redIT

REDIT MANAGED FIREWALL DEDICATED & SHARED

Leistungsbeschreibung / Nutzungsbedingung

Inhaltsverzeichnis

1 SERVICE LEVELS

- Die jährliche garantierte Verfügbarkeit der Services beträgt 99.5%. redIT stellt während dieser Zeit den reibungslosen Betrieb der gesamten Umgebung sicher und nimmt Anpassungen und Fehlerbehebungen vor, die nötig sind, um den Betrieb sicherzustellen.
- 7 X 24h Störungsannahme (E-Mail und *Telefon)
  (*nur für Kunden mit separatem Wartungsvertrag; ansonsten gilt Mo - Fr, 07:00 - 17:00 Uhr)
- Maximal 2h Reaktionszeit (Mo - Fr, 07:00 - 17:00 Uhr)

2 EINLEITUNG

Unsere redIT Managed Firewall basiert auf einer mehrfach ausgezeichneten Next Generation Firewall, welche eine neue Generation von Real-Time Security Gateways definiert. Die redIT Managed Firewall ist mehr als nur eine einfache Managed Firewall. Die redIT Managed Firewall ist eine ASIC-beschleunigte Security Appliance, die die wichtigsten Security- und Netzwerk-Funktionalitäten vereint, einschliesslich Firewall und IPsec-VPN, Antivirus, Intrusion Prevention, Web Filtering, Antispam, Application Control, Data Loss Prevention, SSL Traffic Inspection und WAN-Optimierung. UTM steht für Unified Threat Management und beschreibt die zentrale Bündelung verschiedener Sicherheitsfunktionen. Die Signaturen der redIT Managed Firewall-Systeme werden weltweit automatisch und rund um die Uhr aktualisiert. Dies stellt den Echtzeitschutz vor contentbasierten Internetbedrohungen wie Viren, Würmern, Intrusions, unerwünschtem Netzwerkverkehr und weiteren Bedrohungen sicher.
Eine redIT Managed Firewall arbeitet als Filter zwischen dem Internet und dem Netzwerk des Kunden. Sie verfügt über ein Regelwerk, das die Filtereigenschaften gemäss den Security Policies, dem Netzwerk und den Systemvoraussetzungen des Kunden abbildet. Mögliche Angriffe, die sich auf sämtliche Netzwerk-Layer beziehen, werden innerhalb der redIT Managed Firewall erkannt und abgewehrt. Dies gilt für Angriffe auf die redIT Managed Firewall und die zu schützenden Netzwerke.

3 PRODUKTSPEZIFIKATIONEN

Die redIT Managed Firewall ist in folgenden Varianten erhältlich:

redIT Dedicated Managed Firewall Variante M
redIT Dedicated Managed Firewall Variante L
redIT Shared Managed Firewall Variante M
redIT Shared Managed Firewall Variante L
redIT Shared Managed Firewall Variante XL

Die redIT Managed Firewall ist als Dedicated Managed Firewall oder als Shared Managed Firewall erhältlich.
Bei der redIT Dedicated Managed Firewall wird dem Kunden eine dedizierte Firewall bereitgestellt. Diese kann entweder in den Rechenzentren der redIT oder beim Kunden vor Ort betrieben werden.
Bei der redIT Shared Managed Firewall wird die Firewall-Infrastruktur gemeinsam mit anderen Kunden genutzt. Diese Variante wird ausschliesslich in den Rechenzentren der redIT betrieben und ist nicht für den Einsatz beim Kunden vor Ort vorgesehen.

Die redIT Managed Firewall besteht aus technischen Einrichtungen, die eine abgesicherte Verbindung mit dem Internet ermöglichen. Diese Einrichtungen werden dem Kunden für die Dauer des Vertragsverhältnisses bereitgestellt und umfassen insbesondere:

- Firewall-Funktionalitäten inklusive UTM-Signaturen, Application Control, IPS und SSL Inspection
- VPN-Verbindungen für den sicheren Datenverkehr zwischen mehreren Standorten
- Sicherung, Monitoring, Firmware-Updates und zentrales Logging
- Hardware-Austausch bei Defekt gemäss Next Business Day Service
- Leistungsmerkmale gemäss gewählter Variante, insbesondere Firewall-, Threat-Protection- und VPN-Durchsatz

3.1 Grundkonfiguration (nach Aufwand)

Die Grundkonfiguration der redIT Managed Firewall erfolgt auf Basis der mit dem Kunden abgestimmten Security Policies. Diese Security Policies werden gemeinsam mit dem Kunden besprochen, definiert und redIT vor der Inbetriebnahme mitgeteilt. Der Kunde hat keine Möglichkeit, die Konfiguration der redIT Managed Firewall zu verändern. Auf Wunsch des Kunden stellt redIT einen Read-only-Benutzer zur Verfügung. Mit diesem Benutzer hat der Kunde Einsicht in die Konfigurationseinstellungen und Logs der Firewall.

3.2 Konfigurationsänderungen

Eine Änderung an der Konfiguration kann nur schriftlich per Support-Ticket beantragt werden. Für die Bestätigung wird redIT den Kunden telefonisch kontaktieren und den Änderungszeitpunkt mit ihm vereinbaren. Konfigurationsänderungen werden immer nach Aufwand verrechnet.

3.3 UTM-Signaturen

Der Kunde hat die Möglichkeit, Security Policies inklusive Application Control und IPS, Web Filtering und Antivirus zu aktivieren. redIT verwendet die vom Hersteller offiziell zur Verfügung gestellten UTM-Signaturen und richtet die redIT Firewall so ein, dass diese automatisch aktualisiert werden. UTM-Signaturen sind Updates datenbankbasierter Services wie Antivirus, IPS, Webfilter, etc. Für die Funktionsweise und Wirksamkeit der Signaturen des Herstellers kann redIT keine Haftung übernehmen.

3.4 Sicherung der aktuellen redIT Managed Firewall Konfiguration

redIT erstellt bei der Erstkonfiguration sowie bei jeder weiteren Konfigurationsänderung automatisch eine Sicherung der Firewall-Konfiguration. Dadurch ist gewährleistet, dass beispielsweise beim Austausch eines defekten Gerätes die zuletzt verfügbare Konfiguration verwendet und der Austausch möglichst rasch und unkompliziert durchgeführt werden kann.

3.5 Permanente Überwachung Ihrer redIT Firewall

Im Leistungsumfang ist die permanente technische Überwachung der Firewall enthalten. Dabei setzt redIT geeignete Monitoring-Methoden ein, um die Erreichbarkeit und den Betriebszustand der Firewall zu überwachen. Bei einer Störung des Gerätes während der Öffnungszeiten kontaktiert redIT den Kunden proaktiv, schlägt Lösungsmassnahmen vor oder leitet je nach Störung selbständig entsprechende Massnahmen ein, um den Fehler möglichst rasch zu beheben.

3.6 Austauschservice NBD (Next Business Day)

Bei einem Defekt oder Ausfall der Firewall stellt redIT dem Kunden während der Bürozeiten (07:00 bis 17:00 Uhr) bis zum nächsten Arbeitstag ein Gerät mit der zuletzt gesicherten Konfiguration zur Verfügung. Das Gerät wird auf dem Postweg zugestellt oder kann vom Kunden direkt bei redIT abgeholt werden. Auf Wunsch des Kunden kann redIT einen Techniker für den Austausch vor Ort einsetzen; dieser Einsatz wird nach Aufwand verrechnet.

3.7 VPN-Verbindungen für den sicheren Datenverkehr zwischen mehreren Standorten

Für den Aufbau von VPN-Tunneln stützt sich redIT auf die mit dem Kunden abgestimmten Angaben zur gewünschten Konfiguration.

3.8 Haftung

Datentransfers, welche nicht über die redIT Firewall laufen, entziehen sich deren Kontrolle. Ebenso kann die redIT Firewall keine verschlüsselten oder mehrfach komprimierten Inhalte auf schadhafte Bedrohungen untersuchen. Der Service gewährleistet nicht die Sicherheit des Kundennetzwerkes, sondern stellt einen Sicherheitsmechanismus zur Verfügung. Eine redIT Firewall kann keinen 100%igen Schutz vor unbekannten Angriffen gewährleisten.

4 INBETRIEBNAHME

Nach Bestelleingang wird die Machbarkeit überprüft und mit dem Kunden kommuniziert. Der Kunde wird über den weiteren Ablauf informiert und das Installationsdatum bekannt gegeben.

5 VORAUSSETZUNGEN

Damit die redIT Managed Firewall bereitgestellt und betrieben werden kann, sind je nach gewählter Variante folgende Voraussetzungen durch den Kunden sicherzustellen:

- Bereitstellung der für die Umsetzung erforderlichen Netzwerk- und Standortinformationen
- Mitwirkung bei der Definition der Security Policies und Firewall-Regeln
- Benennung einer technischen Ansprechperson für Abstimmung, Inbetriebnahme und Betrieb
- Bereitstellung der erforderlichen Internet- oder WAN-Anbindung
- Bereitstellung der notwendigen internen Netzwerkanschlüsse
- Geeigneter Standort beziehungsweise Rackplatz beim Kunden, sofern eine redIT Dedicated Managed Firewall vor Ort betrieben wird

6 NICHT ENTHALTENE LEISTUNGEN

- Konfiguration der redIT Managed Firewall (nach Aufwand)
- Inbetriebnahme vor Ort bei redIT Dedicated Managed Firewall, sofern vereinbart (nach Aufwand)
- Netzwerkkabel (RJ45 min. CAT 5e)
- Verlängerungskabel und Steckdosenleisten für die Stromversorgung
- Rack Mount Kit (kann separat bestellt werden)

7 ALLGEMEINE BESTIMMUNGEN

redIT kann nicht für Konfigurations- oder Manipulationsfehler des Kunden oder Dritter haftbar gemacht werden. Für Services, bei welchen Systemressourcen geteilt verwendet werden (Shared Services), nimmt der Kunde Rücksicht und schränkt die übermässige Nutzung dieser Ressourcen ein, um eine Beeinträchtigung der Leistung anderer Kunden auf demselben System zu verhindern («Fair Use»). Nutzt der Kunde Systemressourcen in einem Umfang, der die Leistung oder Verfügbarkeit für andere Kunden beeinträchtigen kann, ist redIT berechtigt, geeignete Massnahmen zu ergreifen. Dazu gehören insbesondere die vorübergehende Einschränkung oder Drosselung der betroffenen Services sowie die Unterbreitung eines Angebots für eine höhere Leistungsklasse. Nimmt der Kunde ein solches Angebot nicht an oder bleibt die übermässige Nutzung bestehen, behält sich redIT vor, weitere vertragliche Massnahmen bis hin zur fristlosen Vertragsauflösung zu ergreifen.
Die Services werden «Best effort» gewährleistet. Es gibt, wo nicht anders vermerkt, keine Garantie für bestimmte zugewiesene Systemressourcen oder Leistungsmerkmale. Bestehen Anzeichen eines rechts- oder vertragswidrigen Verhaltens, insbesondere einer missbräuchlichen Nutzung eines Service, kann redIT den Zugriff auf den Service ohne Vorankündigung umgehend entschädigungslos sperren oder einschränken, den Kunden zur rechts- und vertragskonformen Benutzung anhalten, den Vertrag frist- und entschädigungslos auflösen und gegebenenfalls Schadenersatz sowie die Freistellung von Ansprüchen Dritter verlangen.
Sollten einzelne Bestimmungen dieser Leistungsbeschreibung/Nutzungsbedingungen ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der übrigen Bestimmungen des jeweiligen Vertrags nicht tangiert.