



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

Allgemeines

Diese Leistungsbeschreibung gilt ab 14. Juni 2011 für neue Bestellungen. Die auf Grundlage bisheriger veröffentlichter vormaliger LB IT Security abgeschlossenen Verträge bleiben – abgesehen von der Produktnamensänderung – unverändert aufrecht.

A1 Telekom Austria erbringt im Rahmen ihrer technischen und betrieblichen Möglichkeiten A1 IT Security Services nach den Bestimmungen des Telekommunikationsgesetzes (TKG 2003), den Allgemeinen Geschäftsbedingungen für Solutions der A1 Telekom Austria (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 der A1 Telekom Austria, 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 IT Security Solutions, 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.
- Content Security Services bestehen aus den Produkten 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.
- 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 Telekom Austria 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. IT Security Solutions,
2. A1 Professional Secure,
3. A1 Central Firewall,
4. A1 Mail Security,
5. A1 Web Security,
6. A1 Desktop Security.

A1 Telekom Austria lädt den Kunden nach erfolgter Realisierung der gewünschten IT-Security Services zur Abnahme ein. Nimmt die Erfüllung des Auftrags aufgrund der Größe oder Komplexität der Leistung mehrere Monate in Anspruch, ist A1 Telekom Austria 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 Telekom Austria zu vertreten sind, beginnt die Fakturierung mit der Bereitstellung der Leistung.

1 IT Security Solutions

1.1 Produktbeschreibung mit Hardware und Software

A1 Telekom Austria implementiert spezielle IT-Security Lösungen, 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 Telekom Austria 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 der Hardware-Wartung gem. Punkt 1.3.1 (DHS) 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 Telekom Austria 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 die IT Security Solutions 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 Telekom Austria im Zuge der Projektplanung.



1.2 Einmalige Dienstleistungen

1.2.1 Installation von Hardware und Software

A1 Telekom Austria implementiert die gem. Punkt 1.1 beschriebenen Komponenten und führt einen Test im Kundennetz durch. A1 Telekom Austria kann die Installation ausschließlich bei Vorhandensein von insbesondere eines funktionierenden Internet-Zuganges und einer funktionierenden Stromversorgung durchführen. Bei nicht von A1 Telekom Austria betriebenen Sicherheits-Systemen kann auf Anfrage des Kunden und gegen gesondertes Entgelt gem. Punkt 1.4.8 während oder nach der Installation eine Einweisung des Kunden durchgeführt werden.

1.2.2 Support

Bei Nicht-Inanspruchnahme des Wartungsdienstes gem. Punkt 1.3 bietet A1 Telekom Austria Wartungsdienstleistungen wie die Installation von Software-Upgrades und Major Release-Wechsel (z.B. Software-Versionswechsel von 2.0 auf 3.0) auf Anfrage und gegen gesondertes Entgelt (Verrechnung nach Aufwand). Die hierzu erforderlichen Arbeiten erfolgen werktags (Montags bis Freitags von 8:00 bis 17:00 Uhr, ausgenommen 24.12. und 31.12.) in Absprache mit dem Kunden. Dabei ist A1 Telekom Austria zur Außerbetriebnahme des Systems berechtigt. Die im Punkt 1.3 garantierten Leistungsmerkmale kommen hier nicht zur Anwendung.

1.3 Laufende Dienstleistungen

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

Hinweis: A1 Telekom Austria ist ausschließlich bei von ihr gewarteten Geräten verpflichtet, die u.a. Supportzeiten (z.B. Entstör- oder Konfigurationszeiten) einzuhalten. Weiters ist der Kunde verpflichtet, bevor er eine Störungsmeldung im Bereich einer Firewall oder einer VPN-Verbindung an A1 Telekom Austria übermittelt, zu überprüfen, ob die Internet Connectivity und die Stromversorgung funktioniert.

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

A1 Telekom Austria bietet Support Service (d.h. Wartungsdienstleistungen) in zwei Varianten an:

- Data Solutions Hardware Service (DHS): nur Hardware-Wartung bei Störung,
- Data Solutions Comprehensive Service (DCS): Hardware- und Software-Wartung bei Störung.

A1 Telekom Austria wird bei Inanspruchnahme von Support Service die Störungsbehebung von Fehlern der Hardware (DHS) und/oder von Hard- und Software (DCS) auch vor Ort übernehmen (On Site Service).



Das Support Service 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 Telekom Austria 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 Telekom Austria durchgeführt werden.

Als störungsrelevante Ereignisse können nur solche herangezogen werden, die in Form einer Störungsmeldung des Kunden an A1 Telekom Austria gemeldet werden und die zu einer Störungsbehebung durch A1 Telekom Austria geführt haben. Fremdverzögerungen sind Verzögerungszeiten, welche die Entstörungen beeinflussen und vom Kunden oder Dritten, die dem Kunden zu Vertragsleistungen verpflichtet sind, verursacht werden.

Die Störungsbehebung erfolgt gemäß den unten angeführten Reaktions- und Entstörzeiten je nach der vom Kunden gewählten Ausprägung:

- Regular Support (8 Stunden Reaktionszeit, 48 Stunden Entstörzeit),
- Priority Support (4 Stunden Reaktionszeit, 24 Stunden Entstörzeit).

Weiters werden drei Varianten von Störungsannahmen angeboten:

- Standard Service (werktags*, Montag bis Freitag von 8:00 bis 17:00 Uhr),
 - Handel Service (werktags*, Montag bis Samstag von 7:00 bis 19:00 Uhr),
 - 7x24 Service (werktags*, Montag bis Sonntag von 0:00 bis 24:00 Uhr).
- * ausgenommen 24.12. und 31.12.

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

Zeiten außerhalb der Verfügbarkeit des Support Services werden in den oben genannten Reaktionszeiten und Entstörzeiten nicht eingerechnet.

1.3.1.1 Reaktionszeit

A1 Telekom Austria behält sich eine Reaktionszeit für Hardware Service (DHS) und Hard- und Software Service (DCS) gemäß der unter 1.3.1 definierten Parametern vor.

Die Reaktionszeit ist der Zeitraum zwischen der Störungsmeldung durch den Kunden und der Bestätigung der Störungsübernahme durch die für die Störungsbehebung verantwortliche Stelle der A1 Telekom Austria. Die Bestätigung der Störungsübernahme erfolgt telefonisch oder auf elektronischem Weg. Kann eine Bestätigung der Störungsübernahme, aus Gründen, die nicht von A1 Telekom Austria zu vertreten sind, nicht erfolgen, gilt dies als Fremdverzögerung. Nach der Bestätigung der Störungsübernahme wird unverzüglich mit der Störungseingrenzung begonnen.

1.3.1.2 Entstörzeit

A1 Telekom Austria beseitigt die Störung bei Hardware Service (DHS) und Hard- und Software Service (DCS) gemäß der unter 1.3.1 definierten Parametern. Die Entstörzeit ist eingehalten, wenn dem Kunden innerhalb der 48 (im Falle eines Regular Supports) oder 24



Stunden (im Falle eines Priority Supports) die Funktionalität des Systems wiederhergestellt ist oder dem Kunden ein adäquater Ersatz zur Verfügung gestellt wurde.

Als Entstörzeit gilt der Zeitraum zwischen der Störungsmeldung durch den Kunden und dem Abschluss der Störungsbehebung, welche durch die Gutmeldung an den Kunden bestätigt wird. Eventuelle Verzögerungszeiten bei der Entstörung, die nicht durch A1 Telekom Austria verursacht werden, werden in der Entstörzeit nicht berücksichtigt und gelten als Fremdverzögerung. Ebenso werden Verzögerungen, die gegebenenfalls durch Updates, Patches oder Fixes seitens des Software/Hardwareherstellers erforderlich werden, in der Entstörzeit nicht berücksichtigt.

1.3.1.3 Gutmeldung

A1 Telekom Austria informiert den Kunden nach Beendigung der Störung. Die Gutmeldung dient als Bestätigung der erfolgreich abgeschlossenen Entstörung und erfolgt unmittelbar nach dem Abschluss der Störungsbehebung.

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

Darüber hinaus betreibt A1 Telekom Austria folgende IT Security-Systeme, die auf einem von ihr erstellten Konzept und einer von ihr formulierten IT-Sicherheitspolitik basieren, im Rahmen von abgestuften „Managed Security Paketen“. Bei Inanspruchnahme dieser Pakete stellt A1 Telekom Austria eine proaktive Fehlerbehebung zur Verfügung.

Änderung am System können nur durch A1 Telekom Austria durchgeführt werden.

Es werden folgende Managed Security Pakete angeboten:

1.3.2.1 Firewall Management bei Cisco und Barracuda

1.3.2.1.1 Überwachung und Betrieb der Firewall

A1 Telekom Austria überwacht und betreibt das Firewall-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 der Firewall werden kritische Ereignisse des Systems erkannt. Bei Eintritt eines kritischen Ereignisses wird das Network Operation Center (NOC) der A1 Telekom Austria automatisch alarmiert. Eine Analyse der Alarmsituation wird innerhalb der vereinbarten Zeiten durchgeführt oder 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 Telekom Austria erstellt periodisch sowie nach jeder Änderung eine Sicherheitskopie der zur Wiederherstellung der Firewall-Funktionalität benötigten Daten.

1.3.2.1.4 Updates, Patches und Fixes

In Absprache mit dem Kunden führt A1 Telekom Austria Anpassungen der Firewall- 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 Telekom Austria zur Außerbetriebnahme der Firewall berechtigt.

1.3.2.1.5 Verschlüsselter Datenaustausch (VPN-Client, Site-to-Site-VPN, SSL-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-VPNs ermöglicht werden. Ebenso ist es möglich, durch A1 Telekom Austria-Firewalls gesicherte Außenstellen über Site-to-Site-VPNs an die Zentrale anzubinden. Die Konfiguration auf der Firewall wird durch A1 Telekom Austria durchgeführt.

1.3.2.1.6 Änderungen an der Firewall-Konfiguration

In Absprache mit dem Kunden können Standard-Änderungen an der Firewall-Konfiguration ein Mal pro Woche 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 Telekom Austria 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 Firewall Management bei Check Point

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 eines umfassenden Reportings. Änderungen oder Erweiterungen an der Firewall-Konfiguration können von A1 Telekom Austria bis zu vier Stunden pro Woche zu den unter 1.3.2.1.6 beschriebenen Zeiten vorgenommen werden.

Reporting

A1 Telekom Austria stellt autorisierten Mitarbeitern des Kunden bei Bedarf Reports bereit. Die kundenindividuellen Reports werden mittels zentralem 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:

1.3.2.2.1 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.

1.3.2.2.2 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.

1.3.2.2.3 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).

1.3.2.3 Virus Prevention Management

Bei Inanspruchnahme von Firewall Management gemäß 1.3.2.1 und 1.3.2.2 ermöglicht A1 Telekom Austria 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 Telekom Austria 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 des Betriebssystems;
- Updates der Software Releases;
- Regelmäßiges Update der Virenpatterns;
- Backup;
- Alerting bei gefundenen Viren.



1.3.2.4 Proxy Security Services

A1 Telekom Austria 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 Telekom Austria 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;
- Ermöglichung von Berechtigungsprofilen aufgrund unterschiedlicher offizieller IP-Adressen;
- Backup;
- Reporting.

1.3.2.5 Intrusion Prevention Management

Bei Inanspruchnahme von Firewall Management gemäß 1.3.2.1 und 1.3.2.2 ermöglicht A1 Telekom Austria 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 Module (bei Check Point und Barracuda) angesprochen oder mittels dedizierten Komponenten (Radware) eingesetzt werden. A1 Telekom Austria 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;
- Alerting bei Angriffen oder Anomalien.

1.4 Optionen

Da es sich bei IT Security Solutions um Lösungen für spezielle Kundenanforderungen handelt, werden verschiedene Optionen zusätzlich angeboten.



1.4.1 Workshop

A1 Telekom Austria 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.

1.4.2 Konzeptvorschlag

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

1.4.3 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 Dienstrechnern;
- Festlegung der Anzahl der offiziellen IP-Adressen;
- Dienstkonzepte 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.



1.4.4 IT-Sicherheitspolitik

Die IT-Sicherheitspolitik enthält zusätzlich zum Ergebnis des unter Punkt 1.4.2 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.

1.4.5 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 Telekom Austria 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.

1.4.6 DNS-Server

A1 Telekom Austria verkauft, installiert und betreibt auf Basis des Konzeptes und der IT-Sicherheitspolitik die zur Nutzung des Domain Name Services in Firewall-gesicherten Netzwerken benötigte Hard- und Software (DNS-Server). Der DNS-Server kann sowohl als Secondary- als auch als Primary-DNS-Server installiert werden. Die Installation beinhaltet die Eintragung einer Zone. Der Dienst DNS-Server setzt voraus, dass der Kunde bereits ein Domain Name Service besitzt.

1.4.7 Security Assessment

1.4.7.1 Check vor Angriffen

A1 Telekom Austria attackiert mit entsprechender Einwilligung des Kunden dessen IT Security-System oder versucht in das Security-System des Kunden einzudringen. Dabei werden die üblichen, am Internet frei und/oder kommerziell verfügbaren Tools zu einem nicht näher definierten Punkt in einer Zeitspanne von etwa zwei Wochen eingesetzt.

1.4.7.2 Prüfen der Konfigurations-Files und Dokumentation

Die Konfigurations-Files der relevanten Komponenten werden vor Ort geprüft. Bei dieser Gelegenheit werden auch das Know How und die Einstellung der Sicherheitsverantwortlichen gecheckt. Die Kontrolle der relevanten Dokumentation zu den Sicherheitskomponenten und



der Sicherheits-Policy mit User-Richtlinien, Notfall-Plan, Kommunikationsrichtlinien und Schulungsplan runden den Test ab. Mögliche Mängel werden aufgedeckt und dokumentiert.

1.4.7.3 Abschluss des Security Assessments

Der Kunde hat die Wahl zwischen einer Management-Präsentation des aufgrund des Security Assessments verfassten Berichtes oder einer nochmaligen Überprüfung von außen zwei Wochen nach Übergabe des Berichts.

1.4.8 Schulungen

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

2 A1 Professional Secure

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

2.1 Einmalige Dienstleistungen

A1 Telekom Austria implementiert die Komponenten der Firewall und führt einen Test im Kundennetz durch. Für die Installation ist ein fixer A1 Business Breitband Internet-Zugang der A1 Telekom Austria 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 Telekom Austria bereitgestellt. Weiters ist standardmäßig die Hardware-Wartung von Punkt 1.3.1 in der Ausprägung Regular und der Variante Standard inkludiert. Optional wird die Management-Leistung von Punkt 1.3.2.1 angeboten. A1 Telekom Austria ist ausschließlich bei von ihr gewarteten Geräten verpflichtet, Supportzeiten (z.B. Entstör- oder Konfigurationszeiten) einzuhalten. Weiters ist der Kunde verpflichtet, bevor er eine Störungsmeldung im Bereich einer Firewall oder einer VPN-Verbindung an A1 Telekom Austria übermittelt, zu überprüfen, ob die Internet Connectivity und die Stromversorgung funktioniert. A1 Telekom Austria bleibt Eigentümer der bereitgestellten Hardware; hinsichtlich der im Punkt 2.4 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.



2.3 Hardware

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

- In- & Outbound Traffic, 10 User;
- In- & Outbound Traffic, Unlimited User;
- In- & Outbound & DMZ Traffic, Unlimited User.

2.4 Software

Für die Erbringung des Services wird Software von Cisco Systems 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 NOC der A1 Telekom Austria, da die Hardware für diesen Dienst nur ein Interface für die Internet Connectivity aufweist.

3.1 Einmalige Dienstleistungen

A1 Telekom Austria sorgt dafür, dass der IP-Verkehr des Kunden aus dem und in das private Netz über dessen A1 Central Firewall-Instanz geroutet wird. Dafür ist ein Zugang zum Netzwerk 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 Telekom Austria verwendet. A1 Telekom Austria 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, 19:00 bis 4:00 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 1.3.2.2.3.



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):

- VPN-1 VSX Gateway;
- VLAN Trunking-Fähigkeit;
- Zentrales Management;
- Remote VPN Access;
- URL-Filtering.

4 A1 Mail Security

Mit einer mandantenfähigen (vom Kunden selbst individuell einstellbaren) Antispam- und Virenschutzlösung wird der E-Mail-Verkehr des Kunden, bevor er in die E-Mail Boxen der Nutzer 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 der A1 Telekom Austria. 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 Relay 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 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 vireninfierten 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 vireninfierten 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 Telekom Austria, nachfolgender Einstellungen durch den Kunden und entsprechender Verständigung des A1 Service Teams aktiviert. Nach dieser Mitteilung des Kunden sorgt A1 Telekom Austria 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 NOC der A1 Telekom Austria aufgebaut. Es werden die im Punkt 4.3 und 4.4 beschriebene Hardware und Software von A1 Telekom Austria verwendet. A1 Telekom Austria 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 Softwareviren deren Mutationen oder die Entwicklung neuer, virenähnlicher Programme, ein vollständiger und absoluter Schutz (100%) vor Spam E-Mails sowie Virenbefall seitens A1 Telekom Austria nicht ermöglicht werden. A1 Telekom Austria 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 Telekom Austria, die insbesondere durch Spamming, Virenbefall oder Kundeninhalte verursacht wurden, sind, soweit es gesetzlich zulässig ist, ausdrücklich ausgeschlossen. Der Kunde hält weiters A1 Telekom Austria 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 Virenschutzeinstellungen 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, vireninfiizierte E-Mails werden je nach Einstellung des Kunden zugestellt, entfernt oder gelöscht. Es werden Settings definiert, nach denen die Software auf den A1 Telekom Austria Servern die ein- und ausgehenden E-Mails scannt. Kunden, die über mehrere Domains bei A1 Telekom Austria 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 Nutzer 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 Support

Support durch das A1 Service Team:

- Annahme der Störung im First Level: Mo-So 0:00-24:00;
- Verfügbarkeit eines Technikers:
werktags, ausgenommen 24.12. und 31.12., Mo-Sa 7:00-19:00.

4.3 Hardware

Die Hardware ist entsprechend des Traffic-Aufkommens des Kunden sehr leistungsfähig und skalierbar.

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 Security-Softwareherstellers IKARUS zum Einsatz, das mittels verschiedenster Methoden und selbstlernenden Algorithmen E-Mails regelbasierend klassifiziert.

Die mandantenfähige Virenschutzlösung 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 Telekom Austria jederzeit vor.

5 A1 Web Security

Mit einer mandantenfähigen (vom Kunden selbst individuell einstellbaren) Proxy-Lösung wird der HTTP-Verkehr des Kunden, bevor er zu den Internet Arbeitsplätzen der Nutzer 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 der A1 Telekom Austria. 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 Nutzer geändert. 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 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 Telekom Austria und nachfolgender Einstellungen durch den Kunden aktiviert. Der Verkehr wird über die A1 Web Security Infrastruktur geroutet, was über eine Änderung des Proxyserver-Eintrags durch den Kunden passiert.

5.2 Laufende Dienstleistungen

Die Infrastruktur wird im NOC der A1 Telekom Austria aufgebaut. Es werden die im Punkt 5.3 und 5.4 beschriebene Hardware und Software von A1 Telekom Austria verwendet. A1 Telekom Austria 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 Telekom Austria nicht ermöglicht werden. A1 Telekom Austria übernimmt für etwaige daraus dem Kunden entstandene Schäden keinerlei Verantwortung, Gewähr oder sonstige Haftung. Haftungsansprüche etc. gegen A1 Telekom Austria sind, soweit es gesetzlich zulässig ist, ausdrücklich ausgeschlossen. Der Kunde hält weiters A1 Telekom Austria 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 Telekom Austria Servern den HTTP-Verkehr scannt. Kunden, die über mehrere offizielle IP-Adressen bei A1 Telekom Austria 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 Support

Support durch das A1 Service Team:

- Annahme der Störung im First Level: Mo-So 0:00-24:00;
- Verfügbarkeit eines Technikers:
werktags, ausgenommen 24.12. und 31.12., Mo-Sa 7:00-19:00.

5.3 Hardware

Die Hardware ist entsprechend des Traffic-Aufkommens des Kunden sehr leistungsfähig und skalierbar.

5.4 Software

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

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

Änderungen der Software behält sich A1 Telekom Austria jederzeit vor.

6 A1 Desktop Security

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 der A1 Telekom Austria.



Es gelten die im Punkt 6.1 und 6.2 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 Telekom Austria vorkonfiguriert) für die Komponenten Antivirus & Antispyware, Firewall, Intrusion Prevention und Proaktiver Bedrohungsprüfung. Die Einstellungen der Clients können durch die Nutzer geändert werden, nach Zuweisung von Berechtigungsprofilen durch den Kunden oder seinen Administrator:

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

Support durch das A1 Service Team für Client-Software und zentrale Applikation:

- Annahme der Störung im First Level: Mo-So 0:00-24:00;
- Verfügbarkeit eines Technikers: werktags, ausgenommen 24.12. und 31.12., Mo-Sa 7:00-19:00.

Ein über das Produkt hinausgehender, etwa persönlicher Support (etwa EDV-Support und Unterstützung bei Problemen mit Computer, Betriebssystemen, Router und Netzwerkkonfigurationen durch das A1 Service Team) 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 Telekom Austria nicht ermöglicht werden. A1 Telekom Austria übernimmt für etwaige daraus dem Kunden entstandene Schäden keinerlei Verantwortung, Gewähr oder sonstige Haftung. Haftungsansprüche etc. gegen A1 Telekom Austria sind, soweit es gesetzlich zulässig ist, ausdrücklich ausgeschlossen. Der Kunde hält weiters A1 Telekom Austria 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:

- Intel Pentium-Prozessor oder kompatible Architektur (32-Bit und 64-Bit);
- Itanium wird nicht unterstützt;
- Arbeitsspeicher mindestens 256 MB RAM;
- Festplatte mindestens 600 MB.



6.2 Software

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

Systemanforderungen Windows-Betriebssysteme 32-Bit und 64-Bit Versionen:

- Windows 2000 Professional, Server, Advanced Server, Datacenter Server ab Service Pack 3;
- Windows XP Home, Tablet PC, Media Center 2002, Professional ab Service Pack 1;
- Windows Vista Home Basic, Home Premium, Business, Enterprise, Ultimate;
- Windows Server 2003 Standard, Enterprise, Datacenter, Storage, Web, Cluster, Small Business Server ab Service Pack 1;
- Windows Server 2008 Standard, Enterprise, Datacenter, Web, Core, Small Business Server Standard und Premium, Essential Business Server Standard und Premium;
- Windows 7.