf gesonderte E-Mail Boxen oder Löschen dieser E-Mails (vom Kunden-IT-Administrator festzulegen).
- Konfiguration von White Lists: Werden erwünschte und/oder reguläre E-Mails als „Spam“ klassifiziert, kann der Kunden-IT-Administrator bestimmte Regeln definieren, damit diese E-Mails trotzdem zum Empfänger gelangen. Trifft auf eine E-Mail eine solche Regel zu, wird nicht mehr überprüft, ob sie als Spam zu klassifizieren ist oder nicht, sondern wird sofort zugestellt. Bei den genannten Regeln handelt es sich um Keywords, die wahlweise in Absender-E-Mail-Adresse, Empfänger-E-Mail-Adresse, im Subject und Body überprüft werden.
- Konfiguration von Black Lists: Es wird dem Kunden-IT-Administrator ermöglicht, nach Kriterien (Absender-E-Mail-Adresse, Empfänger-E-Mail-Adresse, Keywords im Subject und Keywords im Body) festzulegen, welche E-Mails trotzdem als Spam behandelt werden, obwohl sie zuvor als reguläres E-Mail eingestuft waren.
- Automatische Updates der Antispam-Software.
- Statistiken und Reporting:
  - Auswertung der Anzahl der E-Mails;
  - Generierter Traffic mit Anzahl der als Spam klassifizierten E-Mails;
  - Welche Regel (White List und Black List) wie oft gegriffen hat – dadurch können die Regeln optimiert werden;
  - Die Darstellung der Statistik kann vom Kunden aufgrund vorhandener Parameter individuell zusammengestellt werden.

4.2.3 Service Desk

Dem Kunden-IT-Administrator steht ein Service Desk werktags, Montag bis Samstag von 7:00 bis 19:00 Uhr, ausgenommen 24.12. und 31.12. für Support-Anfragen zu A1 Mail Security zur Verfügung.

4.3 Hardware

Die Hardware ist entsprechend des Traffic-Aufkommens des Kunden sehr leistungsfähig, skalierbar und ausfallsicher in zwei verschiedenen Rechenzentren aufgebaut.

4.4 Software

Bei der mandantenfähigen Antispam-Lösung kommt in erster Linie ein intelligentes Greylisting zum Einsatz, welches über Reverse-Lookup Kontrolle, SPF-Check, FQDN-Check und weitere Funktionen die Absenderseite von E-Mails bewertet. In zweiter Linie kommt ein Antispam-Modul des Software-Herstellers IKARUS zum Einsatz, das mittels verschiedenster Methoden und selbstlernenden Algorithmen E-Mails regelbasierend klassifiziert.

Die mandantenfähige Virenschutz-Lösung beschreibt sich durch folgende Eigenschaften:

- Scanning des gesamten Simple Mail Transfer Protocol (SMTP)-Verkehrs mit Hilfe von 3 verschiedenen Scantechnologien (IKARUS T3 Scanner);
- Unterstützung von 17 verschiedenen Packalgorithmen (zip, arj, rar, tar, etc.);
- Entfernung von gefundenen Computerviren in E-Mails und Attachments;
- Blocking beliebig definierbarer Dateien.

Änderungen der Software behält sich A1 jederzeit vor.

5 A1 Web Security

A1 Web Security kann ab 04. Mai 2020 nicht mehr neu bestellt werden.

Mit einer mandantenfähigen (vom Kunden selbst individuell einstellbaren) Proxy-Lösung wird der HTTP-Verkehr des Kunden, bevor er zu den Internet Arbeitsplätzen der User gelangt, zentral auf Malware (Schadsoftware) und nicht freigegebene Web-Sites mittels URL-Filtering untersucht. Voraussetzung für die Inanspruchnahme von A1 Web Security ist der Bezug eines fixen A1 Business Breitband Internet-Zugangs.

A1 Web Security schützt vor Web-Sites unerwünschten Inhalts und eventuell schädlichen Programmen wie zum Beispiel Viren, Würmern oder Trojaner. Dazu wird der Proxyserver-Eintrag im Web-Browser der User geändert. Alternativ – nach Prüfung der technischen Machbarkeit durch den A1 Service Desk – kann der Proxyserver-Eintrag am Router des A1 Business Breitband Internet-Zugangs konfiguriert werden. Dabei ist es möglich, den einzelnen offiziellen IP-Adressen des Kunden verschiedene Regeln zuzuweisen, nach denen der HTTP-Verkehr gescannt werden soll. Über eine Web-Oberfläche gelangt der Kunde oder sein IT-Administrator mittels Username und Password zu den kundenspezifischen Konfigurationen.

Der Kunde erklärt sich ausdrücklich damit einverstanden, dass HTTP-Verkehr anhand der vom Kunden individuell festzulegenden Parameter auf Schadsoftware untersucht wird. Die Konfiguration liegt in der alleinigen Verantwortung des Kunden. Der Kunde ist verpflichtet, bestehende rechtliche, insbesondere arbeits- und datenschutzrechtliche Bestimmungen einzuhalten.

5.1 Einmalige Dienstleistungen

A1 Web Security wird nach Vorkonfiguration durch A1 und nachfolgender Einstellungen durch den Kunden aktiviert. Der Verkehr wird über die A1 Web Security Infrastruktur geroutet, was über eine Änderung des Proxyserver-Eintrags im Web-Browser durch den Kunden oder alternativ nach Prüfung der technischen Machbarkeit am Internet-Router durch A1 passiert.

5.2 Laufende Dienstleistungen

Die Infrastruktur wird im A1 NOC aufgebaut. Es werden die im Punkt 5.3 und 5.4 beschriebene Hardware und Software von A1 verwendet. A1 bleibt Eigentümer der bereitgestellten Hardware; hinsichtlich der im Punkt 5.4 beschriebenen Software, erwirbt der Kunde insbesondere kein Lizenzrecht, sondern nur die Möglichkeit die Applikationen, die für die Funktionalität des Produktes notwendig sind, für die Vertragsdauer zu nutzen.

Der zur Verfügung gestellte Dienst A1 Web Security entspricht dem verfügbaren Stand der Technik bei der Bekämpfung von unerwünschten Web-Inhalten. Dennoch kann, insbesondere aufgrund der ständigen Neu- und Weiterentwicklung von Schadsoftware und Angriffstechniken, ein vollständiger und absoluter Schutz (100%) seitens A1 nicht ermöglicht werden. A1 übernimmt für etwaige daraus dem Kunden entstandene Schäden keinerlei Verantwortung, Gewähr oder sonstige Haftung. Haftungsansprüche etc. gegen A1 sind, soweit es gesetzlich zulässig ist, ausdrücklich ausgeschlossen. Der Kunde hält weiters A1 hinsichtlich sämtlicher von Dritter Seite erhobenen Ansprüche aufgrund Gewährleistung, Schadenersatz oder sonstig mit den Kundeninhalten in Zusammenhang stehend auf erstes Anfordern und in vollem Umfang schad- und klaglos.

5.2.1 Antimalware und URL-Filtering Services

Folgende Leistungen sind bei A1 Web Security beinhaltet:

- Das Scannen des HTTP-Verkehrs des Kunden in Echtzeit.
- Das Verhindern des Downloads von Viren, Trojanern und Würmern, Adware, Spyware und Keylogger, Rootkits und Backdoors, sowie Malicious Code.
- Das Filtern und Blocken von Web-Sites unerwünschten Inhalts.
- Die Filterung von unerwünschten Dateitypen und Downloads aus dem Datenverkehr.
- Das selbständige Konfigurieren der Einstellungen über eine Web-Oberfläche.
- Automatische Updates der Viren- und URL-Filtering-Datenbanken.
- Statistiken und Reporting:
  - Auswertung der Anzahl der Proxy-Requests;
  - Generierter Traffic mit Anzahl der geblockten Web-Sites;
  - Information über die Top 5 Viren;
  - Information über die Top 5 geblockten Web-Sites;
  - Die Darstellung der Statistik kann vom Kunden aufgrund vorhandener Parameter individuell zusammengestellt werden.

Bei A1 Web Security werden Settings definiert, nach denen die Software auf den A1 Servern den HTTP-Verkehr scannt. Kunden, die über mehrere offizielle IP-Adressen bei A1 verfügen und den darüber laufenden HTTP-Verkehr prüfen wollen, ist es frei gestellt, für jede IP-Adresse eigene beliebige Settings zu definieren.

Der Einsatz von A1 Web Security als Reverseproxy-Lösung, bei Kunden mit eigenen Web-Servern, ist nicht möglich.

5.2.2 Service Desk

Dem Kunden-IT-Administrator steht ein Service Desk werktags, Montag bis Samstag von 7:00 bis 19:00 Uhr, ausgenommen 24.12. und 31.12. für Support-Anfragen zu A1 Web Security zur Verfügung.

5.3 Hardware

Die Hardware ist entsprechend des Traffic-Aufkommens des Kunden sehr leistungsfähig, skalierbar und ausfallsicher in zwei verschiedenen Rechenzentren aufgebaut.

5.4 Software

Für die mandantenfähige Proxy-Lösung kommt Software des Herstellers IKARUS zum Einsatz, die sich durch folgende Eigenschaften beschreibt:

- Innovative Scantechnologie: Pattern-Scanning, heuristisches Scanning und heuristisches Script-Scanning;
- Effektives URL-Filtering von IKARUS: Verschiedenste Themengruppen können ausgewählt werden, um unterschiedliche User-Gruppen zu schützen;
- MIME-Type Blocking: Filtert unerwünschte Attachments und Downloads aus dem Datenverkehr;
- IP-Address-Grouping: Dieses Feature ermöglicht das Erstellen von verschiedenen User-Gruppen mit Regeln auf Basis von IP-Adressen;
- Proxy Authentication: Dieses Feature ermöglicht IT-Administratoren z.B. an Teleworker ein Zugriffspasswort für die Proxy-Nutzung zu vergeben.

Änderungen der Software behält sich A1 jederzeit vor.

6 A1 Desktop Security

A1 Desktop Security wird mit 06. Juli 2020 eingestellt.

Das Produkt A1 Desktop Security besteht aus einer dezentralen Client-Software für Antivirus & Antispyware, Firewall, Intrusion Prevention und bietet weitreichenden Schutz am/an Kunden Laptops, Desktops und Server. Nach Bestellung von A1 Desktop Security wird ein Download-Link auf einer Web-Oberfläche dargestellt. Die bereit gestellte Software ist vom Kunden nach dem Download auf seinen Arbeitsplätzen oder Server zu installieren. Nutzungsvoraussetzung und nicht Leistungsinhalt von A1 Desktop Security ist ein fixer A1 Business Breitband Internet-Zugang.

Es gelten die 6.1 beschriebenen Hardware- und Betriebssystemanforderungen an die Arbeitsplätze und Server des Kunden; hinsichtlich der im Punkt 6.2 genannten Software, erwirbt der Kunde insbesondere kein Lizenzrecht, sondern nur die Möglichkeit die Applikationen, die für die Funktionalität des Produktes notwendig sind, für die Vertragsdauer zu nutzen.

Zum anderen besteht das Produkt A1 Desktop Security aus einer zentralen Web-basierenden Applikation zur Verwaltung der dezentralen Clients. Die Einstellungen der Clients sind in sogenannten Policies festlegbar (von A1 vorkonfiguriert) für die Komponenten Antivirus & Antispyware, Firewall, Intrusion Prevention und Proaktiver Bedrohungsprüfung. Die Einstellungen der Clients können durch die User geändert werden, nach Zuweisung von Berechtigungsprofilen durch den Kunden oder seinen IT-Administrator:

- „Hohe Sicherheit“ – vorkonfigurierte Policy, User darf Komponenten nicht konfigurieren bzw. deaktivieren;
- „Mittlere Sicherheit“ – User darf Komponenten konfigurieren;
- „Niedrige Sicherheit“ – User darf Komponenten deaktivieren.

Weiters bietet die zentrale Applikation die Möglichkeit der automatischen Erstellung von Sicherheitsberichten über aktuelle Informationen zum Sicherheitsstatus der Endgeräte für eine Überwachung des Netzwerks durch den Kunden-IT-Administrator.

Dem Kunden-IT-Administrator steht ein Service Desk werktags, Montag bis Samstag von 7:00 bis 19:00 Uhr, ausgenommen 24.12. und 31.12. für Support-Anfragen zu A1 Desktop Security zur Verfügung. Ein über das Produkt hinausgehender, etwa persönlicher Support (etwa EDV-Support und Unterstützung bei Problemen mit Computer, Betriebssystemen, Router und Netzwerkkonfigurationen durch den Service Desk) ist nicht Teil der Leistung A1 Desktop Security.

Die zur Verfügung gestellte Software entspricht dem verfügbaren Stand der Technik hinsichtlich Endgerätesicherheit. Updates werden mittels einer in der Software integrierten Live-Update-Funktion automatisch durchgeführt. Dennoch kann, insbesondere aufgrund der ständigen Neu- und Weiterentwicklung von Schadsoftware und Angriffstechniken, ein vollständiger und absoluter Schutz (100%) seitens A1 nicht ermöglicht werden. A1 übernimmt für etwaige daraus dem Kunden entstandene Schäden keinerlei Verantwortung, Gewähr oder sonstige Haftung. Haftungsansprüche etc. gegen A1 sind, soweit es gesetzlich zulässig ist, ausdrücklich ausgeschlossen. Der Kunde hält weiters A1 hinsichtlich sämtlicher von Dritter Seite erhobenen Ansprüche aufgrund Gewährleistung, Schadenersatz oder sonstig mit den Kundeninhalten in Zusammenhang stehend auf erstes Anfordern und in vollem Umfang schad- und klaglos.

6.1 Hardware

Systemanforderungen für Windows:

- 32-bit Prozessor für Windows: ab 2-GHz Intel Pentium III (empfohlen Intel Pentium 4) oder kompatibler Prozessor
- 64-bit Prozessor für Windows: ab 2-GHz Pentium 4 mit x86-64 Unterstützung oder kompatibler Prozessor, Itanium Prozessoren werden nicht unterstützt
- Arbeitsspeicher mindestens 1 GB RAM (empfohlen 2 GB) oder höher falls seitens Betriebssystem erforderlich
- Festplatte mindestens 900 MB

6.2 Software

Für die mandantenfähige Endgerätesicherheits-Lösung wird die Software Symantec Endpoint Protection verwendet. Änderungen der Software behält sich A1 jederzeit vor.

Systemanforderungen Windows -Betriebssysteme:

- Windows 10 (32-bit, 64-bit)
- Windows 7 (32-bit, 64-bit; RTM und SP1), Windows 7 Embedded Standard
- Windows 8 (32-bit, 64-bit), Windows 8 Embedded (32-bit)
- Windows 8.1 (32-bit, 64-bit) Windows 8.1 embedded (32-bit)
- Windows Server 2008 (32-bit, 64-bit; R2, SP1 und SP2),
- Windows Essential Business Server 2008 (64-bit)
- Windows Small Business Server 2011 (64-bit)
- Windows Server 2012 (sowie R2, R2 Update 4/2014, R2 Update 8/2014))