



Geschäftsbedingungen für von Kaspersky Hosted Security

Diese Geschäftsbedingungen (Terms & Conditions, T&Cs) regeln die Bereitstellung von Kaspersky Hosted Security (KHS) durch Kaspersky Lab für den Kunden.

1 Definitionen und Interpretationen

Im Rahmen dieser T&Cs haben nachstehende Begriffe die nachstehende Bedeutung:

Kunde: bezeichnet die Gesellschaft oder eine andere juristische Person, der die KHS zur Verfügung gestellt wird.

Kaspersky Lab: bezeichnet im Rahmen dieses Plans die Kaspersky-Gruppe.

Kaspersky Hosted E-Mail Security: bezeichnet die Kaspersky Hosted Security für E-Mail im Sinne der jeweils aktuellen Version der KHS-Beschreibung.

Kaspersky Hosted Web Security: bezeichnet die Kaspersky Hosted Security für Web im Sinne der jeweils aktuellen Version der KHS-Beschreibung.

Kaspersky Hosted Security (KHS): bezeichnet die Kaspersky Hosted E-Mail Security und/oder die Kaspersky Hosted Web Security oder eine Kombination von beiden im Sinne der jeweils aktuellen Version der KHS-Beschreibung.

KHS-Beschreibung: bezeichnet Bestimmungen, in denen technische Beschreibungen der KHS enthalten sind und deren aktuelle Version diesen T&Cs beigefügt ist.

Malware: bezeichnet ein mit der ausdrücklichen Absicht geschriebenes Computerprogramm, Daten und/oder Codes auf einem dafür vorgesehenen Computer zu schädigen oder zu gefährden und/oder dessen Nutzbarkeit zu verringern und/oder unbefugten Zugang zu diesem Computer zu ermöglichen.

Monatsgebühr: bezeichnet 1/12 des vom Kunden für ein Jahr KHS-Nutzung gezahlten Preises oder den Preis, der vom Kunden für einen Monat KHS-Nutzung gezahlt wird.

Open Relay: bezeichnet einen SMTP-Server, der so konfiguriert ist, dass er von jedermann im Internet zum Versenden von E-Mails benutzt werden kann und damit nicht nur für Mails, die für bekannte Nutzer oder Domains bestimmt sind oder von solchen stammen.

Zulässige Anzahl von Nutzern: bezeichnet die im Lizenzzertifikat angegebene Anzahl von Nutzern.

Portal: bezeichnet eine webbasierte Konfiguration, die vom Kunden für Zwecke der Handhabung der KHS und der Berichterstattung genutzt wird.

Lizenzzertifikat: bezeichnet das Zertifikat, das die Lizenzgewährung für die KHS, den Abonnementzeitraum und die zulässige Anzahl von Nutzern bestätigt und dem diese T&Cs beigefügt sind.

Abonnementzeitraum: bezeichnet den vom Kunden bezahlten Zeitraum, während dessen die KHS vom Kunden nach Maßgabe des Lizenzzertifikats genutzt wird.

Starttermin: bezeichnet das im Lizenzzertifikat angegebene KHS-Aktivierungsdatum.

Spam und Spam-Mail: bezeichnet unerwünschte Massen-E-Mails, die wahllos verschickt werden.

Nutzer: bezeichnet (i) eine körperliche oder virtuelle (in Fällen gemeinsam genutzter Mailboxen) Organisation, die über 1 firmeneigene Mailbox mit einem oder mehreren zugehörigen Pseudonymen verfügt, und für die die Kaspersky Hosted E-Mail Security E-Mails scannt und/oder (ii) eine körperliche oder virtuelle (in Fällen gemeinsam genutzter Computer) Organisation, die auf Internet-Ressourcen zugreifen kann und für die die Kaspersky Hosted Web Security Web-Inhalte verarbeitet.

Web-Inhalte: bezeichnet Daten jeder Art sowie Anfragen nach Daten, die von der Kaspersky Hosted Web Security verarbeitet werden, einschließlich unter anderem Daten, auf die unter Nutzung der Internet-Protokolle HTTP und FTP zugegriffen wird.

2 Anwendungsbereich dieser T&Cs

2.1 Kaspersky Lab gewährt dem Kunden das Recht, die KHS im Einklang mit den hierin vorgegebenen Geschäftsbedingungen zu nutzen.

2.2 Diese T&Cs gelten für die Bereitstellung der KHS durch Kaspersky Lab. Die ihnen beigefügten Pläne und Anlagen gelten insofern, als der darin beschriebene KHS-Teil im Lizenzzertifikat angegeben wird. Sämtliche abweichenden T&Cs, die in der Kundenbestellung oder anderen Unterlagen des Kunden benannt sind, werden abgelehnt und sind unwirksam, sofern sie nicht ausdrücklich von beiden Parteien in Schriftform vereinbart werden.

3 Laufzeit

- 3.1 Diese T&Cs werden am Starttermin wirksam und bleiben – vorbehaltlich der Regelungen in Klausel 4 – bis zum Ablauf des Abonnementzeitraums in Kraft.

4 Kündigung

- 4.1 Kaspersky Lab ist berechtigt, die T&Cs per Mitteilung an den Kunden mit sofortiger Wirkung zu kündigen, falls dieser seinen Zahlungspflichten für die KHS nach Maßgabe der einschlägigen Bestimmungen nicht nachkommt.
- 4.1.1 Kaspersky Lab überwacht die Nutzung der KHS durch den Kunden. Falls die tatsächliche Anzahl der Nutzer deren zulässige Anzahl übersteigt, ist Kaspersky Lab berechtigt, nach seinem alleinigen Ermessen entweder die T&Cs per Mitteilung an den Kunden mit sofortiger Wirkung zu kündigen oder eine anteilige und sofort zahlbare Rechnung für die zusätzliche Anzahl von Nutzern zu stellen.
- 4.2 Ungeachtet weiterer Rechte, die einer Partei gegebenenfalls nach diesen T&Cs zustehen, kann jede Partei die T&Cs per schriftlicher Nachricht an die andere Partei mit sofortiger Wirkung kündigen, wenn die andere Partei einen wesentlichen Verstoß gegen diese T&Cs begeht und es versäumt, den Verstoß innerhalb von dreißig (30) Tagen nach entsprechender schriftlich erfolgter Aufforderung zu beheben (sofern der betreffende Verstoß behoben werden kann).
- 4.3 Nach erfolgter Kündigung des Kunden nach Klausel 4.2 wegen Verstoßes gegen diese T&Cs durch Kaspersky Lab ist der Anteil an vom Kunden gezahlten Gebühren, der sich auf den nicht in Anspruch genommenen Abonnementzeitraum nach dem Kündigungsdatum bezieht, dem Kunden zurückzuerstatten.
- 4.4 Nach erfolgter Kündigung der T&Cs als Folge eines Verstoßes des Kunden gegen diese T&Cs erlischt das Recht des Kunden zur Nutzung der KHS mit sofortiger Wirkung und alle Rechnungen werden fällig und zahlbar.
- 4.5 Folgende Klauseln gelten trotz Kündigung dieser T&Cs fort: Klauseln 1, 7, 8, 9, 10, 13, 14 und 20.

5 KHS-Bereitstellung

- 5.1 Kaspersky Lab unternimmt alle zumutbaren Anstrengungen, um die KHS der zulässigen Anzahl von Nutzern während des Abonnementzeitraums zur Verfügung zu stellen.
- 5.2 Kaspersky Lab behält sich das Recht vor, vor der Anmeldung für die Kaspersky Hosted E-Mail Security und jederzeit während der Bereitstellung der Kaspersky Hosted E-Mail Security zu überprüfen, ob das E-Mail-System des Kunden als Open Relay funktioniert. Wenn die Kundensysteme nachweislich als Open Relay funktionieren, informiert Kaspersky Lab den Kunden hierüber und behält sich das Recht vor, die Funktion der Kaspersky Hosted E-Mail Security unverzüglich ganz oder teilweise so lange auszusetzen, bis das Problem gelöst wurde.
- 5.3 Wenn die Bereitstellung der KHS für den Kunden die Sicherheit der KHS aufgrund von unter anderem Hacking, Denial-of-Service-Attacken, Flooding oder anderen böswilligen Aktionen gefährden würde, die vom Netzwerk des Kunden ausgehen oder dieses zum Ziel haben, behält sich Kaspersky Lab das Recht vor, die Funktion der KHS unverzüglich ganz oder teilweise so lange auszusetzen, bis das Problem gelöst wurde. In einem solchen Fall informiert Kaspersky Lab den Kunden umgehend entsprechend und arbeitet mit diesem dabei zusammen, die betreffenden Probleme zu lösen – wobei der Kunde zur Kooperation verpflichtet ist –, damit die KHS ihre Funktion zur frühestmöglichen Gelegenheit wieder aufnehmen kann.
- 5.4 Wenn der Kunde die Kaspersky Hosted E-Mail Security zur Verbreitung von Spam benutzt, behält sich Kaspersky Lab das Recht vor, die Funktion der Kaspersky Hosted E-Mail Security ganz oder teilweise unverzüglich und so lange auszusetzen, bis das Problem gelöst wurde.
- 5.5 Sollte die Funktion der KHS aus irgendeinem Grund ausgesetzt oder beendet werden, macht Kaspersky Lab alle Konfigurationsänderungen rückgängig, die bei der Anmeldung für die KHS vorgenommen wurden, und es liegt in der Verantwortung des Kunden, alle weiteren erforderlichen Konfigurationsänderungen vorzunehmen, um seinen E-Mail- und/oder Web-Verkehr korrekt umzustellen.
- 5.6 Vorbehaltlich geltenden Rechts kann Kaspersky Lab die KHS unter Nutzung jeglicher Hardware-Installationen an jedem Ort der Welt zur Verfügung stellen und die Bereitstellung der KHS zu jeder Zeit von einer Installation auf eine andere übertragen.
- 5.7 Um seinen Verpflichtungen nachzukommen, kann Kaspersky Lab die KHS und alle zugehörigen Unterlagen gelegentlich aus beliebigen Gründen abändern, wobei es sich unter anderem um Änderungen in Übereinstimmung mit Branchenstandards sowie rechtlichen, geschäftlichen oder technischen Gesichtspunkten handeln kann. Änderungen werden wirksam, sobald Kaspersky Lab eine neue KHS-Beschreibung auf dem Portal veröffentlicht.

6 Verpflichtungen des Kunden

- 6.1 Der Kunde erkennt an, dass die KHS mit den Kaspersky-Lab-Standard-Einstellungen bereitgestellt wird und es die alleinige Verantwortung des Kunden ist, die KHS mithilfe des Portals nach seinen eigenen Anforderungen zu konfigurieren. Kaspersky-Lab-Vertreter können dabei behilflich sein, die KHS so zu konfigurieren, wie es für den Betrieb optimal ist. Kaspersky Lab behält sich das Recht vor, Kundeneinstellungen in Notfallsituationen zu ändern, um die KHS-Qualität für einen oder mehrere Kunden zu bewahren.
- 6.2 Der Kunde stellt Kaspersky Lab alle technischen Daten und alle weiteren Informationen zur Verfügung, die das Unternehmen von Zeit zu Zeit anfordern kann, um es ihm zu ermöglichen, dem Kunden die KHS zur Verfügung zu stellen. Alle vom Kunden vorgelegten Informationen müssen vollständig und richtig sein sowie in gutem Glauben übermittelt werden. Solche Informationen werden im Rahmen der Geschäftsbedingungen dieser T&Cs als vertrauliche Informationen behandelt.



- 6.3 Der Kunde hat dafür zu sorgen, dass sein E-Mail-System
- 6.3.1 nicht als Open Relay funktioniert und
 - 6.3.2 keine Spam-Mails versendet.
- 6.4 Der Kunde bestätigt, dass an den und vom Kunden geschickte Informationen die KHS passieren, weshalb sich der Kunde dazu verpflichtet:
- 6.4.1 alle einschlägigen Gesetze einzuhalten, die für die Verwendung des Internets und von E-Mails gelten,
 - 6.4.2 die KHS nur für legitime Geschäftszwecke zu gebrauchen, wozu das Verschieken und Empfangen von geschäftlichen wie persönlichen E-Mails bzw. die Verwendung von Web-Inhalten durch seine Mitarbeiter gehören,
 - 6.4.3 die KHS nicht zur Weiterleitung von Spam zu benutzen,
 - 6.4.4 die jeweils im Internet veröffentlichten und von der Mehrheit der Internet-Nutzer übernommenen Protokolle und Standards einzuhalten und
 - 6.4.5 Kaspersky Lab von jeder Haftung gegenüber Dritten freizustellen, die eine Folge von Informationen des Kunden ist, die die KHS passieren.
- 6.5 Der Kunde verpflichtet sich, die KHS nicht für rechtswidrige Zwecke zu verwenden und Kaspersky Lab für sämtliche Verluste, Kosten und Aufwendungen zu entschädigen, die bei Kaspersky Lab aufgrund solcher rechtswidrigen Aktivitäten entstehen können, zu denen unter anderem folgende gehören:
- 6.5.1 zivil- oder strafrechtliche Verletzungen von geistigen Eigentumsrechten, einschließlich unter anderem der Verletzung von Urheberrechten, Marken und Patenten,
 - 6.5.2 Übertragung oder Veröffentlichung obszöner, anstößigen oder pornografischen Materials,
 - 6.5.3 Begehen von Straftaten im Sinne des jeweils geltenden Rechts,
 - 6.5.4 Übertragung oder Veröffentlichung von Materialien, die verleumderischer, anstößiger, missbräuchlicher oder bedrohlicher Natur sind,
 - 6.5.5 Übertragung oder Veröffentlichung von Materialien, die gegen das Datenschutzgesetz von 1998 oder vergleichbare Gesetze verstoßen oder
 - 6.5.6 Einsatz der KHS in einer Art und Weise, die gegen die Rechte von Einzelpersonen, Organisationen oder Gesellschaften verstößt bzw. diese verletzt.
- 6.6 Der Kunde darf nur solche E-Mail-Domains hinzufügen, die ihm gehören oder bei denen er über einen rechtlich anerkannten Nachweis verfügt, dass er berechtigt ist, die betreffende Domain dem Kaspersky Hosted Security Sicherheitssystem hinzuzufügen. Kaspersky Lab behält sich das Recht vor, das Eigentum an der jeweiligen Domain oder eine solche Berechtigung zu überprüfen, bevor die KHS installiert wird.
- 6.7 Der Klarstellung halber wird angemerkt, dass ein Verstoß gegen Klauseln 6.3 bis einschließlich 6.6 einen wesentlichen Verstoß gegen die T&Cs darstellt. Für den Fall, dass der Kunde seinen in den Klauseln 6.3-6.6 dargelegten Verpflichtungen nicht nachkommt, kann Kaspersky Lab ungeachtet seiner weiteren Rechte aus den T&Cs oder der Vereinbarung die Verwendung der KHS durch den Kunden jederzeit so lange aussetzen, bis dieser das Problem gelöst hat.
- 6.8 Die KHS wird dem Kunden für seine eigene Verwendung zur Verfügung gestellt, weshalb er sie auch nicht an Dritte weiterverkaufen darf.

7 Gewährleistung

Soweit dies gesetzlich zulässig ist, schuldet Kaspersky Lab nur den Einsatz aller angemessenen fachlichen Kenntnisse und Sorgfalt, die für die Bereitstellung der KHS erforderlich sind. Die vorangehenden Konditionen gelten anstelle aller anderen ausdrücklichen und stillschweigenden Garantien, Bedingungen bzw. anderen Bestimmungen und schließen diese aus, einschließlich unter anderem Garantien hinsichtlich einer zufrieden stellenden Qualität und Eignung für einen bestimmten Zweck.

8 Haftungsbeschränkung

JEDLICHE BEGRÜNDETEN, RECHTMÄßIGEN ANSPRÜCHE DES KUNDEN IN BEZUG AUF DIE VERFÜGBARKEIT UND/ODER DIE QUALITÄT DER KHS SOWIE ALLE WEITEREN ANSPRÜCHE IM ZUSAMMENHANG MIT DER KHS UNTERLIEGEN DEN NACHFOLGENDEN BESCHRÄNKUNGEN:

- 8.1 DIE HAFTUNG VON KASPERSKY LAB FÜR TATSÄCHLICHE VERLUSTE UND SCHÄDEN BEIM KUNDEN (EINSCHLIEßLICH DES VERLUSTS VON DATEN) ODER ANSPRÜCHE DRITTER, DIE EINE FOLGE DER KUNDENANSPRÜCHE SEIN KÖNNEN, AUF DER GRUNDLAGE DER NICHT-EINHALTUNG DER KHS-BESCHREIBUNG DURCH DIE KHS (WIE ETWA UNVERFÜGBARKEIT ODER MÄNGEL BEI DER QUALITÄT DER KHS), DIE EINE FOLGE DER FAHRLÄSSIGKEIT VON KASPERSKY LAB, SEINEN MITARBEITERN ODER VERTRETEREN IST, WIRD DER HÖHE NACH AUF DEN ZULETZT AKTUELLEN VOM KUNDEN FÜR DIE KHS WÄHREND EINES ZEITRAUMS VON EINEM (1) JAHR ZU ZAHLENDEN BETRAG BEGRENZT. DIESE BEGRENZUNG GILT FÜR JEDEN EINZELFALL ODER JEDE REIHE VON ZUSAMMENHÄNGENDEN EINZELFÄLLEN.
- 8.2 JEDLICHE ANSPRÜCHE DES KUNDEN AUF ENTSCHÄDIGUNG WEGEN ENTGANGENEN



GEWINNS/UMSATZEINBUßEN/RUFSCHÄDIGUNG/VERLUST VON VERTRÄGEN UND/ODER KUNDEN ODER
ENTSCHÄDIGUNGEN WEGEN VERLUST VON DATEN SIND AUSGESCHLOSSEN.

- 8.3 KASPERSKY LAB HAFTET NICHT FÜR SCHÄDEN, DIE VOM KUNDEN DURCH NICHTBEFOLGUNG DER T&CS
ODER DURCH EINE VERWENDUNG DER KHS VERURSACHT WERDEN, DIE NICHT DEN T&CS ENTSPRICHT.
- 8.4 DIE VORSTEHENDEN HAFTUNGSBESCHRÄNKUNGEN UND -AUSSCHLÜSSE GELTEN NICHT:
- 8.4.1 BEI TODESFÄLLEN ODER PERSONENSCHÄDEN BZW. SCHÄDEN AN DER GESUNDHEIT EINER
PERSON,
- 8.4.2 IM FALL VON HAFTUNGSVERBINDLICHKEITEN, DIE AUFGRUND GESETZLICHER VORSCHRIFTEN
WEDER BEGRENZT NOCH AUSGESCHLOSSEN WERDEN KÖNNEN, ODER
- 8.4.3 IN BEZUG AUF DIE HAFTUNGSFREISTELLUNG BEI GEISTIGEN EIGENTUMSRECHTEN, DIE IN
KLAUSEL 14 DARGELEGT IST.
- 8.5 **DIE BESONDERE AUFMERKSAMKEIT DES KUNDEN WIRD AUF DIE TATSACHE GELENKT**, DASS DIE KHS
DURCH DEN EINSATZ ELEKTRONISCHER VERFAHREN UND ALGORITHMEN GEMÄß DEN ANGABEN IN DEN
T&CS UND DER KHS-BESCHREIBUNG ZUR VERFÜGUNG GESTELLT WIRD:
- 8.5.1 DA SIE MIT DEM STAND DER TECHNOLOGISCHEN ENTWICKLUNG VERKNÜPFT SIND, WERDEN
DIESE VERFAHREN VON KASPERSKY LAB IN EINEM ANGEMESSENEN UMFANG GEPFLEGT, UM SO
SICHERZUSTELLEN, DASS NORMALERWEISE NUR E-MAILS, DIE VIREN ENTHALTEN ODER ALS
SPAM ZU BETRACHTEN SIND, ALS „POSITIV“ ERKANNT WERDEN, UND DAHER NACH MAßGABE
DER IN DIESEN T&CS UND DER KHS-BESCHREIBUNG DARGELEGTE REGELUNGEN BLOCKIERT
UND UNTER QUARANTÄNE GESTELLT WERDEN KÖNNEN. ES IST ALLERDINGS NICHT MÖGLICH, ZU
GEWÄHRLEISTEN, DASS IN BESTIMMTEN FÄLLEN UND UNTER BESTIMMTEN UMSTÄNDEN (ZU
DENEN DIE KONFIGURATION DES KUNDEN GEHÖREN KANN) AUCH ERWÜNSCHTE ODER NICHT
VIRUS-INFIZIERTE E-MAILS BLOCKIERT UND UNTER QUARANTÄNE GESTELLT WERDEN („FALSCH
POSITIV“). DER KUNDE AKZEPTIERT DAHER DIE VERPFLICHTUNG, DIE QUARANTÄNE-BOX DER
KHS IN REGELMÄßIGEN ABSTÄNDEN ZU ÜBERPRÜFEN. KASPERSKY LAB AKZEPTIERT KEINERLEI
HAFTUNG FÜR VERLUSTE UND/ODER SCHÄDEN, DIE EINE FOLGE DER NICHTAUSLIEFERUNG
FALSCH POSITIVER E-MAILS SIND, UND ÜBERNIMMT AUßERDEM KEINERLEI HAFTUNG FÜR DEN
FALL, DASS „FALSCH POSITIVE“ E-MAILS 30 TAGE NACH DEM DATUM IHRER VERSENDUNG
GELÖSCHT WORDEN SIND.

9 Vertraulichkeit

- 9.1 Beide Parteien sagen zu und verpflichten sich, während der Dauer des Abonnementzeitraums und dreier (3) sich
anschließender Jahre Informationen vertraulichen Charakters (einschließlich Geschäftsgeheimnissen und Informationen von
wirtschaftlichem Wert), die an eine Partei durch die andere Partei oder deren Unterauftragnehmer weitergeleitet oder ihr
bekannt gemacht worden sind („vertrauliche Informationen“), vorbehaltlich der Regelungen in Klauseln 9.2 und 9.3 vertraulich
zu behandeln und weder für eigene Zwecke zu nutzen noch an Dritte weiterzugeben, ohne vorher die schriftliche Zustimmung
der jeweils anderen Partei einzuholen. Verpflichtungen bezüglich vertraulicher Informationen bestehen dann nicht, wenn die
Informationen allgemein bekannt sind oder eine Partei nachweisen kann, dass ihr die Informationen zum Zeitpunkt der
Offenlegung bereits bekannt waren oder die Informationen im Anschluss allgemein bekannt werden, ohne dass hierfür ein
Verstoß gegen diese T&Cs ursächlich ist, oder die Informationen im Anschluss in rechtmäßiger Weise von einem Dritten
erhalten werden, der keiner Vertraulichkeitsverpflichtung unterliegt. Weder die Parteien noch ihre Unterauftragnehmer werden
als gegen diese Klausel verstoßend betrachtet, wenn sie gesetzlich verpflichtet sind, vertrauliche Informationen offen zu legen,
was allerdings voraussetzt, dass die betreffende Partei zunächst die andere Partei mindestens 14 Tage im Voraus von der
gesetzlichen Auflage der Offenlegung informiert hat.
- 9.2 Soweit dies erforderlich ist, um die Regelungen dieser T&Cs umzusetzen und/oder einzuhalten, ist jede Partei berechtigt, die
vertraulichen Informationen an diejenigen Mitarbeiter und Unterauftragnehmer weiterzuleiten, die die vertraulichen
Informationen für diese Zwecke kennen müssen; hierbei ist allerdings zu berücksichtigen, dass jede Partei vor jeglicher
Weitergabe diese Mitarbeiter und Unterauftragnehmer mit ihren Vertraulichkeitspflichten aus diesen T&Cs vertraut macht und
dafür sorgt, dass diese von den Mitarbeitern und Unterauftragnehmern auch eingehalten werden.
- 9.3 Kaspersky Lab erkennt an, dass der Inhalt aller an den Kunden versandten oder von ihm erhaltenen E-Mails und alle Web-
Inhalte des Kunden sowie Anfragen nach Web-Inhalten vertraulicher Natur sind. Sofern dies nicht zur Einhaltung seiner
vertraglichen Verpflichtungen geschieht, darf Kaspersky Lab den Inhalt der E-Mails, Web-Inhalte oder Anfragen nach Web-
Inhalten weder überprüfen noch verwenden. Außer für Zwecke der Bereitstellung der KHS darf Kaspersky Lab im Rahmen
des normalen Betriebs der KHS auf E-Mails und/oder deren Anlagen, Web-Inhalte und Anfragen nach Web-Inhalten weder
zugreifen noch dieselben lesen und/oder kopieren. Alle Daten werden strikt vertraulich behandelt.
- 9.4 Kaspersky Lab behält sich jedoch das Recht vor, den virusrelevanten Inhalt solcher E-Mails und/oder ihrer Anlagen bzw.
virusrelevante Web-Inhalte sowie die Daten der vom Kunden genutzten Internetverbindung ausschließlich für folgende
Zwecke zu benutzen:
- 9.4.1 Pflege und Verbesserung von Leistungsfähigkeit und Integrität der KHS,
- 9.4.2 Einhaltung aller regulatorischen, gesetzlichen oder vertraglichen Auflagen und
- 9.4.3 Weiterleitung virusrelevanter Inhalte an Lizenzgeber der KHS für Zwecke der Weiterentwicklung und Aufwertung



der KHS.

- 9.5 Kaspersky Lab behält sich außerdem das Recht vor, Spam-relevante Inhalte solcher E-Mails und/oder ihrer Anlagen, die an die Domain des Kunden gesendet werden, für die keine E-Mail-Adresse auf dem Kunden-Server konfiguriert ist, ausschließlich für folgende Zwecke zu benutzen:
- 9.5.1 Pflege und Verbesserung von Leistungsfähigkeit und Integrität der KHS,
 - 9.5.2 Einhaltung aller regulatorischen, gesetzlichen oder vertraglichen Auflagen und
 - 9.5.3 Weiterleitung Spam-relevanter Inhalte an Lizenzgeber der KHS für Zwecke der Weiterentwicklung und Aufwertung der KHS.

10 Datenschutz und Regelung polizeilicher Ermittlungsbefugnisse

- 10.1 Der Kunde ergreift alle notwendigen Maßnahmen, um zu gewährleisten, dass er und alle seine Mitarbeiter ihre Verantwortlichkeiten nach allen geltenden Datenschutzgesetzen und/oder -vorschriften kennen. Der Kunde stellt Kaspersky Lab in vollem Umfang von der Haftung für jegliche Ansprüche Dritter frei, die sich auf etwaige Verstöße gegen das Datenschutzgesetz von 1998 oder vergleichbare geltende Gesetze durch den Kunden beziehen, da Kaspersky Lab keinerlei Kontrolle oder Einfluss über bzw. auf die von der KHS verarbeiteten Inhalte der E-Mails bzw. der Web-Inhalte hat.
- 10.2 Der Kunde holt die entsprechenden Zustimmungen ein und gibt diejenigen Hinweise, die in Zusammenhang mit der Verarbeitung, Speicherung und Nutzung personenbezogener Daten, die für die Bereitstellung der KHS nach Maßgabe dieser T&Cs notwendig sind, benötigt werden.
- 10.3 Soweit bei der Bereitstellung der KHS personenbezogene Daten verarbeitet werden, geschieht dies ausschließlich unter Einhaltung der Bestimmungen dieser T&Cs und nur für Zwecke der Bereitstellung der KHS und nur in dem Umfang, in dem dies für diese Zwecke erforderlich ist.
- 10.4 Der Kunde sichert zu, dass er alle geltenden Regelungen und Vorschriften in Zusammenhang mit der Umsetzung einer E-Mail-/Internet-Richtlinie in seiner Organisation sowie, falls dies erforderlich ist, die Zustimmung seiner Mitarbeiter bzw. des Betriebsrats insbesondere für das Abfangen, Lesen, Kopieren oder Filtern von E-Mails und/oder deren Anlagen oder von Web-Inhalten durch die KHS erhalten hat.
- 10.5 Entsprechend den Auflagen des jeweils geltenden Rechts informiert der Kunde (etwa mithilfe einer Bannermeldung bei E-Mails) diejenigen Personen, die von der KHS erfasste Kommunikationssysteme benutzen, dass durch diese Systeme übertragene Kommunikationen abgefangen und überwacht werden können, und erläutert die Zielsetzungen dieses Abfangens und Überwachens. Keine der Parteien darf mithilfe der KHS erhaltene Daten für unrechtmäßige Zwecke verwenden oder die andere Partei zu einem solchen Vorgehen auffordern.

11 Höhere Gewalt

Die Verpflichtungen beider Parteien aus diesen T&Cs werden für den Zeitraum und in dem Umfang ausgesetzt, in dem die betreffende Partei unvermeidlicher Weise daran gehindert oder davon abgehalten wird, diesen Verpflichtungen nachzukommen, und zwar aufgrund von Ursachen, die sich nach vernünftiger Anschauung ihrer Kontrolle entziehen und zu denen unter anderem folgende Ereignisse gehören: Streiks, Aussperrungen, Krieg, Terrorismus, Aufruhr, zivile Unruhen, mutwillige Beschädigung, Befolgung von Gesetzen oder behördlichen Verfügungen, Vorschriften oder Anweisungen, Unfall, Brand, Überflutung, Sturm, Stromausfälle oder Ausfälle bei wesentlichen Service-Systemen oder -Verbindungen Dritter.

12 Unterbrechung

Etwaige Unterbrechungen der KHS-Funktion, die nach diesen T&Cs zulässig sind, verlängern nicht den Abonnementzeitraum, sofern sie nicht auf einem Verschulden von Kaspersky Lab beruhen.

13 Geistige Eigentumsrechte

Der Kunde erkennt an, dass die KHS und deren Urheberschaft sowie die Systeme, Konzepte, Betriebsverfahren, Dokumentationen und andere in der KHS enthaltene Informationen geschütztes geistiges Eigentum und/oder wertvolle Geschäftsgeheimnisse von Kaspersky Lab oder seinen Partnern darstellen, und dass Kaspersky Lab und seine Partner je nach Sachlage zivil- oder strafrechtlichen Schutz genießen und durch die Gesetze zu Urheberrechten, Geschäftsgeheimnissen, Marken und Patenten der Russischen Föderation, der europäischen Gemeinschaft und den USA sowie anderer Länder und durch internationale Abkommen geschützt sind. Diese T&Cs gewähren dem Kunden keinerlei Rechte am besagten geistigen Eigentum einschließlich etwaiger Handels- oder Dienstleistungsmarken von Kaspersky Lab und/oder seinen Partnern („Marken“). Die zulässige Nutzung von Marken verleiht dem Kunden keine Eigentumsrechte an den betreffenden Marken. Der Rechteinhaber und/oder seine Partner sind und bleiben Eigentümer aller Rechte, Titel und Ansprüche an bzw. auf die KHS, einschließlich unter anderem aller Fehlerkorrekturen, Erweiterungen, Updates oder anderer Änderungen der KHS, seien diese durch Kaspersky Lab oder einen Dritten ausgeführt, und aller daran bestehenden Urheberrechte, Patente, Rechte an Geschäftsgeheimnissen, Marken und anderen geistigen Eigentumsrechte. Durch seinen Gebrauch der KHS erhält der Kunde keine Eigentümerstellung hinsichtlich des geistigen Eigentums an der KHS; außerdem erwirbt er keinerlei Rechte an der KHS, soweit dies nicht ausdrücklich in diesen T&Cs vorgesehen ist. Soweit hierin keine diesbezüglichen Feststellungen getroffen sind, gewähren diese T&Cs dem Kunden keinerlei geistigen Eigentumsrechte an der KHS, der darüber hinaus anerkennt, dass ihm die nachstehend definierte KHS-Produktlizenz, die nach diesen T&Cs erteilt wird, nur ein Recht zur Nutzung der KHS im Rahmen dieser T&Cs für einen begrenzten Zeitraum verleiht. Kaspersky Lab behält sich alle Rechte vor, die dem Kunden nicht ausdrücklich im Rahmen dieser T&Cs eingeräumt werden.



14 Fremde geistige Eigentumsrechte

- 14.1 Für den Fall, dass die KHS gegen fremde geistige Eigentumsrechte verstößt, wird sich Kaspersky Lab gegen entsprechende Ansprüche Dritter verteidigen und/oder diese beilegen, sofern:
- 14.1.1 der Kunde Kaspersky Lab umgehend nach seinem Kenntniserhalt von solchen Ansprüchen in Schriftform über diese informiert,
 - 14.1.2 der Kunde Kaspersky Lab die alleinige Kontrolle über solche Rechts- oder Gerichtsverfahren überlässt,
 - 14.1.3 der Kunde in vollem Umfang mit Kaspersky Lab kooperiert und so viel Hilfestellung leistet, wie Kaspersky Lab vernünftigerweise verlangen kann, um solche Rechts- oder Gerichtsverfahren (auf Kosten von Kaspersky Lab) beizulegen und/oder sich im Rahmen solcher Verfahren zur Wehr zu setzen, und
 - 14.1.4 etwaige Kostenerstattungen und/oder Schadenersatzleistungen Kaspersky Lab zugutekommen.
- 14.2 Falls die KHS fremde geistige Eigentumsrechte verletzt, kann Kaspersky Lab nach eigenem Ermessen entweder die KHS durch ein Produkt ersetzen, das keine fremden Rechte verletzt, oder diese T&Cs per schriftlicher Mitteilung an den Kunden mit sofortiger Wirkung kündigen, in welchem Falle jegliche Ansprüche auf Schadenersatz ausgeschlossen sind; allerdings hat der Kunde Anspruch auf Rückerstattung desjenigen Anteils der bereits gezahlten Gebühren, die den verbleibenden Rest des Abonnementzeitraums abdecken.
- 14.3 Die Bestimmungen der vorstehenden Klauseln 14.1 und 14.2 gelten nicht für Rechtsverletzungen, die eine Folge der nachstehenden Handlungen sind:
- 14.3.1 Gebrauch der KHS in einer Art und Weise, die nicht mit den nach diesen T&Cs zulässigen Gebrauchsformen übereinstimmen, oder
 - 14.3.2 Kombination der KHS mit fremden Produkten und/oder Leistungen oder vom Kunden vorgenommene Modifikationen, ohne hierfür die vorherige schriftliche Zustimmung von Kaspersky Lab einzuholen, falls die betreffende Kombination oder Modifikation für die Verletzung ursächlich ist.

15 Öffentlichkeitsarbeit

Der Kunde und Kaspersky Lab vereinbaren, dass jede Partei bekannt geben kann, dass beide Parteien eine Geschäftsbeziehung eingegangen sind. Kaspersky Lab ist insbesondere berechtigt, den Kunden in seine Referenzkundenliste aufzunehmen. Weitere Einzelheiten der Geschäftsbeziehung sowie Einzelheiten der Vereinbarung oder dieser T&Cs dürfen allerdings nicht ohne die ausdrückliche Zustimmung der jeweils anderen Partei bekannt gemacht werden.

16 Ergänzungen

- 16.1 Ergänzungen, Änderungen oder Aufhebung dieser T&Cs sind nur dann wirksam, wenn sie in Schriftform erfolgen. Dies schließt die Änderung oder Aufhebung dieser Klausel selbst ein.
- 16.2 Ungeachtet vorangehender Klausel 16.1 behält sich Kaspersky Lab das Recht vor, technische Details der KHS zu modifizieren, solange dadurch ihre Qualität nicht beeinträchtigt wird. Sollte eine solche Modifizierung für den Kunden aus wahrhaftigen Gründen unakzeptabel sein, haben beide Parteien die Möglichkeit, die T&Cs mit sofortiger Wirkung zu kündigen. Sämtliche Ansprüche auf Schadenersatz sind in diesem Fall ausgeschlossen, wobei der Kunde allerdings Anspruch auf Rückerstattung desjenigen Anteils der bereits gezahlten Gebühren hat, der den verbleibenden Rest des Abonnementzeitraums abdeckt.

17 Abtretung

Der Kunde ist nicht berechtigt, diese T&Cs oder daraus hervorgehende Ansprüche ohne die vorherige schriftliche Zustimmung von Kaspersky Lab abzutreten.

18 Salvatorische Klausel

Wenn eine dieser T&Cs unwirksam ist oder wird, bleibt der restliche Teil dieser T&Cs in vollem Umfang in Kraft. Die Parteien verpflichten sich in einem solchen Fall, die unwirksame Bestimmung durch eine andere gültige Bestimmung zu ersetzen, die mit der unwirksamen Bestimmung und den Zielsetzungen des Vertrags möglichst weitgehend übereinstimmt.

19 Pläne

Die KHS-Beschreibung und die hier beigefügten Pläne stellen einen wesentlichen Bestandteil dieser T&Cs dar.

20 Anwendbares Recht und Gerichtsstand

- 20.1 Diese T&Cs unterliegen dem Recht des Landes, in dem die KHS erworben wurde, und werden nach diesem Recht auch ausgelegt.
- 20.2 Die Parteien vereinbaren unwiderruflich, dass die englischen Gerichte für die Beilegung aller Streitigkeiten oder Ansprüche, die aus oder in Verbindung mit diesen T&Cs entstehen, nicht-ausschließlich zuständig sind.



Beschreibung der Kaspersky Hosted Security

1 Zusammenfassung

Kaspersky Lab ist ein Unternehmen, das sich auf IT-Sicherheitsprodukte spezialisiert. Wir bieten Kaspersky-Hosted Security (KHS) an, um den Sicherheitsrichtlinien von Unternehmen zur Durchsetzung zu verhelfen. Die KHS steht für E-Mail-Verkehr (Kaspersky Hosted E-Mail Security) und Web-Inhalte (Kaspersky Hosted Web Security) zur Verfügung. Dieses Dokument beschreibt alle KHS-Bestandteile, unabhängig davon, welche Bestandteile der Produktfamilie im Einzelfall lizenziert sind.

Diese KHS-Beschreibung ist nur insofern anwendbar, als der Kunde für den jeweiligen Bestandteil der KHS Lizenzen erworben hat; außerdem unterliegt die Beschreibung den Geschäftsbedingungen der T&Cs, denen sie beigefügt ist. Großgeschriebene Wörter, die nicht in dieser KHS-Beschreibung definiert werden, haben die ihnen in den T&Cs zugewiesene Bedeutung.

2 Definitionen

- 2.1 **Designierter Cluster** bezeichnet einen Server-Cluster, der dazu vorgesehen ist, dem Kunden die KHS auf nicht-ausschließlicher Basis bereitzustellen.
- 2.2 **Normaler Arbeitstag** bezeichnet die Tage von Montag bis Freitag, ohne öffentliche Feiertage, wie sie am Geschäftssitz von Kaspersky Lab anerkannt sind.
- 2.3 **Außerhalb der Arbeitszeit** bezeichnet jeden Zeitpunkt außerhalb der Arbeitszeit.
- 2.4 **Garantien** bezeichnet in zusammengefasster Form die Parameter der KHS-Aufgaben, wie sie in dieser KHS-Beschreibung definiert werden.
- 2.5 **Arbeitszeit** bezeichnet die Geschäftszeiten an jedem normalen Arbeitstag.

3 Verfügbarkeit der KHS

- 3.1 Die KHS wird vierundzwanzig (24) Stunden pro Tag und sieben (7) Tage pro Woche von der Kaspersky-Lab-Einsatzzentrale aus zur Verfügung gestellt. Die KHS wird auf Verfügbarkeit, Leistung und Nutzung der Netzwerk-Ressourcen überwacht. Aufgrund strenger Überwachung werden regelmäßige Anpassungen der KHS vorgenommen, um auf diese Weise zu gewährleisten, dass eine optimale Effizienz beibehalten wird.
- 3.2 Die KHS ist hoch verfügbar und skalierbar. Der gesamte Verkehr unterliegt einem Lastenausgleich zwischen Rechenzentren in verschiedenen geografischen Gebieten. Jedes Rechenzentrum selbst ist in einer hoch verfügbaren Art und Weise errichtet, um die maximal verfügbare Betriebszeit anzubieten. Im unwahrscheinlichen Fall des kompletten Ausfalls eines Rechenzentrums übernimmt das für den Kunden vorgesehene Backup-Rechenzentrum die Verantwortlichkeit, ohne dass dies zu einer merklichen Unterbrechung des Verkehrsflusses führt.
- 3.3 Die Garantien gelten NICHT,
 - 3.3.1 wenn der Kunde die KHS zur Verbreitung von Spam einsetzt,
 - 3.3.2 wenn das E-Mail-System des Kunden als Open Relay funktioniert,
 - 3.3.3 wenn der Kunde nicht die Technologie der designierten Cluster verwendet,
 - 3.3.4 während des Probezeitraums,
 - 3.3.5 wenn die System-Konfiguration des Kunden nicht allen jeweils veröffentlichten Standard-Konfigurationsleitlinien von Kaspersky Lab entspricht,
 - 3.3.6 während der Dauer von geplanten Wartungszeiträumen (vorbehaltlich Klausel 4) und von Zeiträumen der Nichtverfügbarkeit, die entweder auf höherer Gewalt oder Handlungen bzw. Unterlassungen des Kunden oder eines Dritten beruhen,
 - 3.3.7 während Zeiträumen, in denen Kaspersky Lab den KHS-Betrieb im Einklang mit den T&Cs unterbrochen hat,
 - 3.3.8 bei Ausfällen der Kunden-Infrastruktur oder -Internetverbindung,
 - 3.3.9 im Fall von KHS-Nichtverfügbarkeit, die auf unrichtigen, vom Kunden vorgelegten Informationen beruht, und
 - 3.3.10 bei Vorliegen von Gründen, die sich nach vernünftiger Anschauung der Kontrolle von Kaspersky Lab (im Sinne der Definition in den T&Cs) entziehen.

4 Geplante Wartungsarbeiten

- 4.1 Geplante Wartungsarbeiten bezeichnen Wartungszeiträume, die die Unterbrechung des KHS-Betriebs aufgrund der Nichtverfügbarkeit von Clustern oder Teilen davon zur Folge haben können. Wann immer möglich, werden geplante Wartungsarbeiten ohne Beeinträchtigung der KHS durchgeführt. Im Allgemeinen wird dies dadurch erreicht, dass geplante Wartungsarbeiten in Zeiten voraussichtlich geringen E-Mail-Verkehrs und in solchen Zeitspannen stattfinden, die so konzipiert sind, dass nachteilige Auswirkungen für Kunden vermieden werden. Während geplanter Wartungszeiträume kann der Verkehr auf Sektionen des Netzwerks umgeleitet werden, die nicht von Wartungsarbeiten betroffen sind, um die Unterbrechung des KHS-Betriebs möglichst gering zu halten.



- 4.2 Geplante Wartungsarbeiten finden nicht zwischen 8.00 und 18.00 Uhr (in der Zeitzone, in der sich ein Cluster befindet) statt.
- 4.3 Der Kunde wird von Kaspersky Lab über geplante Wartungsarbeiten mindestens sieben (7) Tage vor Aufnahme der Wartungsarbeiten informiert. Kaspersky Lab kann den Kunden durch Versenden einer E-Mail und/oder Veröffentlichung einer Warnmeldung auf dem Portal benachrichtigen.
- 4.4 Wenn unvorhergesehene Wartungsarbeiten notwendig werden und die Funktion der KHS voraussichtlich beeinträchtigen, bemüht sich Kaspersky Lab, den Kunden zu informieren, und kann eine Warnmeldung auf dem Portal veröffentlichen.

5 Web-Portal

- 5.1 Einen integralen Bestandteil der KHS bildet ein webbasiertes Konfigurations-, Management- und Berichterstattungs-Tool, das als Portal bezeichnet wird. Nachdem sich ein Kunde für die KHS angemeldet hat, werden ein spezifischer Benutzername und ein spezifisches Passwort erstellt, um dem Administrator des Kunden vollen Zugang zum Portal-Konto des Kunden zu verschaffen, in dem die Strategien und Einstellungen konfiguriert werden können. Das Portal ermöglicht auch den Zugang zu Statistiken, Meldungen und unter Quarantäne gestellten E-Mails.
- 5.2 Das Portal ist in englischer, französischer, deutscher und russischer Sprache verfügbar.

6 Technischer Support

- 6.1 Kaspersky Lab bietet technischen Support an vierundzwanzig (24) Stunden pro Tag und sieben (7) Tagen pro Woche. Support kann per Telefon oder E-Mail angefordert werden.
- 6.2 Während der Arbeitszeit steht der Support in englischer, französischer, deutscher und russischer Sprache zur Verfügung. Außerhalb der Arbeitszeit wird der Support nur in englischer Sprache angeboten.
- 6.3 Kaspersky Lab setzt sich zum Ziel und unternimmt zumutbare Anstrengungen, alle Anrufe binnen 60 Sekunden zu beantworten und mit der Bearbeitung jedes einzelnen Falls innerhalb einer Stunde zu beginnen.
- 6.4 Kunden erhalten für jede Support-Anfrage eine Ticketnummer.
- 6.5 Kontaktangaben:

	E-Mail-Adresse	Telefonnummer
Beneluxländer (holländisch)	KHS-Support@kaspersky.com	+31(0)307529539
Dänemark, Finnland, Norwegen, Schweden (dänisch, finnisch, norwegisch, schwedisch, englisch)	KHS-Support@kaspersky.com	+46(0)85 785 3031
Deutschland, Österreich, Schweiz (deutsch)	KHS-Support@kaspersky.com	+49(0)84198189760
Frankreich (französisch)	KHS-Support@kaspersky.com	+33(0)141398933
Italien	KHS-Support@kaspersky.com	
Russland (russisch)	KHS-Support@kaspersky.com	+7 (495) 9567800
Spanien ()	KHS-Support@kaspersky.com	+34 913983566
GB (englisch)	KHS-Support@kaspersky.com	+44(0)8454590165
Andere Länder (englisch)	KHS-Support@kaspersky.com	+7 (495) 9567800

- 6.6 Alle eingehenden Support-Anfragen werden erfasst und anhand folgender Matrix priorisiert:

Priorität	Problem	Rückmeldung während der Arbeitszeit	Rückmeldung außerhalb der Arbeitszeit	Lösung
I	KHS nicht verfügbar oder größerer Zwischenfall	1 Stunde	1 Stunde	Sobald wie vernünftigerweise möglich, in jedem Fall jedoch innerhalb von 24 Stunden
II	Teilweiser Verlust der KHS-Funktion, Verkehr wird aber noch verarbeitet	2 Stunden	12 Stunden	So bald wie vernünftigerweise möglich, jedoch unter Aufbietung aller Anstrengungen, eine Lösung innerhalb von zwei normalen Arbeitstagen zu erreichen



III	Technische oder Konfigurationsprobleme	4 Stunden	Am nächsten Arbeitstag	Vereinbarung zwischen Kunde und Support-Team
IV	Standard-Fragen, Quarantäne-Support, Informationsprobleme	Nach einem normalen Arbeitstag	Am nächsten Arbeitstag	Vereinbarung zwischen Kunde und Support-Team

7 Kreditanträge

- 7.1 Falls ein Kunde der Auffassung ist, dass ihm nach Maßgabe dieser KHS-Beschreibung eine Entschädigung zusteht, muss er einen Kreditantrag stellen. „Kreditantrag“ bezeichnet die Mitteilung, die der Kunde via KHS-Support@kaspersky.com mit dem Begriff „Kreditantrag“ in der Betreffzeile (soweit keine anderen Hinweise von Kaspersky Lab erfolgen) innerhalb der in der KHS-Beschreibung angegebenen Frist vorzulegen hat. Vorbehaltlich einer Überprüfung des jeweiligen Anspruchs durch Kaspersky Lab räumt das Unternehmen dem Kunden im Einklang mit den entsprechenden Regelungen dieser KHS-Beschreibung einen Kredit ein. Eine Rückerstattung bereits gezahlter Gebühren findet nicht statt. DER KUNDE ERKENNT AN, DASS AUFZEICHNUNGEN NUR FÜR EINE BEGRENZTE ANZAHL AN TAGEN AUFBEWAHRT WERDEN, WESHALB AUSSERHALB DES VORGEgebenEN ZEITRAHMENS EINGEREICHTE KREDITANTRÄGE ALS UNGÜLTIG BETRACHTET WERDEN, WAS DAZU FÜHRT, DASS DEM KUNDEN KEIN RECHT AUF EINEN KREDIT ZUSTEHT.

Kaspersky Hosted E-Mail Security

8 Definitionen

- 8.1 **Falsch negativ** bezeichnet eine Spam- und/oder Malware-infizierte E-Mail, die weder als Spam und/oder Malware erkannt wird,
- 8.2 **Falsch positiv** bezeichnet eine legitime E-Mail, die unrichtigerweise als Spam und/oder Malware gekennzeichnet bzw. erfasst wird,
- 8.3 **Bekannte Malware** bezeichnet Malware, die bereits erkannt worden ist und für die eine Signatur oder Definition bereitgestellt worden ist, die die Malware aufspürt, wenn sie entweder von Kaspersky Lab oder einem seiner Technologiepartner, dessen Anti-Malware-Technologie im Rahmen der Kaspersky Hosted E-Mail Security zum Einsatz kommt, mindestens zwanzig (20) Minuten, bevor die KHS eine mit der betreffenden Malware infizierte E-Mail scannt, im Verkehr eingesetzt wird.

9 Überblick

- 9.1 Die Kaspersky Hosted E-Mail Security bietet das Anti-Spam- und Anti-Malware-Scannen von E-Mails und deren Anlagen, um festzustellen, ob sie Malware oder Spam enthalten. Sowohl ein- als auch ausgehende E-Mails werden gefiltert.
- 9.2 Die Kaspersky Hosted E-Mail Security steht Kunden zur Verfügung, deren E-Mail-Systeme mit dem Internet permanent mithilfe einer festen IP-Adresse verbunden sind. Sie kann nicht für Kunden bereitgestellt werden, deren E-Mail-Systeme mit dem Internet via Dial-up oder ISDN-Leitungen verbunden sind oder deren IP-Adresse dynamisch zugeteilt wird.
- 9.3 Der gesamte E-Mail-Verkehr wird unter Einsatz von SMTP über einen designierten Cluster geleitet.
- 9.4 Kaspersky Lab bietet einen opportunistisch verschlüsselten Link zwischen dem zugewiesenen Datenzentrum und dem Mail-Server des Kunden unter Nutzung von TLS (sofern der Mail-Server des Kunden die TLS-Verschlüsselung unterstützt).
- 9.5 Die Kaspersky Hosted E-Mail Security kann E-Mails bis zu einer maximalen Größe von 100 MB scannen. E-Mails mit einer Größe von mehr als 100 MB werden mit einem entsprechenden Fehlercode zurückgewiesen.
- 9.6 Bei allen eingehenden Mails wird die IP-Reputation des Absenders überprüft. E-Mails, die von einer zweifelhaften Quelle stammen (wie etwa Spammer), werden verlangsamt oder an der Verbindungsebene zurückgewiesen, um die KHS-Auswirkungen zu minimieren.
- 9.7 Der Kunde kann das Portal für Zwecke des Filterns von E-Mails um E-Mail-Domains erweitern.
- 9.8 Die Kaspersky Hosted E-Mail Security bietet mehrere Optionen für die Handhabung durch den Nutzer. Der Kunde kann entscheiden, welche Option er akzeptiert: alle E-Mail-Adressen für eine Domain werden automatisch hinzugefügt, nur manuell definierte E-Mail-Adressen, nur als gültig bestätigte E-Mail-Adressen, die eine SMTP-Autorisierung verwenden oder nur E-Mail-Adressen, die vom Service per LDAP-Abfrage beim Directory-Server des Kunden als gültig bestätigt werden.

10 Kaspersky Hosted E-Mail Security. Anti-Spam

- 10.1 Die Anti-Spam-Funktion verwendet mehrere Technologien, um höchstmögliche Spam-Erkennungsraten zu gewährleisten.
- 10.2 Die Anti-Spam-Engine wird kontinuierlich justiert, um E-Mails zu erkennen, bei denen es sich mit großer Sicherheit um Spam („Spam“) und vermutlich um Spam („vermutliches Spam“) handelt.
- 10.3 Der Kunde kann getrennte Einstellungen konfigurieren, die auf Spam- oder vermutliche Spam-E-Mails angewendet werden. Folgende Einstellungen sind verfügbar: Keine Aktion, Kennzeichnung des Betreffs, Löschen der E-Mail und E-Mail unter Quarantäne stellen.
- 10.4 Liste bestätigter Absender: E-Mail-Adressen, Domains oder IP-Adressen von E-Mail-Servern können der Liste bestätigter Absender hinzugefügt werden. Der Inhalt solcher eingehender E-Mails wird nicht auf Spam gescannt, und, sofern sie nicht wegen anderer Stellen in der Richtlinie gefiltert werden, etwa weil sie Malware enthalten, werden sie ausgeliefert.
- 10.5 Liste blockierter Absender: E-Mail-Adressen, Domains oder IP-Adressen von E-Mail-Servern können der Liste blockierter Absender hinzugefügt werden, und E-Mails mit Adressen aus dieser Liste werden mit einer entsprechenden Fehlermeldung zurückgewiesen.
- 10.6 Einträge in den Listen bestätigter und blockierter Absender können in der KHS unter Verwendung des Portals konfiguriert werden.
- 10.7 Gruppen-Funktionen ermöglichen, dass Nutzer oder E-Mail-Domains für Zwecke der Anwendung von Richtlinien oder Anzeige von Meldungen zusammengefasst werden. Für jede Gruppe kann eine eigene Richtlinie gelten.

11 Kaspersky Hosted E-Mail Security. Anti-Malware

- 11.1 Die Anti-Malware-Funktion der KHS besteht aus mehreren Anti-Malware-Technologien, um ein Höchstmaß an Sicherheit zu bieten. Anti-Malware-Engines verwenden auf Mustererkennung basierte oder signaturbasierte Technologien sowie heuristische Algorithmen (Kaspersky BitHunt Engine), um Kunden vor Zero-Hour-Malware zu schützen.



- 11.2 Kaspersky BitHunt ist eine hoch entwickelte und geschützte Engine von Kaspersky Lab, die nur über die KHS verfügbar ist und Kunden vor Zero-Hour-Malware schützt, indem sie bösartige E-Mails noch vor dem Einsatz von auf Mustererkennung basierter Technologie erkennt.
- 11.3 Wenn Malware in einer E-Mail entdeckt wird, muss eine Maßnahme eingeleitet oder eine Anordnung getroffen werden. Diese Anordnung kann vom Kunden konfiguriert werden. Er gibt folgende Optionen: einen Tag in der Betreffzeile hinzufügen, die E-Mail löschen, eine Anlage löschen oder die E-Mail unter Quarantäne stellen.

12 Kaspersky Hosted E-Mail Security. Geschäftskontinuität

- 12.1 Kaspersky Lab überwacht die Anzahl der E-Mails für jeden Kunden in den Warteschlangen auf seinen E-Mail-Servern kontinuierlich. Wenn im Fall einer verbundenen Domain eine sich vergrößernde Warteschlange erkannt wird, überprüft Kaspersky Lab die Kapazität des empfangenden Mail-Servers zum Empfang von E-Mails. Falls Kaspersky Lab nicht in der Lage ist, E-Mails an den Mail-Server eines Kunden auszuliefern, speichert das Unternehmen eingehende E-Mails des Kunden für bis zu sieben (7) Tage. Während dieses Zeitraums unternimmt Kaspersky Lab periodische Versuche, die in der Warteschlange befindlichen E-Mails auszuliefern; wenn dies möglich wird, geschieht dies auf kontrollierte Art und Weise.
- 12.2 Kaspersky Lab bietet dem Kunden Zugang zu allen eingehenden E-Mails, die sich in der Warteschlange befinden, weil der E-Mail-Server des Kunden nicht in der Lage ist, sie über ein Portal zu empfangen. Solche Mails sind im Portal verfügbar.

13 Kaspersky Hosted E-Mail Security. Anlagenverwaltung

- 13.1 Die Funktion Anlagenverwaltung ermöglicht die Kontrolle von Größe, Typ und Bezeichnungen von Anlagen zu E-Mails.
 - 13.1.1 Kaspersky Hosted E-Mail Security kann zwischen Dokumenten, ausführbaren Dateien, Archiven, Grafiken sowie Audio-, Video und anderen Datei-Typen unterscheiden.
 - 13.1.2 Ein freies Textfeld steht zur Verfügung, um Text hinzuzufügen (ein Teilstring), der dann gegen die Anlage auf nachfolgende Arten abgeglichen werden kann: Name enthält Teilstring, Name entspricht Teilstring, Extension enthält Teilstring, Extension entspricht Teilstring, Name oder Extension enthalten Teilstring oder Name oder Extension entsprechen Teilstring.
- 13.2 Der Kunde kann konfigurieren, wie mit einem Passwort verschlüsselte Dateien zu behandeln sind. Verfügbare Einstellungen für die vorstehenden Anlageregulungen sind: keine Maßnahmen, den Betreff kennzeichnen, die E-Mail löschen und die E-Mail unter Quarantäne stellen.

14 Kaspersky Hosted E-Mail Security. Quarantäne

- 14.1 Alle unter Quarantäne gestellten E-Mails werden für 30 Tage gespeichert und sodann automatisch gelöscht.
- 14.2 Alle in Quarantäne befindlichen E-Mails können über das Portal in sicherer Form aufgerufen und verwaltet werden.
- 14.3 Der Quarantäne-Bereich des Portals verfügt über eine Textsuchfunktion in den Betreff-, Empfänger- und Absenderfeldern. Im Anschluss an eine Suche werden E-Mails, die den Kriterien entsprechen, mit Uhrzeit, Absender, Empfänger, Betreff, Status und Größe angezeigt.
- 14.4 Von der Suchergebnisseite können E-Mails geöffnet, gelöscht oder freigegeben werden.
- 14.5 Zusätzliche und detaillierte Kopfzeileninformationen sind für jede in Quarantäne befindliche E-Mail verfügbar, indem die E-Mail und die Schaltfläche für Kopfzeilen angeklickt werden.
- 14.6 Listen blockierter und bestätigter Absender von Domain oder Absender können durch Anklicken der entsprechenden Schaltflächen in der Quarantäne-Ansicht modifiziert werden.
- 14.7 Nutzer können unter Quarantäne gestellte Mails mithilfe des Quarantäne-Berichts freigeben.

15 Kaspersky Hosted E-Mail Security. Berichte

- 15.1 Berichte können innerhalb des Portals erstellt werden. Die Verfügbarkeit solcher Berichte hängt von den KHS-Bestandteilen ab, für die der Kunde eine Lizenz erworben hat.
- 15.2 Alle Berichte stehen in grafischem (HTML) oder PDF-Format zur Verfügung.
- 15.3 Berichte können für bestimmte Zeiträume und Domains, für Mailboxen, Gruppen von Mailboxen und Gruppen von Domains erstellt werden.
- 15.4 Ein zusammenfassender Bericht über Kontenbewegungen zeigt die Anzahl der Transaktionen sowie deren Kategorien und Größenordnungen an.
- 15.5 Berichte sind in Bezug auf E-Mails, Nutzer, Malware, Spam, Phishing und Quarantäne erhältlich.
- 15.6 Detaillierte Aufzeichnungen können innerhalb des Berichtsbereichs des Portals aufgerufen werden.
- 15.7 E-Mail-Berichte geben die Anzahl von E-Mails und das Volumen des Verkehrs an.



- 15.8 Berichte zeigen ein- wie ausgehenden Verkehr an.
- 15.9 Der Quarantäne-Bericht (quarantine report, QR) stellt jedem Nutzer einen Bericht zur Verfügung, der alle ihre in Quarantäne befindlichen E-Mails anzeigt. Dieser Bericht kann unter Verwendung des Portals angefordert werden und wird per E-Mail ausgeliefert bzw. kann durch Anmeldung im Portal eingesehen werden.
- 15.9.1 Berichtshäufigkeit: Täglich, wöchentlich, monatlich und in mit einem Nutzer abgesprochenen Intervallen.
- 15.9.2 Berichtszeitraum: Heute, gestern, diese Woche, letzte Woche, dieser Monat, letzter Monat.
- 15.9.3 Informationen im QR: Berichtszeitraum, E-Mail-Anzahl, E-Mails in Quarantäne und der Grund dafür, warum jede einzelne E-Mail unter Quarantäne gestellt wurde
- 15.10 Nutzer können die Freigabe von in Quarantäne befindlichen Mails veranlassen, während sie den Quarantäne-Bericht durchgehen.
- 15.11 Berichte werden in Echtzeit erstellt.

16 Kaspersky Hosted E-Mail Security. Garantien

- 16.1 Verfügbarkeit. Kaspersky Lab garantiert für die Kaspersky Hosted E-Mail Security eine Uptime von 99,999 %.
- 16.2 Im Verhältnis zu E-Mail-Sicherheit wird Verfügbarkeit als die Fähigkeit definiert, eine SMTP-Session auf Port 25 des designierten Clusters einzurichten, wie von Kaspersky Lab gemessen. Diese Garantie gilt nur dann, wenn alle erforderlichen Konfigurationen vom Kunden vorgenommen wurden, die den designierten Cluster in die Lage versetzen, für den Kunden eingehende E-Mails zu empfangen und vom Kunden zu versendende E-Mails auf der Basis von 24 Stunden pro Tag und 7 Tagen pro Woche zu akzeptieren.
- 16.3 Wenn die Verfügbarkeit in einem beliebigen Kalendermonat unter 99,999 % beträgt, kann der Kunde einen Anspruch auf den folgenden Kreditprozentsatz geltend machen:

Verfügbarkeit pro Kalendermonat	Kreditprozentsatz der Monatsgebühr
< 99,999 %, aber >= 99,99 %	10 %
< 99,99 %, aber >= 99 %	25 %
< 99 %, aber >= 98 %	50 %
< 98 %	100 %

- 16.4 Sofern die Verfügbarkeit in einem beliebigen Kalendermonat unter achtundneunzig Prozent (98 %) fällt, ist der Kunde berechtigt, die T&Cs mit sofortiger Wirkung zu kündigen und den Anteil an Gebühren zurückzuerhalten, der sich auf den angegebenen, nicht in Anspruch genommenen Zeitraum ab dem Kündigungsdatum bezieht.
- 16.5 Falls der Kunde annimmt, dass er Anspruch auf Abhilfe nach Maßgabe von Klausel 16.3 hat, muss er innerhalb von vierzehn (14) Tagen nach Ablauf des fraglichen Kalendermonats einen Kreditantrag stellen.
- 16.6 E-Mail-Latenzzeit. Kaspersky Lab garantiert, dass die durchschnittliche Zeit für die Verarbeitung von E-Mails (die von Kaspersky Lab per Versenden von E-Mails alle 5 Minuten an den designierten Cluster gemessen wird) weniger als 60 Sekunden beträgt. Wenn in einem beliebigen Kalendermonat die Latenzzeit über die Verzögerungen hinausgeht, die in der nachfolgenden Tabelle angegeben werden, kann der Kunde einen Anspruch auf den folgenden Kreditprozentsatz geltend machen:

Durchschnittliche Roundtrip-Zeit pro Monat	Kreditprozentsatz der Monatsgebühr
>1 Min. aber <= 1 Min. 30 Sek.	25 %
>1 Min. 30 Sek. aber <= 2 Min.	50 %
>2 Min. aber <= 2 Min. 30 Sek.	75 %
>2 Min. 30 Sek.	100 %

- 16.7 Falls der Kunde annimmt, dass er Anspruch auf Abhilfe nach Maßgabe von Klausel 16.6 hat, muss er innerhalb von vierzehn (14) Tagen nach Ablauf des fraglichen Kalendermonats einen Kreditantrag stellen.
- 16.8 Malware-Erkennung: Kaspersky Lab erkennt alle bekannte Malware im von der KHS verarbeiteten Verkehr zu 100 %.
- 16.9 Falls in einem beliebigen Kalendermonat eine oder mehrere Kopien von bekannter Malware, die von der KHS gescannt worden ist, nicht erkannt werden und die Infizierung der Kundensysteme ausgelöst haben, übernimmt Kaspersky Lab angemessene Arbeitskosten, die direkt und nachweislich zur Entfernung der Malware vom Kunden-Netzwerk angefallen sind,



bis zu einem Maximalbetrag in Höhe von 3 Monatsrechnungen. Um eine solche Kostenerstattung zu erhalten, muss der Kunde Kaspersky Lab innerhalb von 14 Tagen nach dem Eintritt der Verletzung dieser Garantie einen Kreditantrag senden. Der Kreditantrag hat die Malware und die Infektionsursache zu beschreiben und dabei darzulegen, dass die KHS nicht in der Lage war, die betreffende Malware herauszufiltern, und einen Nachweis für die entstandenen Kosten zu enthalten, deren Erstattung verlangt wird.

16.10 Die Systeme des Kunden gelten als infiziert, wenn ein Virus, der Bestandteil des Verkehrs ist, der über die KHS empfangen wird, in den Kundensystemen entweder automatisch oder per manueller Intervention aktiviert worden ist.

16.11 Die in Klauseln 16.8 und 16.9 enthaltene Malware-Garantie findet keine Anwendung, wenn

16.11.1 sich die Malware in einer E-Mail befand, die von der KHS weder gescannt noch analysiert werden konnte (z. B. verschlüsselte oder mit einem Passwort geschützte E-Mails),

16.11.2 Kaspersky Lab den Kunden unmittelbar nach Auslieferung einer E-Mail mit der Malware entsprechend informiert und der Kunde dennoch keine angemessenen Maßnahmen ergriffen hat,

16.11.3 die Malware vom Kunden aus der Quarantäne entlassen worden oder

16.11.4 es seitens des Kunden zu einer Selbst-Infizierung gekommen ist.

16.12 Spam-Erkennungsrate: Kaspersky Lab garantiert, 98 % aller eingehenden Spam-Mails zu erkennen und im Einklang mit der vom Kunden unter Nutzung des Portals konfigurierten Richtlinie vorzugehen.

16.13 Falls in einem beliebigen Kalendermonat die Spam-Erkennungsrate, die als die Zahl der korrekt identifizierten Spam-Mails dividiert durch die Summe aus korrekt identifizierten Spam-Mails und falsch negativen E-Mails berechnet wird, geringer ist als in der Tabelle angegeben, kann der Kunde einen Anspruch auf den folgenden Kreditprozentsatz geltend machen:

Spam-Erkennungsrate im Kalendermonat	Kreditprozentsatz der Monatsgebühr
< 98 %, aber >= 97 %	25 %
< 97 %, aber >= 96 %	50 %
< 96 %, aber >= 95 %	75 %
< 95 %	100 %

16.14 Um diesen Kredit zu erhalten, muss der Kunde mutmaßliche falsch negative E-Mails innerhalb von 5 Tagen nach Erhalt der E-Mail als Anlage an KHS-Support@kaspersky.com schicken und dabei darauf achten, dass alle Kopfzeilen in den Original-E-Mails intakt bleiben. Kaspersky Lab untersucht und teilt sodann mit, ob es sich bei der E-Mail um eine falsch negative Spam-Mail handelt, und zeichnet das Resultat auf. Wenn der Kunde am Ende eines Kalendermonats annimmt, dass ihn die Anzahl bestätigter falsch negativer Spam-Mails zu einem Anspruch im Einklang mit Klausel 16.13 berechtigt, muss er Kaspersky Lab innerhalb von 14 Tagen nach Ablauf des jeweiligen Kalendermonats einen Kreditantrag zusenden.

16.15 Diese Garantie gilt nicht, wenn:

16.15.1 der Kunde bei der Konfiguration der KHS nicht nach Kaspersky Labs bewährten Verfahren vorgegangen ist oder

16.15.2 die E-Mail nicht an eine legitime Adresse versandt worden ist.

16.16 Für E-Mails, die asiatische und arabische Zeichensätze enthalten, gilt eine geringere Spam-Erkennungsrate von 95 %. Falls die Spam-Erkennungsrate unter 95 % fällt, hat der Kunde Anspruch auf einen Kreditprozentsatz von 25 der Monatsgebühr. Falls die Spam-Erkennungsrate unter 90 % fällt, hat der Kunde Anspruch auf einen Kreditprozentsatz von 100 % der Monatsgebühr.

16.17 Falsch positive Spam-Mails Wenn die durchschnittliche Erkennungsrate bezüglich falsch positiver Spam-Mails in einem beliebigen Kalendermonat über 0,0004 % des gesamten E-Mail-Verkehrs des Kunden steigt, kann der Kunde einen Kredit nach Maßgabe der nachstehenden Tabelle geltend machen.

Erkennungrate falsch positiver Spam-Mails während des Kalendermonats	Kreditprozentsatz der Monatsgebühr
>0,0004 %, aber <= 0,004 %	25 %
> 0,004 %, aber <= 0,04 %	50 %
> 0,04 %, aber <= 0,4 %	75 %
>0,4 %	100 %

16.18 Um einen Kredit nach Maßgabe dieser Klausel 16.17 erhalten zu können, muss der Kunde mutmaßliche falsch positive E-Mails innerhalb von 5 Tagen nach Erhalt der E-Mail als Anlage an KHS-Support@kaspersky.com versenden. Kaspersky Lab untersucht und teilt sodann mit, ob es sich bei der E-Mail um eine falsch positive E-Mail handelt, und zeichnet das



Resultat auf. Wenn der Kunde am Ende eines Kalendermonats annimmt, dass ihn die Anzahl bestätigter falsch positiver E-Mails zu einem Anspruch im Einklang mit Klausel 16.17 berechtigt, muss er Kaspersky Lab innerhalb von 14 Tagen nach Ablauf des jeweiligen Kalendermonats einen Kreditantrag zusenden.

- 16.19 Im Rahmen dieser Garantie stellen die folgenden E-Mails keine falsch positiven E-Mails dar:
- 16.19.1 E-Mails, die keine legitimen geschäftlichen E-Mails sind,
 - 16.19.2 E-Mails, deren Absender der Liste der blockierten Absender des Kunden angehört,
 - 16.19.3 E-Mails, die von einer kompromittierten Quelle aus versandt und nach Klausel 9.6 zurückgewiesen werden,
 - 16.19.4 E-Mails, die von einer Maschine versandt werden, die auf der Liste von blockierten Absendern eines Dritten geführt wird, und
 - 16.19.5 E-Mails, die an mehr als 20 Empfänger versandt worden sind und zu mindestens 80 % über einen gemeinsamen Inhalt verfügen.

Kaspersky Hosted Web Security

17 Überblick

- 17.1 Die Konfigurationseinstellungen, die erforderlich sind, um diesen externen Verkehr durch die Kaspersky Hosted Web Security zu leiten, werden vom Kunden vorgenommen und aufrechterhalten und hängen von dessen technischer Infrastruktur ab. Der Kunde sollte sicherstellen, dass interner HTTP/FTP-über-HTTP-Verkehr (etwa zum betrieblichen Intranet) nicht durch die KHS geleitet wird. Wenn der Kunde Internet-Dienste in Anspruch nimmt, die eine direkte Verbindung anstelle eines Proxy-Anschlusses voraussetzen, liegt es in seiner Verantwortung, die notwendigen Änderungen an seiner eigenen Infrastruktur vorzunehmen, um dies zu ermöglichen.
- 17.2 Sobald die relevanten Konfigurationsänderungen durchgeführt worden sind, werden Anfragen nach Websites und Anlagen elektronisch durch die Kaspersky Hosted Web Security geleitet und digital auf Malware untersucht.
- 17.3 Die externen HTTP und FTP-über-HTTP-Anfragen des Kunden einschließlich aller Anlagen, Makros und ausführbaren Dateien werden durch die Kaspersky Hosted Web Security geführt. Andere durch HTTP geleitete Inhalte (wie etwa Streaming-Medien) können ebenfalls durch die Kaspersky Hosted Web Security geleitet werden; sie werden allerdings nicht gescannt.
- 17.4 Der Zugang zur KHS wird über Scanning-IPs beschränkt, also die IP-Adresse(n), von denen der Web-Verkehr des Kunden seinen Ausgang nimmt. Die Scanning-IPs werden auch zur Erkennung des Kunden und zur dynamischen Auswahl kundenspezifischer Einstellungen benutzt.
- 17.5 Nutzer können durch die IP-Adresse des Kunden-Gateways oder über den Verzeichnisdienst identifiziert werden.
- 17.6 Die Kaspersky Hosted Web Security scannt die Website und ihre Anlagen im größtmöglichen Umfang. Es ist unter Umständen nicht möglich, bestimmte Websites, Inhalte oder Anlagen zu scannen (etwa, wenn sie mit einem Passwort geschützt sind). Anlagen, die spezifisch als nicht scanbar kenntlich gemacht sind, werden nicht blockiert. Gestreamter und verschlüsselter Verkehr (d. h. Streaming-Medien und/oder HTTPS/SSL) kann nicht gescannt werden und passiert die Kaspersky Hosted Web Security daher ungescannt.
- 17.7 Kaspersky Lab legt Wert auf die Feststellung, dass die Konfiguration der Kaspersky Hosted Web Security der alleinigen Kontrolle des Kunden unterliegt. Die in dieser KHS-Beschreibung dargestellte KHS soll ausschließlich dafür benutzt werden, den Kunden in die Lage zu versetzen, einer bereits existierenden, wirksam umgesetzten und akzeptablen Richtlinie zur Nutzung von Computern (oder einer vergleichbaren Richtlinie) zur Durchsetzung zu verhelfen. In bestimmten Ländern kann es erforderlich sein, die Zustimmung der einzelnen Mitarbeiter zu erhalten, weshalb Kaspersky Lab dem Kunden rät, vor der Inbetriebnahme der Kaspersky Hosted Web Security in jedem Fall die jeweilige örtliche Gesetzeslage zu prüfen.
- 17.8 Benutzer-E-Mails können vom Administrator so festgelegt werden, dass sie den Benutzer informieren, wenn ein Virus oder Spyware entdeckt worden ist.
- 17.9 Der Administrator kann eine weiße Liste für Adware-Programme anlegen.

18 Kaspersky Hosted Web Security. Berichterstattung

- 18.1 Zusammenfassende Berichte können täglich, wöchentlich, monatlich oder jährlich erstellt werden.
- 18.2 Zusammenfassende Berichte können als grafische Darstellung, XML, CSV oder Tabelle angelegt werden.
- 18.3 Regelmäßige Berichte können aufgrund folgender Ereignisse erstellt werden:



- 18.3.1 Blockade von Top-Viren
- 18.3.2 Blockierte Viren nach Anzahl der Treffer
- 18.3.3 Top-Gruppen nach blockierten Viren
- 18.3.4 Protokoll-Trend nach Bandbreite
- 18.3.5 Protokoll-Trend nach Verbindungen
- 18.3.6 Top-Nutzer nach blockierten Viren
- 18.3.7 Zulässige Verkehrsberichte
- 18.3.8 Blockierte Verkehrsberichte
- 18.4 Die Häufigkeit regelmäßiger Berichte kann wie folgt sein:
 - 18.4.1 Nur ein einziges Mal
 - 18.4.2 Täglich
 - 18.4.3 Wöchentlich
 - 18.4.4 Monatlich
- 18.5 Forensische Berichte können für bestimmte Nutzer oder Gruppen in eigens festgelegten Zeitabständen erstellt werden.

19 Kaspersky Hosted Web Security. Scannen von Viren (AV)

- 19.1 Sobald die relevanten Konfigurationsänderungen vorgenommen worden sind, werden Websites und Anlagen mit branchenführenden Anti-Virus-Engines gescannt.
- 19.2 AV scannt die Website und ihre Anlagen im größtmöglichen Umfang. Es ist unter Umständen nicht möglich, bestimmte Websites oder Anlagen zu scannen (etwa, wenn sie mit einem Passwort geschützt sind). Nicht scanbare Anlagen werden blockiert. Verschlüsselter Verkehr (d. h. HTTPS/SSL) kann nicht gescannt werden und passiert AV ungescannt.
- 19.3 Wenn die Website eines Kunden oder deren Anlagen nachweislich Malware enthält (oder als nicht scanbar betrachtet wird), wird der Zugang zur Website oder zur Anlage verhindert und dem Internet-Nutzer wird automatisch eine Virenwarn-Website angezeigt. Eine entsprechende Benachrichtigung kann auch per E-Mail an einen Kunden-Administrator versandt werden.
- 19.4 AV scannt die ersten 100 MB jeder Datei-Übertragung. Im Fall eines Downloads von mehr als 100 MB werden die ersten 100 MB gescannt und der Rest der Datei passiert ungescannt.

20 Kaspersky Hosted Web Security. Screening von Spyware (SPS)

- 20.1 Sobald die relevanten Konfigurationsänderungen vorgenommen worden sind, werden Websites und Anlagen gescannt und gefiltert.
- 20.2 SPS scannt die Websites oder ihre Anlagen im größtmöglichen Umfang. Es ist unter Umständen nicht möglich, bestimmte Websites oder Anlagen zu scannen (etwa, wenn sie mit einem Passwort geschützt sind). Nicht scanbare Anlagen werden blockiert. Verschlüsselter Verkehr (d. h. HTTPS/SSL) kann nicht gescannt werden und passiert SPS ungescannt.
- 20.3 Wenn die Website eines Kunden oder deren Anlagen nachweislich Spyware enthält (oder als nicht scanbar betrachtet wird), wird der Zugang zur Website oder zur Anlage verhindert und dem Internet-Nutzer wird automatisch eine Spyware-Warnwebsite angezeigt. Eine entsprechende Benachrichtigung kann auch per E-Mail an einen Kunden-Administrator versandt werden.
- 20.4 SPS scannt die ersten 100 MB jeder Datei-Übertragung. Im Fall eines Downloads von mehr als 100 MB werden die ersten 100 MB gescannt und der Rest der Datei passiert ungescannt.

21 Kaspersky Hosted Web Security. Web-Filtering (WF)

- 21.1 Sobald die relevanten Konfigurationsänderungen vorgenommen worden sind, werden Websites und Anlagen unter Einsatz von URL-Kategorisierung und Inhaltsanalyse gefiltert. URLs werden per Bezugnahme auf eine Anzahl vorab definierter Kategorien entsprechend den Vorgaben im Portal eingestuft.
- 21.2 Der Kunde ist in der Lage, das Web-Filtering zu konfigurieren, um Richtlinien für eine Zugangsbeschränkung zu erstellen (die sowohl auf Kategorien als auch auf Inhaltsarten basieren) und diese zu bestimmten Zeiten gegenüber bestimmten Internet-Nutzern oder Gruppen zum Einsatz zu bringen. Eine Reihe weiterer Features (wie etwa die Funktionen von Listen bestätigter und blockierter URLs) steht ebenfalls zur Verfügung.
- 21.3 WF filtert die Website und ihre Anlagen im größtmöglichen Umfang. Es ist unter Umständen nicht möglich, bestimmte Websites oder Anlagen zu filtern (etwa, wenn sie mit einem Passwort geschützt sind). Kunden können auch bestimmte Ausnahmen für Websites konfigurieren, die nicht gefiltert werden sollen. Verschlüsselter Verkehr (d. h. HTTPS/SSL) kann nicht gefiltert werden und passiert WF ungefiltert, sofern keine anderen Vorgaben des Kunden in Bezug auf bestimmte Kategorien von Inhalten vorliegen. WF filtert nur Websites, die von WF nach Maßgabe der Kategorie eingestuft worden sind, für die der Kunde das Filtern angeordnet hat.



- 21.4 Der Kunde kann sich bezüglich des Einsatzes der jeweiligen Agent-Software-Applikation zwischen der Ausübung individueller und/oder gruppenbasierter Verwaltungs- und Berichterstattungsfähigkeiten entscheiden. Der Einsatz der Agent-Applikation unterliegt dem Endnutzer-Lizenzvertrag, der zusammen mit der Applikation vorgelegt wird.
- 21.5 Wenn ein Internet-Nutzer eine Website oder eine Anlage anfordert, auf die eine Richtlinie zur Zugangsbeschränkung Anwendung findet, wird der Zugang zu der betreffenden Website oder Anlage verhindert und dem Nutzer automatisch eine Warn-Website angezeigt. Eine entsprechende Benachrichtigung kann auch per E-Mail an einen Kunden-Administrator versandt werden.

22 Kaspersky Hosted Web Security Connector

- 22.1 Kaspersky Lab stellt den Kunden optionale Software („Connector“) bereit. Wenn der Kunde die Connector-Software bestellt, wird sie ihm von Kaspersky Lab zur Verfügung gestellt, um in seinem Netzwerk im Einklang mit den Installationsanleitungen von Kaspersky Lab installiert zu werden. Es gibt zwei Arten von Connector-Software:
- Der Arbeitsgruppen-Connector ist für Kunden mit einer einfachen Netzwerk-Konfiguration gedacht. Er ermöglicht die Erkennung einzelner Nutzer, wenn sie auf die Dienste (unter Nutzung eines Lizenzschlüssels) zugreifen. Kunden sind daher in der Lage, das Portal zur Anwendung von Richtlinien zu nutzen sowie individuelle Nutzer oder Gruppen im Sinne der Definition in vorhandenen Kundenverzeichnissen zu verwalten und diesen gegenüber Bericht zu erstatten, soweit dies vom Connector unterstützt wird. Der Arbeitsgruppen-Connector läuft im Stand-alone-Modus und bietet sowohl Weiterleitung als auch AD-Integration.
 - Der Unternehmens-Connector ist für Kunden bestimmt, die bereits über Edge-Einrichtungen (z. B. ISA Server, Checkpoint, Cisco, Blue Coat) verfügen und die KHS mit diesen integrieren müssen.
- 22.2 Der Connector ermöglicht Nutzern, sich mit den Diensten auch ohne eine statische IP-Adresse unter Verwendung eines Lizenzschlüssels zu verbinden. Wenn Nutzer andere Dienste in Anspruch nehmen, die für Identifikationszwecke auf eine feste IP-Adresse angewiesen sind, können sie für spezifische Websites, Domains, Hosts oder Netzwerke direkte Verbindungen konfigurieren.
- 22.3 Administratoren sind berechtigt, Lizenzschlüssel für Connector-Software pro Gruppe oder pro Nutzer zu erstellen, zurückzunehmen, zu aktivieren und zu deaktivieren.
- 22.4 Der Connector unterstützt nicht alle potenziellen Kundensysteme und -konfigurationen. Technische Informationen können unter <http://support.kaspersky.com/faq/?qid=208281752> eingesehen werden.

23 Kaspersky Hosted Web Security. Garantien

- 23.1 Verfügbarkeit. Kaspersky Lab garantiert für die Kaspersky Hosted Web Security eine Uptime von 99,999 %.
- 23.2 Uptime wird im Fall der Kaspersky Hosted Web Security als die Fähigkeit definiert, die vom Kunden ausgehenden Web-Anforderungen zu akzeptieren, und ist nur dann maßgeblich, wenn Host, Gateway-Geräte oder Proxy(s) des Kunden in korrekter Art und Weise auf der Basis von 24 Stunden pro Tag und sieben Tagen pro Woche konfiguriert sind.
- 23.3 Alle Maßeinheiten der beschriebenen Funktionen und Garantien werden für einen Kalendermonat festgelegt.
- 23.4 Für den Fall, dass Kaspersky Lab die in der nachstehenden Tabelle festgehaltene Verfügbarkeitsverpflichtung nicht einhält, kann der Kunde den folgenden Kreditprozensatz geltend machen:

Verfügbarkeit pro Kalendermonat	Kreditprozensatz der Monatsgebühr
< 99,999 %, aber >= 99,99 %	10 %
< 99,99 % ,aber >= 99 %	25 %
< 99 %, aber >= 98 %	50 %
< 98 %	100 %

- 23.5 Um den Kredit zu erhalten, muss der Kunde an KHS-Support@kaspersky.com innerhalb von 14 Tagen nach dem Eintritt der Verletzung dieser Garantie einen Kreditantrag schicken.

