# NetUSE Threat Emulation E-Mail

## **Spezielle Leistungsbeschreibung,** Version 1.1, 08.04.2019

1. Leistungsmerkmale NetUSE Threat Emulation E-Mail

1.1 Allgemeine Dienstbeschreibung

Dieser Dienst umfasst die Bereitstellung, den Betrieb, die Überwachung, die Lizenzen, die notwendigen (Image-, OS-, Engine-, Pattern-)Updates und das Backup einer redundanten Threat-Emulation-Lösung für E-Mail-Anhänge (Attachments) auf Basis des Protokolls SMTP (Simple Mail Transfer Protocol) in den Rechenzentren der NetUSE AG, die via Mailrouting integriert wird. Die Bereitstellung erfolgt auf gemeinsam genutzter Infrastruktur. Bei Threat Emulation handelt es sich ganz allgemein um die Ausführung von potentiell schädlichen Dateien in einer isolierten Sandbox, um mit der Analyse des Laufzeitverhaltens bislang unbekannte Schadsoftware zu identifizieren und herauszufiltern.

1.2 Mailtransport

Der Dienst NetUSE Threat Emulation E-Mail ermöglicht dem Kunden den Austausch von elektronischen Nachrichten im Store-and-Forward-Verfahren auf der Basis international anerkannter Normen (Simple Mail Transfer Protocol (SMTP), Extended SMTP (ESMTP)) für den Mailtransport zwischen dem Mailsystem des Kunden und den NetUSE Mailrelay-Gateways ausschließlich für aus Sicht des Kunden eingehende E-Mails. Die NetUSE Mailrelay-Gateways unterstützen eine verschlüsselte Übertragung von E-Mails via TLS (Transport Layer Security).
Die NetUSE Mailrelay-Server nehmen dabei im Rahmen dieses Services ausschließlich Mails von ausgewählten IP-Adressen (Mailservern) des Kunden und nur für die konfigurierten Mail-Domains des Kunden an. Alternativ kann der Kunde über den Service NetUSE Mailrelay ein vollständiges Mailrelay (primärer MX) für seine Mail-Domains beauftragen.

1.3 Analyse von Attachments (Threat Emulation bzw. TE)

Der Service NetUSE Threat Emulation E-Mail analysiert E-Mails hinsichtlich ihrer Attachments wie folgt:

1.3.1 vom Service jeweils aktuell unterstützte Archivformate werden (bei geschachtelten Archiven aktuell bis zu einer Tiefe von 7) ausgepackt,

1.3.2 aus Sicht des Service nicht emulierbare bzw. nicht entpackbare Attachments werden durchgelassen,

1.3.3 aus Sicht des Service emulierbare Attachments (bzw. ausgepackte Dateien) werden per Hash mit bereits bekannten Attachment Hashes verglichen und die Einstufung (Malware oder keine Malware) und Behandlung entsprechend übertragen,

1.3.4 aus Sicht des Service emulierbare Attachments (bzw. ausgepackte Dateien), die noch unbekannt sind, werden emuliert, um sie auf Malware-typisches Verhalten zu analysieren.

1.3.5 Als potentielle Malware erkannte Attachments werden geblockt, andernfalls werden die Attachments mit der jeweiligen E-Mail durchgelassen. Im Falle von Archiven mit mehreren Dateien werden die kompletten Archive geblockt, sofern eine Datei in dem Archiv als potentielle Malware erkannt wurde. Auch bei geblockten Attachments (bzw. Archiven) werden die zugehörigen E-Mails mit einem entsprechenden Block-Vermerk an alle ursprünglichen Empfänger zugestellt.

1.4 Analyse von Web-Links

Der Service NetUSE Threat Emulation E-Mail analysiert E-Mails mit im E-Mail-Body enthaltenen direkten URLs (Uniform Resource Locator) mit der Zugriffsmethode HTTP bzw. HTTPS wie folgt:

1.4.1 erkannte URLs werden dahingehend analysiert, ob es sich um einen direkten Link handelt, also die URL direkt auf eine Datei (mit einer Dateiendung) zeigt,

1.4.2 E-Mails ohne direkte URLs werden durchgelassen, ebenso E-Mails, deren direkte URLs ausschließlich auf Dateien mit vom Service derzeit nicht emulierbaren bzw. nicht entpackbaren Dateitypen verweisen,

1.4.3 aus Sicht des Service emulierbare Dateien (bzw. ausgepackte Dateien) werden per Hash mit bereits bekannten Attachment Hashes verglichen und die Einstufung (Malware oder keine Malware) und Behandlung entsprechend übertragen,

1.4.4 aus Sicht des Service emulierbare Dateien (bzw. ausgepackte Dateien), die noch unbekannt sind, werden heruntergeladen und emuliert, um sie auf Malware-typisches Verhalten zu analysieren.

1.4.5 Falls einzelne Dateien als potentielle Malware erkannt wurden, wird die komplette E-Mail geblockt, eine Information an die Empfänger erfolgt nicht. Andernfalls wird die die E-Mail durchgelassen.

1.5 Emulationsumgebungen

Eine Emulationsumgebung ist eine Kombination aus einer Betriebssystemversion mit festgelegten Anwendungsversionen für ausgewählte Anwendungen (z.B. Office-Umgebung und PDF-Reader). NetUSE Threat Emulation E-Mail bietet prinzipiell alle vom Hersteller jeweils vorgefertigt bereitgestellten Emulationsumgebungen an. Im Rahmen des Service NetUSE Threat Emulation E-Mail kann der Kunde für die Emulation seiner E-Mail-Attachments hieraus bis zu 4 Emulationsumgebungen auswählen, die seinen Clients am ehesten entsprechen. Änderungen der gewählten Emulationsumgebungen werden nach Aufwand gemäß der NetUSE-Service-Preisliste abgerechnet.

1.6 Threat Extraction (TX)

Die optionale Funktionalität Threat Extraction im Rahmen des Service NetUSE Threat Emulation E-Mail entfernt zusätzlich aktive Inhalte (z.B. auch klickbare Web-Links) aus Attachments von E-Mails. Der Ablauf ist (abweichend von der reinen Analyse von Attachments gemäß 1.3) dabei wie folgt:

1.6.1 vom Service jeweils aktuell unterstützte Archivformate werden (bei geschachtelten Archiven aktuell bis zu einer Tiefe von 7) ausgepackt,

1.6.2 aus Sicht des Service nicht emulierbare bzw. nicht entpackbare Attachments werden durchgelassen,

1.6.3 aus Sicht des Service emulierbare Attachments (bzw. ausgepackte Dateien) werden per Hash mit bereits bekannten Attachment Hashes verglichen und die Einstufung (Malware oder keine Malware) und Behandlung entsprechend übertragen,

1.6.4 die Attachments mit vom Service jeweils aktuell bzgl. TX unterstützten Dokumentenformaten werden entsprechend einer der beiden folgenden Varianten inhaltlich bearbeitet, sofern sie aktive Inhalte enthalten. Dokumente ohne aktive Inhalte werden nicht verändert.

1.6.4.1. PDF Print
Die Attachments mit vom Service jeweils aktuell bzgl. TX unterstützten Dokumentenformaten werden komplett in ein PDF-Dokument ohne aktive Inhalte überführt.

1.6.4.2. Selektive Entfernung aktiver Inhalte
Bei den Attachments mit vom Service jeweils aktuell bzgl. TX unterstützten Dokumentenformaten werden alle vom Service als potentiell kritisch eingestuften aktiven Elemente unter Beibehaltung des jeweiligen Dokumenttyps aus dem Dokument entfernt. Falls diese selektive Entfernung aktiver Inhalte bei einem Attachment ausnahmsweise nicht möglich ist, wird dieses automatisch gemäß PDF Print (siehe 1.6.4.1) behandelt.

Und die bearbeiteten Dokumente werden mit der ursprünglichen E-Mail direkt an die ursprünglichen Empfänger weitergeleitet. Der Dateiname der via TX gereinigten Attachments an der zugestellten E-Mail wird um einen Reinigungsvermerk ergänzt.

1.6.5 aus Sicht des Service emulierbare Attachments (bzw. ausgepackte Dateien), die noch unbekannt sind, werden emuliert, um sie auf Malware-typisches Verhalten zu analysieren. Dies erfolgt sowohl für von TX aktuelle unterstützte als auch nicht unterstützte Dokumentenformate.

1.6.6 Als potentielle Malware erkannte Attachments werden geblockt, andernfalls werden die Attachments mit der jeweiligen E-Mail durchgelassen (sofern sie nicht zuvor bereits in ihrer via TX bearbeiteten Form weitergeleitet wurden) bzw. in einem Downloadbereich für alle Empfänger der E-Mail zur Verfügung gestellt (sofern sie bereits zuvor in ihrer via TX bearbeiteten Form weitergeleitet wurden). Im Falle von Archiven mit mehreren Dateien werden die kompletten Archive geblockt, sofern eine Datei in dem Archiv als potentielle Malware erkannt wurde. Auch bei geblockten Attachments (bzw. Archiven) werden die zugehörigen E-Mails mit einem entsprechenden Block-Vermerk an alle ursprünglichen Empfänger zugestellt, im Falle von per TX bearbeiteten Attachments enthält die E-Mail zusätzlichen einen Web-Link für den Download des Original-Attachments.

Die Aktivierung dieser Maßnahme ist optional und muss für alle Mail-Domains des Kunden, für die NetUSE Threat Emulation E-Mail genutzt wird, gemeinsam und mit derselben Variante (gemäß 1.6.4) erfolgen.

1.7 Threat Extraction Whitelisting/Blacklisting

Bei der Aktivierung von TX kann der Kunde wählen zwischen

1.7.1 Whitelisting

Es werden prinzipiell alle eingehenden E-Mails gemäß TX behandelt. Optional kann eine vom Kunden definierte TX-Whitelist erstellt werden, in der Absender-Domains (*@domain.tld) oder -Adressen (user@domain.tld) und/oder Empfänger-Domains oder -Adressen benannt werden, für deren E-Mails keine Behandlung gemäß TX erfolgen soll. Eine Kombination von Absender und Empfänger in einem Whitelist-Eintrag ist nicht möglich, sondern es werden bei Nutzung eines Whitelist-Eintrages generell alle E-Mails von einem Absender oder an einen Empfänger von der Behandlung gemäß TX ausgenommen.

1.7.2 Blacklisting

Es werden trotz Aktivierung der Option TX prinzipiell keinerlei eingehenden E-Mails gemäß TX behandelt, solange die Blacklist keine Einträge enthält. Optional kann eine vom Kunden definierte TX-Blacklist erstellt werden, in der Absender-Domains (*@domain.tld) oder -Adressen (user@domain.tld) und/oder Empfänger-Domains oder -Adressen benannt werden, für deren E-Mails eine Behandlung gemäß TX erfolgen soll. Eine Kombination von Absender und Empfänger in einem Blacklist-Eintrag ist nicht möglich, sondern es werden bei Nutzung eines Blacklist-Eintrages generell alle E-Mails von einem Absender oder an einen Empfänger der Behandlung gemäß TX zugeführt.

Nachträgliche Änderungen dieses generellen Verhaltens sowie der Inhalte von TX-White- oder TX-Blacklist werden nach Aufwand gemäß der NetUSE-Service-Preisliste abgerechnet.

1.8 Threat Extraction Download-Portal

Falls im Rahmen von TX Attachments verändert werden, werden die Originaldokumente nach erfolgter Emulation, sofern sie dabei nicht als potentielle Malware erkannt wurden, auf einem Webportal allen Empfängern der E-Mail zum Download bereitgestellt. Der Zugriff erfolgt per HTTPS (Hypertext Transfer Protocol Secure) verschlüsselt und kann nur über einen in der Original-E-Mail eingefügten (je Empfänger eindeutigen) Web-Link erfolgen. Der Benutzer kann das Originaldokument erst herunterladen, wenn dieses durch die Threat Emulation geprüft wurde. Dieses wird in dem über den Link erreichbaren Downloadbereich für das Dokuments angezeigt. Der Download eines Dokuments ist für jeden Empfänger nur für 7 Tage nach dem ersten angestoßenen Download über seinen (personalisierten) Link möglich.

Die für den Download bereitgestellten Originaldokumente werden in einem Verzeichnis auf einem System der NetUSE AG gespeichert. Der Kunde wird hiermit informiert, dass dort evtl. vertrauliche Daten liegen können. Eine Weitergabe an Dritte erfolgt grundsätzlich nur nach Rücksprache mit dem Kunden. Die NetUSE AG behält sich vor, Dateien in diesem Verzeichnis nach vier Wochen zu löschen. Der Kunde kann innerhalb dieser Frist die Bereitstellung der Dateien gegen Berechnung nach Aufwand gemäß der NetUSE-Service-Preisliste anfordern, sofern er sie nicht selbst über den in der Original-E-Mail bereitgestellten Link herunterladen möchte.

Optional kann der Zugriff auf das von der NetUSE AG für den Kunden bereitgestellte Download-Portal auf vom Kunden benannte ausgewählte Quell-IP-Adressen bzw. -Netze eingeschränkt werden.

1.9 Rahmenparameter

NetUSE Threat Emulation E-Mail kann nur für ganze Mail-Domains oder Subdomains des Kunden realisiert werden; eine selektive Abschaltung dieses Dienstes auf der Basis von Usern bzw. E-Mail-Adressen ist nicht möglich. Die Analyse der Attachments erfolgt ausschließlich für aus Sicht des Kunden eingehende E-Mails. Alle Konfigurationsoptionen gelten einheitlich für alle Mail-Domains des Kunden.

1.10 Verzögerung der Mailzustellung

NetUSE Threat Emulation E-Mail arbeitet mit sogenannten Mail-Queues, die die E-Mails annehmen und in der Regel sofort ggf. aber zeitverzögert weiterleiten. Dabei kann diese Zeitverzögerung von wenigen Sekunden bis hin zu mehreren Tagen variieren, wenn das System z.B. durch Spam-Wellen stark belastet wird.

Zum Schutz des Kunden werden E-Mails während der Emulation ihrer Anhänge von NetUSE Threat Emulation E-Mail gequeued. Die sich daraus bei der Mailzustellung ergebende Verzögerung beträgt typischerweise etwa 5 Minuten. Falls zusätzlich die optionale Funktionalität Threat Extraction eingesetzt wird, werden die E-Mails jedoch bereits unverzüglich nach Entfernung der aktiven Inhalte aus den Attachments weitergeleitet. Die sich daraus bei der Mailzustellung ergebende Verzögerung beträgt typischerweise weniger als 1 Minute. Eine zeitverzögerte Zustellung ist kein Mangel.

Für den Fall einer außergewöhnlich hohen Lastsituation auf den Emulationsumgebungen behält sich die NetUSE AG das Recht vor, die Emulation für weitere eingehende E-Mails zu unterbrechen und die E-Mails ohne vorherige Analyse durch NetUSE Threat Emulation E-Mail an den Kunden weiterzuleiten, um eine zügigere E-Mailzustellung sicherzustellen.

1.11 Veränderung von Mailinhalten

Der Vorgang der Untersuchung oder Reinigung von Daten durch NetUSE Threat Emulation E-Mail kann zur Veränderung von Inhalten führen, zum Beispiel durch Anhängen eines Prüf- oder Reinigungsvermerks oder im Falle von Threat Extraction durch Einfügen eines Web-Links zum Download des unveränderten Original-Attachments. Dies kann in der Folge auch dazu führen, dass eine bereits vorhandene Signatur der E-Mail ungültig wird. Der Kunde erklärt hierzu sein Einverständnis.

Bei Nutzung der Option Threat Extraction werden zusätzlich die zugestellten Attachments bei den von TX unterstützten Dateiformaten inhaltlich verändert (konkret in PDFs umgewandelt oder von aktiven Inhalten gereinigt). Dabei können Informationen (z.B. Farben, Formatierungen, Bilder) verloren gehen, oder das Dokument lässt sich nicht mehr wie vorgesehen nutzen (z.B. Macros in Tabellenkalkulationen oder Formulare). Der Kunde erklärt hierzu sein Einverständnis. Dass es durch inhaltliche Veränderungen zu Veränderungen der Aussagekraft der E-Mail kommen könnte, kann nicht ausgeschlossen werden; dieser Umstand ist der NetUSE AG bislang nicht bekannt geworden. Sollten solche Umstände eintreten, hat der Kunde die NetUSE AG darüber umgehend in Kenntnis zu setzen.

1.12 Threat Emulation Quarantäne

Von NetUSE Threat Emulation E-Mail als potentielle Malware klassifizierte Attachments (und komplette Archiv-Attachments, die einzelne als potentielle Malware klassifizierte Dateien enthalten) werden in ein Quarantäne-Verzeichnis auf einem System der NetUSE AG verschoben. Der Kunde wird hiermit informiert, dass dort evtl. vertrauliche Daten liegen können. Eine Weitergabe an Dritte zur Untersuchung auf Malware erfolgt grundsätzlich nur nach Rücksprache mit dem Kunden. Die NetUSE AG behält sich vor, Dateien im Quarantäne-Verzeichnis nach einer Woche zu löschen. Der Kunde kann innerhalb dieser Frist die Bereitstellung der Dateien gegen Berechnung nach Aufwand gemäß der NetUSE-Service-Preisliste anfordern.

1.13 Verschlüsselte Daten

Eine Überprüfung von Daten, die mittels Ende-zu-Ende-verschlüsselter E-Mail übertragen werden, kann durch NetUSE Threat Emulation E-Mail nicht stattfinden, da diese Daten aufgrund der Verschlüsselung für NetUSE Threat Emulation E-Mail nicht lesbar sind. Ebenso können verschlüsselte Attachments an unverschlüsselt übertragenen E-Mails nicht analysiert werden.

1.14 Leistungsgrenzen von NetUSE Threat Emulation E-Mail

1.14.1 Leistungsgrenzen Threat Emulation

Die Emulation von Attachments hat das Ziel, auffälliges Verhalten von ausgewählten emulierbaren Attachments zu erkennen. Dies ist insofern reaktiv, als dass nur auffälliges Verhalten bzgl. bekannter möglicher Angriffswege auf das Betriebssystem bzw. die Anwendungen untersucht wird. Dadurch können nicht alle potentiell gefährlichen Attachment-Typen emuliert und analysiert werden, sondern nur die vom Service unterstützten. Ebenfalls werden nur ausgewählte Emulationsumgebungen (typische Kombinationen aus Betriebssystemversion und Anwendungsversionen) verwendet und nicht alle theoretisch möglichen Kombinationen.

1.14.2 Leistungsgrenzen Analyse von Web-Links

Um die Zustellung von E-Mails nicht übermäßig zu verzögern, werden lediglich die ersten 10 erkannten URLs analysiert und bei direkten Links ggf. dahinterliegende Dateien heruntergeladen und emuliert.

1.14.3 Leistungsgrenzen Threat Extraction

Bei Verwendung der Variante der selektiven Entfernung aktiver Inhalte im Rahmen von Threat Extraction werden lediglich die vom Service als potentiell kritisch eingestuften aktiven Elemente entfernt, um eine möglichst hohe Kompatibilität des gereinigten Dokumentes mit dem Orîginaldokument zu erhalten. Dies ist in sofern reaktiv, als dass nur aktive Elemente mit bekannten möglichen Angriffswegen entfernt werden. Dadurch werden nicht alle potentiell gefährlichen aktiven Elemente entfernt, sondern nur die vom Service unterstützen. Ebenso hindert das gereinigte oder konvertierte Dokument den Empfänger nicht daran, auf einen inhaltlichen Angriff hereinzufallen. D.h. auch bei einem gereinigten Dokument kann der Empfänger z.B. einen (nicht mehr aktiven) Link herauskopieren oder abschreiben und manuell in den Browser übertragen und dort ausführen. Ebenso kann über den Download der Originaldokumente durch den Empfänger eine Infektion erfolgen.

Das bedeutet, dass auch mit NetUSE Threat Emulation E-Mail die Infektion mit Malware nicht komplett ausgeschlossen werden kann.

1.15 Reporting

Der Kunde hat für seine Mail-Domains Zugriff auf eine statistische Auswertung der Ergebnisse (Reports) von NetUSE Threat Emulation E-Mail.

1.16 Abrechnungsverfahren

Die Abrechnung des Services NetUSE Threat Emulation E-Mail erfolgt in Form einer Grundgebühr sowie einer nutzungsabhängigen Gebühr, die anhand der Anzahl der emulierten Attachments bzw. Dateien ermittelt wird.

1.16.1 Grundgebühr

Die Grundgebühr wird unabhängig von der realen Nutzung des Dienstes für die Bereitstellung der Infrastruktur und Basislizenzen fällig. Dabei hält die NetUSE AG im Rahmen der Grundgebühr je nach gewählter Größen-Kategorie (bzgl. emulierter Attachments pro Monat) eine angemessene Menge von Ressourcen für die Emulation von Attachments bzw. Dateien vor. Ab Erreichen des zweifachen Wertes der zu einer Größen-Kategorie empfohlenen Maximalmenge von emulierten Attachments bzw. Dateien behält sich die NetUSE AG vor, alle weiteren E-Mails des Kunden über ein Überlast-System zu routen; dies kann zu erhöhten Wartezeiten für eine Emulation und damit zu längeren Mail-Verzögerungen führen.

1.16.2 Abrechnung anhand der Zahl emulierter Attachments

Grundlage für die Abrechnung ist die Anzahl der innerhalb eines Monats von NetUSE Threat Emulation E-Mail tatsächlich emulierten Attachments bzw. Dateien. Dabei wird bei emulierbaren Dateien in einem Archiv, das an einer E-Mail als Attachment hängt, jede emulierte Datei einzeln gezählt. Die Anzahl wird auf 1 Attachment (bzw. Datei) genau ermittelt und, sofern nichts Anderes vereinbart ist, nach angefangenen 1000 emulierten Attachments abgerechnet.

1.17 E-Mail-Größenbeschränkung

Bei NetUSE Threat Emulation E-Mail können über die Mailrelay-Gateways der NetUSE AG E-Mails bis zu einer Größe von 2 GB (1 GB $=10^9$ Bytes) versendet bzw. empfangen werden. Es werden ausschließlich emulierbare Attachments bzw. Dateien bis zu einer maximalen Dateigröße von 15 MB (1 MB $=10^6$ Bytes) emuliert bzw. optional mit TX bearbeitet; größere Dateien werden ohne Emulation und Bearbeitung durch TX weitergeleitet.

1.18 E-Mail-Aufbewahrung

Die NetUSE AG kann für die Speicherung von E-Mail, die die NetUSE AG dem Kunden nicht binnen eines Zeitraums von 8 Stunden zustellen kann, keine Garantie übernehmen. Sofern der Speicherplatzbedarf im Einzelfall ein zumutbares Maß überschreitet, behält sich die NetUSE AG vor, die weiteren für einen Kunden eingehenden Nachrichten abzulehnen.

Falls der Kunde für die entsprechenden Mail-Domains einen Vertrag über NetUSE Mailrelay hat, gelten die dort vereinbarten deutlich längeren Aufbewahrungsfristen.

1.19 Delivery Status Notification Messages (Bounces)

Delivery Status Notification Messages (auch bezeichnet als Postmaster/Mailerdaemon-E-Mails bzw. Error-Bounces), d.h. E-Mails mit den Absendern <> oder MAILER-DAEMON im Envelope-FROM, können bereits nach 4 Stunden (Verweilzeit auf NetUSE-Systemen) gelöscht werden, sofern mindestens ein Zustellversuch fehlgeschlagen ist.

1.20 Fehlercodes bei eingehendem Mailrelay

Liefert ein Mailserver des Kunden bei einem Zustellversuch durch NetUSE-Mailserver bei (aus Sicht des Kunden) eingehendem Mailrelay einen temporären Fehlercode (dies betrifft alle 4er Codes), dann hat die NetUSE AG das Recht, diese gegenüber dem Absender der E-Mail auf einen 5er Code (permanenter Fehler) umzuschreiben.

1.21 Konfigurationssupport

Die Konfiguration von Mailservern, Routern oder Endgeräten auf Seiten des Kunden ist im Preis nicht enthalten und wird ebenso wie ggf. vom Kunden gewünschter Support im Rahmen der Inbetriebnahme oder nachträglich gewünschte Konfigurationsänderungen nach Aufwand gemäß der NetUSE-Service-Preisliste abgerechnet.

1.22 Lizenzvorschriften

Die NetUSE AG verwendet zur Erbringung der oben angeführten und zwischen den Parteien vereinbarten Dienstleistung Produkte der Firma Check Point.

Die Berechtigung zur Verwendung dieser Produkte beruht seinerseits auf der Grundlage eines zwischen der NetUSE AG und der Firma Check Point geschlossenen Lizenzvertrages. Für die Nutzung von Check Point Produkten sind entsprechende Herstellerverwendungsvorgaben von der NetUSE AG als auch von deren Kunden zu beachten und einzuhalten; auf die Einhaltung dieser Verpflichtungen wird hingewiesen und diese nachfolgend angeführt:

1.22.1 Die durch die NetUSE AG verwendeten Produkte der Firma Check Point stehen dieser aufgrund einer Einzelnutzungserlaubnis zur Verfügung; dieser Einzelnutzungscharakter soll sich auch in der vorliegenden Vereinbarung widerspiegeln. Demnach kann die hier zwischen den Parteien vereinbarte Serviceleistung nicht selbständig durch den Kunden ohne vorhergehende schriftliche Vereinbarung und Zustimmung durch die NetUSE AG an Dritte übertragen bzw. von diesen genutzt werden.

1.22.2 Der Kunde hat so weit möglich dafür Sorge zu tragen, dass ausreichende Sicherheitsmaßnahmen vorhanden sind und auch laufend unterhalten werden, dass die Produkte der Firma Check Point vor Diebstahl und unberechtigten Zugriffen geschützt sind.

1.22.3 Der Kunde verpflichtet sich, die vorliegenden vertraglichen Vereinbarungen vertraulich zu behandeln und keiner unberechtigten dritten Partei Einblick in diese zu gewähren. Der Kunde macht seinen Angestellten und Kunden nur solche vertraglichen Informationen bekannt, die auf der Basis des need-to-know erforderlich sind. Weiter verpflichtet sich der Kunde, über sämtliche Erkenntnisse und Informationen, die er im Zusammenhang mit der Verwendung der Produkte der Firma Check Point erlangt oder ihm seitens der NetUSE AG zugetragen werden, grundsätzlich Stillschweigen gegenüber Dritten zu bewahren.

1.22.4 Der Kunde wird ausdrücklich darauf hingewiesen, jedwede Verhaltensweise zu unterlassen, die darauf abzielen könnte, die verwendeten Produkte der Firma Check Point abzuändern, zurückzuübersetzen, zu verändern, zu zerlegen/demontieren, zu kopieren oder das Produkt oder irgendeinen Teil davon nachzubauen, ohne zuvor die schriftliche Zustimmung der NetUSE AG und der Firma Check Point eingeholt zu haben.

1.22.5 Der Kunde verpflichtet sich, die geltenden gesetzlichen und rechtlichen Bestimmungen, die im Zusammenhang mit der Nutzung der vereinbarten Serviceleistung stehen, zu beachten und einzuhalten.

1.22.6 Die NetUSE AG weist ausdrücklich darauf hin, dass die Firma Check Point ihre Produkte stetig weiterentwickelt. Im Rahmen dieses Produktweiterentwicklungsprozesses kann es erforderlich sein, dass die Firma Check Point bestimmte Funktionen ihres Produktes und dessen Funktionsabläufe bei der NetUSE AG automatisch analysiert und verändert. Zu diesem Zweck kann die Firma Check Point auf die Systeme der NetUSE AG, auf denen deren Produkte installiert sind, Einblick nehmen und deren Betriebsumgebung kontrollieren. Dabei kann es seitens der NetUSE AG nicht ausgeschlossen werden, dass die Firma Check Point in mittelbare Berührung mit Informationen des Kunden kommen kann; eine inhaltliche Kontrolle dieser Informationen findet nicht statt.

Dazu stimmt der Kunde der NetUSE AG bereits jetzt die Verwendung eines sog. Aktualisierungskontrolleurs seitens der Firma Check Point zu; die dabei gesammelten Informationen dürfen durch den Hersteller nur zur Produktoptimierung verwandt werden.

1.22.7 Die NetUSE AG weist ergänzend darauf hin, dass seitens des Herstellers keine zusätzlichen Funktionsgarantien für das vom Kunden gewählte und verwendete Produkt und dessen Anwendung gegeben werden.

Die NetUSE AG weist ergänzend darauf hin, dass vorliegend die aktuellen Garantie- und Haftungsbestimmungen der Firma Check Point als vereinbart gelten. Diese können in der Endbenutzervereinbarung eingesehen werden unter:
https://www.checkpoint.com/support-services/software-license-agreement-limited-hardware-warranty/

Außer der Standard-Produkt-Garantie gewährt Check Point keine zusätzlichen Garantien auf seine Produkte.

Die NetUSE AG gibt im Hinblick auf die Herstellerprodukte keine zusätzlichen Garantien, Zusagen bzw. Versprechen oder Entschädigungsversprechen in Bezug auf die Verwendbarkeit der Herstellerprodukte ab.

2. Mitwirkungspflichten des Kunden

2.1 Datenschutz

Im Rahmen der von der NetUSE AG betriebenen Lösung kommt es zur Verarbeitung (siehe Art. 4 Nr. 2 DS-GVO) von personenbezogenen Daten des Kunden und Dritter (E-Mail-Adressen des Kunden, an die E-Mails gesendet werden; E-Mail-Adressen, die E-Mails an den Kunden senden) durch die NetUSE AG.

Der Kunde hat insbesondere vor dem Hintergrund, dass durch die betriebene Lösung auch Inhalte von E-Mails verarbeitet werden können, innerbetrieblich sicherzustellen, dass seine Mitarbeiter und betriebliche Mitbestimmungsbeteiligte über diese Verarbeitung informiert werden.

Die Rechtmäßigkeit der Verarbeitung ergibt sich für die NetUSE AG nach Art. 6 I lit. b DS-GVO.

Der Kunde bleibt dabei Verantwortlicher in Sinne der DS-GVO. Die NetUSE AG nimmt die Verarbeitung weisungsgebunden vor.

2.2 Mail-Domains des Kunden
Der Service NetUSE Threat Emulation E-Mail kann nur für im Voraus festgelegte Mail-Domains des Kunden genutzt werden. Dementsprechend muss der Kunde der NetUSE AG bei Beauftragung alle Mail-Domains benennen, für die er den Dienst nutzen möchte. Eine nachträgliche Änderung der Liste der geschützten Maildomains wird nach Aufwand gemäß der jeweils gültigen NetUSE-Service-Preisliste abgerechnet.

2.3 Threat Extraction
Als Standardeinstellung wird die optionale Funktion TX im Rahmen des Service NetUSE Threat Emulation E-Mail deaktiviert. Sofern die optionale Funktionalität TX aktiviert werden soll, muss der Kunde dies der NetUSE AG bei Beauftragung melden. Eine nachträgliche Änderung wird nach Aufwand gemäß der jeweils gültigen NetUSE-Service-Preisliste umgesetzt.
Bei Aktivierung von TX sind vom Kunden zusätzlich folgende Informationen beizustellen:

2.3.1 Threat Extraction Variante
Bei der Aktivierung von TX kann der Kunde wählen zwischen den Varianten „PDF Print" und „selektive Entfernung aktiver Inhalte" (gemäß 1.5.4). Dementsprechend muss der Kunde der NetUSE AG bei Beauftragung die gewünschte Variante für seine Mail-Domains benennen. Sofern dies nicht erfolgt, wird bei der Einrichtung die Variante „selektive Entfernung aktiver Inhalte" aktiviert. Eine nachträgliche Änderung der TX Variante wird nach Aufwand gemäß der jeweils gültigen NetUSE-Service-Preisliste abgerechnet.

2.3.2 Threat Extraction Whitelisting/Blacklisting
Bei der Aktivierung von TX kann der Kunde wählen zwischen generellem Blacklisting und generellem Whitelisting (gemäß 1.6). Dementsprechend muss der Kunde der NetUSE AG bei Beauftragung das gewünschte Verfahren benennen sowie alle bei Inbetriebnahme einzurichtenden Blacklist- bzw. Whitelisteinträge. Sofern dies nicht erfolgt, wird bei der Einrichtung generelles Blacklisting ohne Blacklist-Einträge konfiguriert. Eine nachträgliche Änderung des Verhaltens sowie der White- bzw. Blacklist-Einträge wird nach Aufwand gemäß der jeweils gültigen NetUSE-Service-Preisliste abgerechnet.

2.3.3 Zugriffsbeschränkung für Download-Portal
Optional kann der Zugriff auf das von der NetUSE AG für den Kunden bereitgestellte Download-Portal auf vom Kunden benannte ausgewählte Quell-IP-Adressen bzw. -Netze eingeschränkt werden. Sofern der Kunde dies nutzen möchte, muss er der NetUSE AG bei der Beauftragung dies melden sowie die freizuschaltenden Quell-IP-Adressen bzw. -Netze benennen. Sofern dies nicht erfolgt, wird bei der Einrichtung ein Zugriff für beliebige Quell-IP-Adressen freigeschaltet. Eine nachträgliche Änderung des Verhaltens sowie der Liste der freigeschalteten IP-Adressen bzw. -Netze wird nach Aufwand gemäß der jeweils gültigen NetUSE-Service-Preisliste abgerechnet.

2.4 E-Mail-Routing
Für die Integration von NetUSE Threat Emulation E-Mail in den aus Sicht des Kunden eingehenden E-Mail-Datenverkehr ist der Kunde verantwortlich. Sofern der Kunde nicht NetUSE Mailrelay für die entsprechenden Mail-Domains beauftragt hat, muss er der NetUSE AG bei der Beauftragung folgende Informationen benennen:

- bis zu 5 IP-Adressen der einliefernden Mailserver des Kunden für die Übergabe von zu analysierenden E-Mails an die NetUSE AG
- bis zu 5 IP-Adressen oder Hostnamen der annehmenden Mailserver des Kunden für die Übergabe bereits von NetUSE Threat Emulation E-Mail analysierter E-Mails an den Kunden

2.5 Absicherung der Mailboxserver
Um die Funktion von NetUSE Threat Emulation E-Mail zu gewährleisten, ist es erforderlich, dass der gesamte zu scannende E-Mail-Datenverkehr (eingehend aus Sicht des Kunden) über die von der NetUSE AG vorgegebenen Systeme geroutet wird und dass direkte Verbindungen zu Mailboxservern des Kunden aus dem Internet durch Access-Listen oder Firewallregeln unterbunden werden. Diese Konfiguration erfolgt kundenseitig und ist nicht Bestandteil dieses Services.

2.6 Empfängercheck
Falls der Kunde für die betreffenden Mail-Domains nicht NetUSE Mailrelay beauftragt hat, hat er sicherzustellen, dass seine Mailserver, an die NetUSE Threat Emulation E-Mail E-Mails zustellen soll, auch alle E-Mails annehmen, die vom Kunden zuvor an NetUSE Threat Emulation E-Mail übergeben wurden. Wenn also ein Empfängercheck bei der Annahme von E-Mails beim Kunden implementiert ist, so ist er vom Kunden vor der Übergabe von E-Mails an NetUSE Threat Emulation E-Mail durchzuführen.

3. Verfahren bei Störungen
Die NetUSE AG leistet innerhalb der Geschäftszeiten (Montag bis Freitag von 8:00 bis 18:00 Uhr; ausgenommen gesetzliche Feiertage) kostenlosen Telefonservice, sofern die Störungen durch die NetUSE AG zu verantworten sind. Stellt sich im Laufe der Bearbeitung heraus, dass die Störungsursache nicht von der NetUSE AG zu verantworten ist, so wird die NetUSE AG dem Kunden die Bearbeitung in Rechnung stellen. Die Berechnung erfolgt dabei nach Aufwand gemäß der jeweils gültigen NetUSE-Service-Preisliste.

4. Spezielle Leistungsbeschreibung, allgemeine Leistungsbeschreibung und AGB
Bei Vertragsschluss oder spätestens bei Nutzung des Dienstes NetUSE Threat Emulation E-Mail werden folgende Bestimmungen in angegebener Reihenfolge Vertragsbestandteil: der Vertrag, die Bestimmungen dieser speziellen Leistungsbeschreibung, die allgemeine Leistungsbeschreibung für NetUSE IP-Dienstleistungen, die NetUSE-Service-Preisliste und die Allgemeinen Geschäftsbedingungen der NetUSE AG.