IT

business@citynet.at
T +43 5223 5855 220

Viren- und Spamfilter B2B

Leistungsbeschreibung
Gültig ab 01.03.2017

I. Beschreibung

Das Produkt Viren- und Spamfilter richtet sich an Kunden, welche keine eigene Mail Security Infrastruktur betreiben bzw. Investitionen in diesem Bereich tätigen wollen. Die Stadtwerke Hall in Tirol GmbH (kurz STW) liefert diese dem Kunden mittels mandantenfähiger Antispam- und Antivirus-Lösung auf Basis ASP (Application Service Provider) Ansatz.
Viren- und Spamfilter schützt vor E-Mails unerwünschten Inhalts und eventuell schädlichen Programmen wie z.B.: Viren, Trojaner, etc. Dazu wird der MX-Eintrag (Mail Exchange) geändert. Es handelt sich somit um einen Mail Relay Service mit Mail-Scanning Funktion. Dabei ist es möglich, einzelne Domains des Kunden verschiedene Regeln zuzuweisen, nach denen der E-Mail Verkehr gescannt werden soll. Über eine Management Oberfläche kann der Kunde bzw. dessen IT-Beauftragter kundenspezifische Konfigurationen vornehmen.
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 im alleinigen Verantwortungsbereich des Kunden. Der Kunde verpflichtet sich, bestehende rechtliche Bestimmungen wie z.B.: Datenschutz, Arbeitsrecht, etc. einzuhalten.
Viren- und Spamfilter ist nur für Unternehmen im Sinne des Konsumentenschutzgesetzes (KSchG) erhältlich.
Die technische Ausführung für das Produkt Viren- und Spamfilter bzw. deren Zusatzprodukte bleibt der STW überlassen. Es gelten die aktuellen Lizenzbestimmungen des jeweiligen Herstellers.

II. Leistungsumfang

Die STW stellt dem Kunden im Rahmen der technischen und betrieblichen Möglichkeiten den Service Viren- und Spamfilter für die Dauer der Vertragslaufzeit zur Verfügung.
Das Produkt entspricht dem aktuellen Stand der Technik bei der Bekämpfung von Spam E-Mails sowie Computerviren. Es wird darauf hingewiesen, dass aufgrund der ständigen Neu- und Weiterentwicklung von Softwareviren, deren Mutation und der Entwicklung neuer, virenähnlicher Programme ein vollständiger und absoluter Schutz (100%) vor Virenbefall und/oder dem Erhalt von Spam nicht möglich ist. Für den Verlust oder die Vernichtung von E-Mails übernimmt STW – außer bei Vorsatz oder grober Fahrlässigkeit – keine Haftung.
STW behält sich das Recht vor – insbesondere bei Gefahr in Verzug (z.B.: neuer Virustyp, Spam-Welle, etc.) – die bestehenden Einstellungen global zu verändern um die Stabilität des Mail-Systems aufrecht zu erhalten.
Verschlüsselte E-Mails, interne und passwortgeschützte Dateien können nicht gescannt werden. Mehrmals täglich wird auf neue Viren- und Spam-Signaturen geprüft und gegebenenfalls aktualisiert.
Die Virenerkennung beschränkt sich auf die den eingesetzten Virenscannern bekannten Viren und Dateiformate. Gefundene Anhänge/E-Mails mit Viren werden unwiderruflich gelöscht und können nicht wiederhergestellt werden.
Die Deklaration einer eingehenden E-Mail als Spam erfolgt über Blacklisten, bayesische Filterung, Ratings, IP-Filterung, Prüfung der Sender-Domain, Sender E-Mail Adresse etc.
Zusätzlich werden Betreff, Body gefiltert und der Reverse DNS geprüft.
Die Backlisten werden zentral gepflegt. Die Aufnahme in eine Blacklist wird automatisch über international zur Verfügung stehende Server diverser Organisationen generiert. Kunden können diese Black- und Whitelisten durch Einträge eigenständig im System konfigurieren.
Die bayesische Filterung wird durch eine definierte Punkteanzahl beeinflusst. Dieser Wert kann pro Domain individuell eingestellt werden.

Insgesamt werden 16 Prüfungsmechanismen angewendet, die eine E-Mail als SPAM klassifizieren:
1. Erkennung von Denial of Service –Angriffen
2. Kontrolle der E-Mail Rate (Flutkontrolle)
3. IP-Sperrliste
4. Absender Authentifizierung
5. Empfängerverifizierung
6. Virencheck

7. Kundenspezifischer Richtlinien
8. Fingerprint Analyse
9. Intent Analyse
10. Bildanalyse
11. Bayes Filteranalyse
12. Spam Scoring
13. Sender Validierung(SPF & DMARC)
14. Heuristische Analyse
15. Mailanhang Filter und Analyse
16. Sandboxing (Optional)

Viren werden innerhalb einer E-Mail mehrfach geprüft. Wird ein Virus erkannt, wird dieser gelöscht oder optional in eine Quarantäne-Box umgeleitet. Isolierte E-Mail Nachrichten können an ein festgelegtes Postfach gesendet werden. Sämtliche E-Mail Nachrichten (mit Ausnahme von solchen, die Viren enthalten) werden vollständig gespeichert. Dazu muss die Quarantäne-Box aktiviert werden. Benutzerbasierend werden isolierte Nachrichten je Domain am Viren- und Spamfilter System gespeichert. Bei Bedarf können E-Mails wieder zugestellt werden.
Kundenspezifische Änderungen können über die Business Supporthotline kostenpflichtig beauftragt bzw. alternativ mittels Web-Oberfläche durch den Kunden durchgeführt werden.

Das Produkt umfasst, soweit nicht anders ausdrücklich festgelegt, folgende Leistungen
- Herstellung und Nutzung bzw. Aktivierung des zentralen Viren- und Spamfilters der STW je Domain
- Business Supporthotline/Business 24x7 Supporthotline (Aufpreis)
- Störungsbehebung und Wartung gemäß nachstehenden SLAs
- Optional wird ein Zugang zur Web-Oberfläche zur Verwaltung der Viren- und Spamfilter Konfiguration eingerichtet.
- Optional kann der Viren- und Spamfilter für weitere Kundendomains kostenpflichtig eingerichtet und aktiviert werden.

Herstellung
- Nach der Bestellung des Kunden bei STW bestätigt dieser dem Kunden die Bestellung und veranlasst die Herstellung.
- Der Dienst gilt als geliefert, sobald die Zugangsdaten an den Kunden übermittelt wurden und das erste eingehende E-Mail erfolgreich durch den Viren- und Spamfilter seitens STW verarbeitet wurde.

Herstellungsdauer
Die Herstellungsdauer wird bei Angebotslegung bekanntgegeben.

Inbetriebnahme
Die Erstinbetriebnahme erfolgt durch den Kunden. Bei Problemen und zusätzlichen
Fragen steht die telefonische Business Supporthotline während der allgemeinen Supportzeiten zur Verfügung. Falls es sich bei dem Problem nicht um eine Störung oder einen Fehler seitens STW handelt, kann die telefonische Support Hotline für maximal 15 Minuten in Anspruch genommen werden.
Sollte weitere Unterstützung von Nöten sein, kann der Kunde einen Technikereinsatz laut „Entgeltbestimmungen Sonstige Dienstleistungen & Material B2B“ beauftragen.

Supporthotline
STW unterstützt den Kunden im Rahmen der Supporthotline bei der Einrichtung des Dienstes sowie der Fehlerbehebung im laufenden Betrieb.

Zugangsdaten
Die Zugangsdaten werden dem Kunden auf Wunsch in Papierform übermittelt oder elektronisch zugesendet. Benötigt der Kunde die Zugangsdaten erneut, können diese dem Kunden in den Geschäftsräumlichkeiten von STW ausgehändigt oder per SMS auf die in den Vertragsstammdaten hinterlegte Mobiltelefonnummer geschickt werden. Der Kunde ist dafür verantwortlich, die hinterlegte Mobiltelefonnummer aktuell zu halten und darauf zu achten, dass diese nach wie vor im Besitz des Kunden ist und erreichbar ist. STW haftet nicht für den

Verlust der Zugangsnummer bei Versand an die hinterlegte Mobilfunknummer, wenn diese sich nicht mehr im Besitz des Kunden befindet.
Der Kunde verpflichtet sich, seine Zugangsdaten (Passwörter, PIN-Codes,…) Dritten nicht zugänglich zu machen und größte Sorgfalt bei der Geheimhaltung dieser Daten walten zu lassen, um einen missbräuchlichen Zugriff auf seine Daten zu vermeiden. Die Zugangsdaten sind unverzüglich zu ändern, wenn seitens Kunden vermutet wird, dass unberechtigte Dritte von diesen Kenntnis erlangt haben.
Die STW haftet nicht für Schäden, die durch die missbräuchliche Verwendung der Zugangsdaten durch den Kunden sowie durch die Verwendung oder Veränderung der übermittelten Daten durch den Kunden oder durch Dritte, die sich unbefugt Zugriff zu diesen Daten verschafft haben, entstanden sind.

Zusatzoptionen:

Sandbox
Das Sandbox Feature ist optional kostenpflichtig erhältlich.
Beim Sandboxing werden in E-Mails enthaltene Anhänge und Weblinks in einer gesicherten und abgeschirmten Umgebung ausgeführt und auf abnormales Verhalten geprüft.
Sollte ein bösartiges Verhalten festgestellt werden, werden die Emails ebenfalls geblockt oder in der Quarantäne abgelegt.
Sandboxing erhöht den E-Mailschutz vor allem in Bezug auf unerwünschte Viren und Skripte (Randsomware, Exploits, …), welche noch nicht als Signaturen in Virendatenbanken aufscheinen (sogenannte Zero-Day Attacken).
Diese Zusatzoption wird auf Basis der bekanntgegebenen Mailboxanzahl des Kunden je Domain angeboten/verrechnet. Sollte STW im Zuge der laufenden Routine-Kontrollen feststellen, dass sich die Mailboxanzahl um >10 Mailboxen erhöht hat, wird seitens STW umgehend der Kunde unterrichtet. Der Kunde muss binnen 14 Werktagen ab Bekanntgabe der erhöhten Mailboxanzahl diese reduzieren bzw. andernfalls diese verbindlich bei STW nachbestellen/beauftragen.

III. Konfiguration Breitbandmodem

Für die Viren- und Spamfilter Leistungen der STW gelten die folgenden Voraussetzungen und Pflichten des Kunden:

a.) Voraussetzungen
- Der Kunde hat die für die Einrichtung erforderlichen Daten zur Verfügung gestellt.
- Der Kunde verfügt über eine aktive Internetanbindung (hierdurch können weitere Kosten entstehen)
- Der Kunde hat Zugriff auf das Viren- und Spamfilter Portal.
- Der Kunde meldet der STW bzw. deren Mitarbeiter, jene Zugänge in das Viren- und Spamfilter Portal, welche in Zukunft nicht mehr benötigt bzw. genutzt werden pro aktiv, damit diese gesperrt bzw. gelöscht werden können.

b.) Pflichten des Kunden
- Der Kunde muss seine bestehenden DNS-Einträge nach Vorgabe der STW für die jeweilige Kundendomain ändern.
- STW setzt voraus, dass seitens des Kunden, die betriebenen Mail-Systeme mittels Firewall oder Virenschutzprogramme, etc. abgesichert sind und ständig aktualisiert werden. Nicht oder nicht ausreichend gesicherte „offene" Server sind eine Einladung zur missbräuchlichen Nutzung durch „Hacker". Sollte STW feststellen, dass der Dienst im erheblichen Maße missbräuchlich durch Dritte genutzt wird (z.B.: im Zuge eines Hackerangriffes), ist STW berechtigt, den Dienst ohne Vorankündigung vom Netz zu trennen. STW wird den Kunden unverzüglich von einer solchen Maßnahme auf Basis der bekannten Vertragsstammdaten unterrichten.
- Der Kunde muss die notwendige Änderung der Firewall/Router Einstellungen nach Vorgabe der STW vornehmen, um die Zustellung seitens STW zu ermöglichen (Portfreigabe, Firewall Regeln, …)
- Der Betrieb offener Mail-Relays oder ähnlichen Systemen, über die z.B.: SPAM-Mails verbreitet werden können, berechtigt die STW, den Server sofort vom Netz zu trennen. Der Kunde wird von STW unverzüglich informiert, sobald er Anhaltspunkte dafür hat, dass Dritte unbefugt seinen Server nutzen. Im Übrigen verbleibt es bei der Regelung der Haftung gemäß den Allgemeinen Geschäftsbedingungen der Stadtwerke Hall in Tirol GmbH, Fachbereich IT B2B.

- Der Kunde muss sein E-Mail System nach aktuellen RFC's betreiben und konfigurieren.

IV. Störungen und Wartung

Supporthotline	
Erreichbarkeit	Mo-Fr 07:30-19:00 Sa 10:00-17:00
Verfügbarkeit Service-Techniker	Mo-Fr 08:00-19:00 Sa 10:00-14:00
Kontaktdaten	Tel: 05223 5855-220 E-Mail: business@citynet.at
Business 24x7 Supporthotline	
Erreichbarkeit	Mo-So 00:00-24:00
Verfügbarkeit Service-Techniker	Mo-So 00:00-24:00
Kontaktdaten	Tel: 05223 5855-230 (PIN-Code erforderlich)

Wartungsfenster:
Wartungsarbeiten werden grundsätzlich angekündigt und sofern möglich, innerhalb des Standardwartungsfensters (Mi, 23:00 bis Do, 04:00) durchgeführt (ausgenommen bei Gefahr in Verzug).

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

Entstörzeit:
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 STW verursacht werden, sind in der Entstörungszeit nicht berücksichtigt und gelten als Fremdverzögerung.

Ermittlung der Entstörzeiten sowie der nicht verfügbaren Zeiten:
Bei der Ermittlung bleibt unberücksichtigt der Zeitraum der Nichtverfügbarkeit durch:
- Vom Kunden zu vertretende Störungen bzw. Verzögerungen.
- Höhere Gewalt.
- Angekündigte Wartungsarbeiten bzw. Wartungsarbeiten während der Standardwartungsfenster.
- Störungen, die aufgrund der mangelnden Information durch den Kunden bzw. Zutrittsbeschränkungen nicht beseitigt werden können.
- Störungen, die durch externe Dritte verursacht werden.
- Notwendige Verlegungen oder Änderung von Spezifikationen auf Grund behördlicher Auflagen oder Genehmigungen.
- Beschädigung durch Dritte, zB. Kabelbruch.

Service-Techniker-Einsätze:
Fehler- und Störungsbehebungen, welche durch den Kunden oder deren Equipment verursacht wurden, werden gemäß den „Entgeltbestimmungen Sonstige Dienstleistungen & Material B2B" verrechnet. Sollte sich herausstellen, dass die Störung im Einflussbereich der STW liegt, wird in diesem Fall der Service-Techniker-Einsatz durch STW übernommen. Die Einsätze werden zum nächstmöglichen freien Zeitpunkt terminisiert. Der Kunde hat an der Störungsbeseitigung mitzuwirken.

Zeiten außerhalb der Erreichbarkeit der Supporthotline unterbrechen die angeführten Reaktions- und Entstörungszeiten.
Kein Support an Sonn- und Feiertagen (ausgenommen Sonder-SLA)

VI. Service Level Agreement

	Standard SLA	Sonder SLA
Garantierte Verfügbarkeit	99,4%	99,8%
max. nicht verfügbare Zeit	53,00 h/Jahr	17,52 h/Jahr
STW Backbone	24x7	24x7
STW Viren- und Spamfilter System	24x7	24x7
Störungsannahme	24x7[1]	24x7
Reaktionszeiten Mo-Fr 07:30-19:00, Sa 10:00-17:00	max 2 h	max. 1 h
Reaktionszeiten Mo-Fr 19:00-07:30, Sa 17:00-10:00, Sonntag oder Feiertage	max. 8 h	max. 2 h
[1] Nicht Sonder-SLA-Kunden wird je Anruf eine Pauschalgebühr verrechnet.		

Sonder-SLA-Kunden erhalten einen eigenen PIN, dieser wird durch das automatische Telefonsystem abgefragt und validiert, nach erfolgreicher Überprüfung wird der Kunde automatisch zum 24x7 Support verbunden.

Garantierte Verfügbarkeit:
Die Messperiode beträgt ein Jahr, beginnend mit dem Datum der ersten Dienstbereitstellung und wiederholt sich jeweils zum Jahrestag der ersten Dienstbereitstellung. Die Verfügbarkeit wird wie folgt berechnet:

$$\text{Verfügbarkeit (\%)} = \frac{\text{Messperiode} - \text{Ausfallzeit} \times 100}{\text{Messperiode}}$$

Monitoring am Backbone:
STW überwacht sein Netz 24 Stunden, 7 Tage in der Woche, 365 Tage im Jahr.

Monitoring des STW Viren- und Spamfilter Systems:
STW überwacht seine Server und seine Services 24 Stunden, 7 Tage in der Woche, 365 Tage im Jahr.