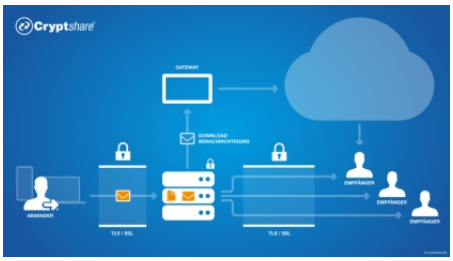
Datentransfer ohne Grenzen

Dr. Götz Güttich

Mit seiner gleichnamigen Lösung hat der deutsche Anbieter Cryptshare ein Produkt zum verschlüsselten Dateiversand im Angebot. Dieses kommt ohne Beschränkungen bei der Dateigröße aus, sorgt für Nachvollziehbarkeit, lässt sich mit beliebigen Kommunikationspartnern ad hoc nutzen und bietet eine Vielzahl weiterer Funktionen. Wir haben uns im Testlabor angeschaut, wie die Arbeit damit abläuft und was die Lösung im praktischen Alltag leisten kann.

Cryptshare kommt in der zum Testzeitpunkt aktuellen Version 4.4 als Server, der als Software on-site oder beim ausgewählten Hosting-Anbieter als virtuelle beziehungsweise Hardware-Appliance betrieben werden kann. Alternativ ist Cryptshare auch als Software as a Service (beim Hersteller selbst) oder in der Private Cloud (im Microsoft Azure Marketplace) erhältlich. Diese Serverlösung speichert die zu versendenden Daten lokal verschlüsselt (dabei wird für jede Kommunikation ein anderer Schlüssel verwendet) und schickt E-Mail-Benachrichtigungen an die Empfänger, die einen Link enthalten, über den sich die Informationen dann über gesicherte Verbindungen herunterladen lassen. Um für Sicherheit zu sorgen, können die Mitarbeiter die einzelnen Dateiübertragungen mit Passwörtern schützen, neben den Mail-Inhalten und den Anhängen auch den Betreff der Nachrichten verschlüsseln und die Gültigkeit der Download-Links, sowie die Aufbewahrungsdauer der Dateien zeitlich beschränken.

Umfassende Nachvollziehbarkeitsfunktionen sorgen für Compliance, die Behandlung der einzelnen Übertragungen wird über Policies geregelt und APIs und



Die Funktionsweise von Cryptshare

Automatisierungsfunktionen sorgen im Betrieb für die nahtlose Integration des Produkts ins Unternehmensumfeld. Auch das Look and Feel der Lösung lässt sich umfassend anpassen. Ein MS Outlook-Add-In, mit dem die Anwender Cryptshare direkt aus dem Mail-Client von Microsoft heraus bedienen, schließt zusammen mit einer HCL Notes-Integration und der QUICK Technology (Quick Use Integrated Cryptshare Key) den Leistungsumfang von Cryptshare 4.4 ab.

Die genannte QUICK-Technologie lässt sich nutzen, um die Passwörter, die zur Verschlüsselung der Datenübertragungen zwischen Kommunikationspartnern zum Einsatz kommen, zu verwalten und die Datentransfers abzusichern. Das bedeutet, mit aktivierter QUICK-Funktion sorgt Cryptshare für die automatische Erzeugung aller Passwörter für die Dateiübertragungen und die Anwender müssen sich mit der Passwortverwaltung – und dem Handling nicht weiter auseinandersetzen, sondern können die Files einfach ganz normal, wie bei bekannten S/MIME-Lösungen, permanent sicher austauschen, ohne dabei jedes Mal ein neues Passwort zu vergeben.

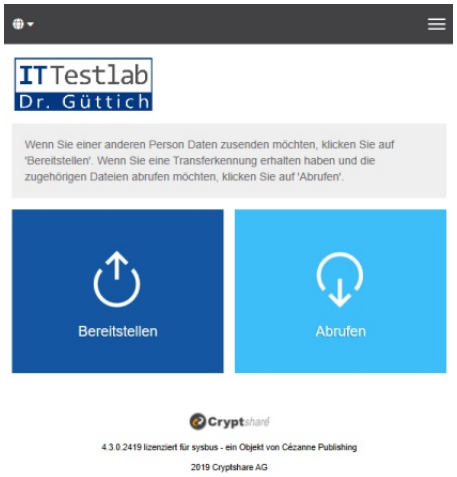
Der Test

Im Test setzten wir bei uns im Testlabor einen Cryptshare-Server auf Basis einer virtuellen Maschine auf. Dieser verwendete dann im Betrieb unseren Exchange 2016-Mail-Server als Relay, um Mails mit unseren Test-Konten auszutauschen. Nach der Erstkonfiguration und Inbetriebnahme des Systems versendeten wir zunächst einmal diverse Dateien an unterschiedliche Konten und prüften, wie die normale Arbeit mit dem Produkt abläuft. Danach setzten wir uns dann mit dem Outlook-Add-In, der QUICK-Technologie, den Optionen zum Anpassen der Benutzeroberfläche und der Nutzung des Systems von mobilen Endgeräten aus auseinander.

Installation als virtuelle Maschine

Für den Test stellte uns Cryptshare zunächst einmal eine Li-

zenzdatei zur Verfügung, die den Cryptshare-Dienst für die von uns verwendeten Domänen freischaltete. Nachdem wir diese Datei erhalten hatten, wechselten



So empfängt das Cryptshare-Web-Interface die Benutzer

wir auf die Webseite https://www.cryptshare.com/de/support/vm-build-service und machten uns daran, die für uns angepasste virtuelle Appliance erstellen zu lassen. Dazu fragte uns der Build-Service zunächst nach dem Typ der virtuellen Maschine (VM). Dabei bietet das System Vmware- und Hyper-V-Maschinen an. Beim Einsatz von Hyper-V muss man sich allerdings über ein Kontaktformular an den Hersteller wenden, nur die Erstellung von Vmware-VMs läuft automatisch ab. Dementsprechend entschieden wir uns zu diesem Zeitpunkt für eine VM für Vmware-Umgebungen.

Anschließend fragte uns der Assistent nach Namen, Telefonnummer und E-Mail-Adresse und wollte, dass wir unsere Lizenzdatei ins Web-Interface hochluden, damit sie direkt in die VM integriert werden konnte. Hat ein Interessent zu diesem Zeitpunkt noch keine Lizenz, so kann er die VM übrigens trotzdem erstellen und die Lizenz später selbst über das Konfigurationswerkzeug des Servers einspielen.

Im nächsten Schritt wollte der Wizard wissen, wie die Absenderadresse für den Mail-Versand von E-Mail-Nachrichten und die Administratoradresse für den Empfang der Systemmeldungen lauten. Zum Schluss ging es an die Netzwerkkonfiguration mit IP-Adresse, Subnetz, Gateway, Hostname, den zu verwendenden DNS-Servern, der Domänensuchliste und dem E-Mail-Gateway. Sobald diese Angaben gemacht wurden, erstellt der Wizard die VM mit den gewünschten Parametern (die sich bei Bedarf im laufenden Betrieb jederzeit ändern lassen) und schickt den Kunden nach wenigen Minuten eine E-Mail mit einem Cryptshare-Link zu, über den sie die fertige VM herunterladen können.

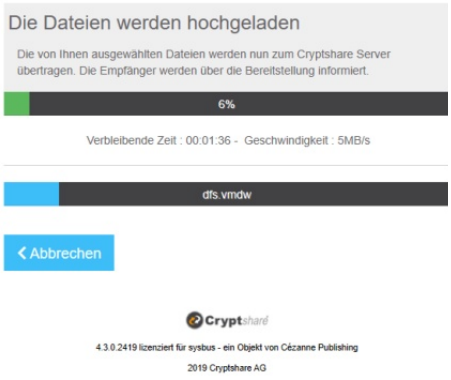
Die VM kommt in Form einer OVF-Datei mit einer knapp zwei GByte großen virtuellen Festplatte im VMDK-Format. Diese beiden Files ließen sich im Anschluss problemlos in einen unserer ESXi-Hypervisoren mit der Version 6.7 Update 3 importieren.

Erstkonfiguration und Inbetriebnahme

Nachdem wir den Import der VM abgeschlossen hatten, machten wir uns daran, das System entsprechend der Dokumentation von Cryptshare in Betrieb zu nehmen. Um die Download-Größe der VM in Grenzen zu halten und da jedes Unternehmen unterschiedliche Anforderungen an den Speicherbedarf des Verzeichnisses für die zu übertragenen Dateien hat, enthält die VM nach dem Import keinen Speicherplatz für Datei-Uploads, Backups und so weiter. In der Dokumentation wird darauf hingewiesen, dass es zunächst erforderlich ist, einen solchen Speicher einzurichten. Sie gibt auch Ratschläge, wieviel Speicher für welche Umgebungen erforderlich sein dürfte.

Dementsprechend fügten wir der virtuellen Appliance zu diesem Zeitpunkt zunächst einmal mit Vmware-Bordmitteln eine virtuelle Festplatte hinzu, die genug Speicher für unsere Testumgebung bereitstellte. Die virtuelle VM kommt mit einer als SCSI (0:0)-konfigurierten Festplatte an, wir definierten unsere neue HDD als SCSI (0:1) am gleichen Controller.

Danach fuhren wir die VM, die unter OpenSuse 15.0 lief, hoch und loggten uns als "root" ein.



Der Upload der zu übertragenen Dateien auf den Server

Die Passwörter für den Zugriff auf die VM und das Konfigurationsinterface fanden sich in der Download-ZIP-Datei der VM, genau wie ein Link zur Dokumentation.

Nach dem Login stellten wir fest, dass Linux die ursprüngliche Festplatte als "/dev/sda" eingebunden hatte und dass unsere neue HDD als "/dev/sdb" er-

reichbar war. Im nächsten Schritt riefen wir nun das Skript "/opt/csappliance/attachHDD.sh" auf, das die neue Festplatte partitionierte, formatierte, mit den benötigten Zugriffsrechten versah und ins System einband.

Zum Schluss unserer Vorbereitungen erzeugten wir auf unserer

Im Rahmen des Dateiversands legen die Nutzer auch fest, ob und wie sie darüber informiert werden sollen, wenn eine Datei vom Empfänger heruntergeladen wird

neuen Festplatte noch ein zusätzliches Verzeichnis für temporäre Dateien, fügten den Pfad zu diesem Verzeichnis wie in der Dokumentation beschrieben zu der Konfigurationsdatei "/opt/cryptshare-3/launcher.ini" hinzu und starteten den Cryptshare-Dienst mit der Befehlssequenz "rccryptshare stop" und "rccryptshare start" neu. Damit war die Arbeit an der Konsole abgeschlossen und wir konnten uns dem Konfigurationsinterface der Lösung zuwenden.

Die Einrichtung über das Browser-Interface

Laut Handbuch ergibt es jetzt Sinn, das SSL-Zertifikat für die Verschlüsselung des Zugriffs auf den Server einzuspielen. Da es sich bei unserer Installation um eine Testumgebung handelte, verzichteten wir auf diesen Schritt und verwendeten das mitgelieferte, selbstsignierte Zertifikat. Außerdem sollten die Administratoren laut Dokumentation zu diesem Zeitpunkt ihre Lizenzdatei einspielen. Auch diesen Schritt konnten wir überspringen, da wir ihn ja bereits beim Anlegen der VM durchgeführt hatten.

Der Login beim Konfigurations-Interface erfolgt über die URL https://{Name des Cryptshare-Servers}:8080. Nach dem ersten Login muss der Administrator zunächst einmal das vorgegebene Standardpasswort ändern, sonst erhält er keinen Zugriff auf die Verwaltungsoberfläche. Wir finden das gut, da auf diese Weise vermieden wird, dass irgendwelche Cryptshare-Server mit Standardpasswörtern in Netz arbeiten.

Für die nun folgende Erstkonfiguration des Systems gibt es keinen Wizard im klassischen Sinn, stattdessen weist die Dokumentation darauf hin, in welchen Bereichen unter den "System Einstellungen" manuelle Anpassungen erforderlich sind. In diesem Zusammenhang spielen zunächst einmal die "Verbindungseinstellungen" eine Rolle, die zur Definition der Basis-URL für die Download-Links dienen, die später per E-Mail verschickt werden. Außerdem lassen sich an dieser Stelle auch sichere Verbindungen (via HTTPS) erzwingen und die iFrame-Sicherheit konfigurieren, die festlegt, ob die Möglichkeit besteht, das Cryptshare-Benutzerinterface in andere Webseiten einzubetten.

Unter "Systembenachrichtigungen" legen die Administratoren im Gegensatz dazu fest, welche Schwellenwerte für das Disk Space Monitoring gelten sollen und unter welchen E-Mail-Adressen Administratoren Benachrichtigungen über Warnungen, Fehler und anstehende Updates erhalten. Die "Verifizierung" sorgt dafür, dass das System überprüft, ob die E-Mail-Adresse, die ein Absender beim Anstoßen einer Datenübertragung angibt, auch wirklich zu ihm gehört. Nachdem der Anwender seine E-Mail-Adresse angegeben hat, sendet ihm der Cryptshare-Server einen Verifizierungs-Code zu, den er dann in der Benutzeroberfläche eintragen muss, um seine Mail-Adresse zu bestätigen.

Der Abschluss eines Cryptshare-Transfers

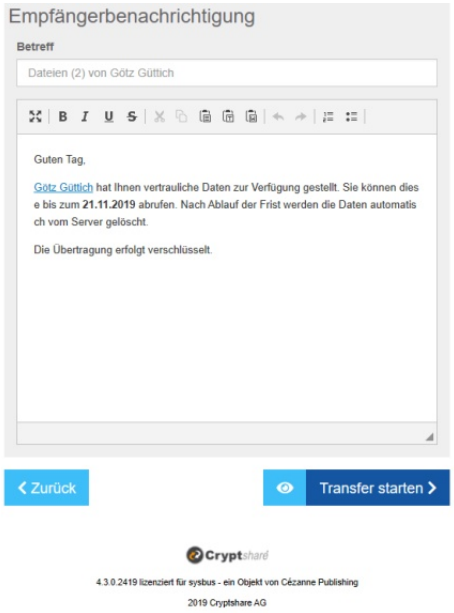
Das Konfigurations-Interface bietet in diesem Zusammenhang die Option, die Gültigkeitsdauer dieser Verifizierungs-Codes festzulegen, die Zahl der Eingaben beziehungsweise Anforderungen für Codes zu beschränken und bestehende Codes zu löschen.

Über die Transfereinstellungen sind die zuständigen Mitarbeiter dazu in der Lage, das Verzeichnis festzulegen, in dem der Server

die zu übertragenden Dateien ablegt. Außerdem lässt sich an gleicher Stelle eine Funktion aktivieren, die Prüfsummen für die Dateien der Transfers erzeugt. Zudem ist es möglich, den Aufbewahrungszeitraum für die Files und – falls gewünscht – ein maximales Transfervolumen festlegen.

Policies als Herzstück des Servers

Jetzt kommen die Policy-Einstellungen an die Reihe. Diese stellen ein Herzstück des Cryptshare-Systems dar und definieren, wer das System wie nutzen darf. Jede Regel besteht aus drei Teilen. Das Absendermuster legt fest, welche Absender (wie etwa alle Mitglieder der Domäne "test-



Die Gültigkeit der Download-Links lässt sich beliebig begrenzen

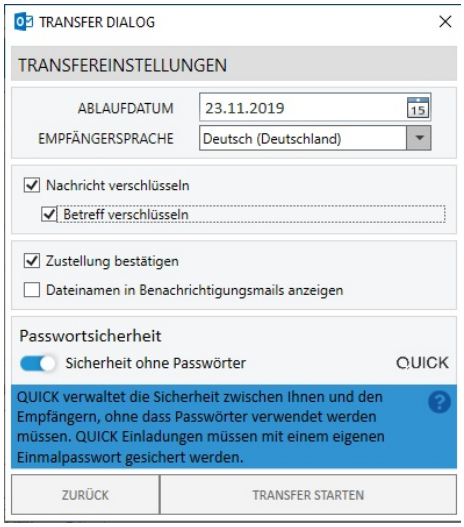
domain.online") einen Datentransfer anstoßen dürfen. Das Empfängermuster definiert im Gegensatz dazu, wer Datenübertragungen erhalten darf und weitere Einstellungen dienen dazu, Einschränkungen und Transfermöglichkeiten festzulegen, die bei der dazugehörigen Absender/Empfänger-Kombination Anwendung finden. Auf diese weiteren Einstellungen gehen wir später noch genauer ein.

Die einzelnen Regeln lassen sich entweder manuell erstellen und bearbeiten oder aus der auf dem Server installierten Lizenz ableiten. Im Test entschieden wir uns zu diesem Zeitpunkt für den letztgenannten Weg und das System erzeugte automatisch Policies, mit denen die Benutzer der von uns lizensierten Domänen Datentransfers an alle Internet-User verschicken konnten und auch dazu in der Lage waren, Daten von allen Internet-Anwendern zu erhalten.

Der letzte Punkt der Schnellstartanleitung befasst sich mit den Einstellungen für den Mail-Server. In diesem Zusammenhang vergeben die Administratoren eine Mail-Adresse und einen Absendernamen, die für den Versand der Mail-Benachrichtigungen zum Einsatz kommen und definieren den SMTP-Host, den SMTP-Port und die SMTP-Authentifizierung. Letztes ist nur auf selbstinstallierten Systemen erforderlich, da die Appliances mit einem eigenen Mail-Server (Postfix) kommen und deshalb hier die Angabe "localhost" ausreicht. Der Postfix-Mail-Server schickt dann die Nachrichten von der Appliance aus an ein Mail-Relay im LAN, in unserem Testlabor kam dazu wie gesagt ein Exchange Server 2016 zum Einsatz, das die Mails dann weiterleitete. Die Konfiguration dieses Mail-Relays erfolgt während der oben beschriebenen Erstellung der VM mit dem Online-Wizard. Soll sie nachträglich geändert werden, so geht das nicht über das Administrations-Interface der Appliance, sondern mit Suse-Linux-Bordmitteln über den Befehl "yast mail". Das genaue Vorgehen dazu wurde im Detail in der Dokumentation beschrieben.

Darüber hinaus lassen sich unter den Mail-Server-Einstellungen des Konfigurations-Interfaces noch Settings zum Mail-Format (HTML, Klartext, Multipart) und zur Codierung (beispielsweise "Quoted Printable") vornehmen. Außerdem legen die zuständigen Mitarbeiter an dieser Stelle auch noch fest, wie Bilder in die E-Mails eingebunden werden sollen und ähnliches.

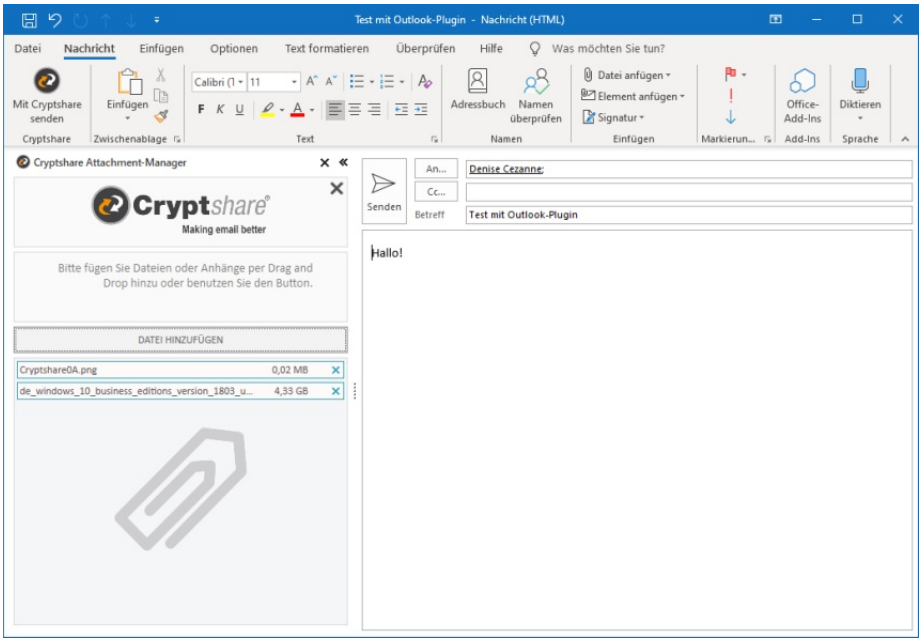
Damit ist die Erstkonfiguration abgeschlossen. Wir überprüften zu diesem Zeitpunkt noch mit der Update-Funktion, ob unserer Server auf dem aktuellen Stand war und konnten das System anschließen nutzen. Während des Tests aktualisierten wir unsere Installation übrigens von der uns ursprünglich zur Verfügung ge-



Der Transferdialog im Outlook-Add-In. Hier lässt sich auch die Verschlüsselung des Betreffs aktivieren.

stellten Version 4.3 auf die neu erschienene Version 4.4, dabei kam es zu keinen Schwierigkeiten. In diesem Zusammenhang ist es aber noch wichtig zu wissen, dass die Update-Funktion des

Web-Interfaces nur zum Aktualisieren der Cryptshare-Software selbst zum Einsatz kommt. Das zugrundeliegende Suse-Linux bringt sich über einen Cron-Job regelmäßig selbst auf den aktuellen Stand. Lediglich größere Upgrades, wie beispielsweise von OpenSuse-Version 15.0 auf 15.1, muss der Administrator selbst anstoßen. Das geht auch über das Web-Interface.



Dateiversand mit dem Outlook-Add-In

Details zu den weiteren Einstellungen der Policies

Bevor wir uns mit unseren Erfahrungen bei der praktischen Arbeit mit der Cryptshare-Lösung auseinandersetzen, ergibt es an dieser Stelle Sinn, noch einmal im Detail auf die weiteren Einstellungen einzugehen, die Teil der Policies sind. Diese lassen sich nutzen, um für Übertragungen, auf die die jeweilige Regel zutrifft, bestimmte Zeiträume vorzugeben, während denen die zu übertragene Datei auf dem Cryptshare-Server vorgehalten wird. Außerdem lässt sich auch eine maximale Transfergröße definieren, so dass beispielsweise Mitarbeiter aus der Grafikabteilung größere Dateien versenden dürfen als Benutzer aus der Buchhaltung. Darüber hinaus kann eine Regel auch das Verschlüsseln einer Nachricht erzwingen, bestimmte Signaturen anhängen oder den Download einer Datei nach einer bestimmten Zahl falscher Passworteingabeversuche sperren. Alle diese Policy-Einträge überschreiben die Default-Einstellungen des Servers, so dass es Sinn ergibt, server-seitig eine bestimmte Grundkonfiguration vorzugeben, die zum Absichern der meisten Übertragungen ausreicht, und dann für kritische Bereiche Policies zu definieren, die die Sicherheitskonfiguration weiter verfeinern. Abgesehen von den genannten Punkten können die Policies unter anderem auch zum Einsatz kommen, um übertragungsbasiert Einstellungen für den Mailserver zu modifizieren und die Settings für das Logging anzupassen.

Die praktische Arbeit mit Cryptshare

Um nun die praktische Arbeit mit Cryptshare unter die Lupe zu nehmen, riefen wir zunächst einmal das Benutzer-Interface (Cryptshare Web Application) unter https://{Hostname des Cryptshare-Servers} über einen Browser auf. Danach wollte das System wissen, ob wir eine Datei bereitstellen oder abrufen wollten. Nachdem wir auf "Bereitstellen" geklickt hatten, wollte das System unseren Namen, unsere Telefonnummer und unsere E-Mail-Adresse in Erfahrung bringen. Daraufhin schickte uns der Cryptshare-Server eine Verifizierungs-E-Mail mit einem Code, den wir anschließend im Web-Interface eintragen mussten, um unsere Mail-Adresse zu bestätigen. Jetzt konnten wir die Empfänger-Mail-Adresse eintragen, dabei besteht auch die Option, mehrere Empfänger, mit Kommas oder Leerzeichen getrennt, anzugeben.

Im nächsten Schritt war es dann möglich, der Nachricht die Dateien anzufügen, die übertragen werden sollten. Außerdem gibt es auch die Option, der Benachrichtigungs-E-Mail mit dem Download-Link eine vertrauliche (verschlüsselte) Nachricht hinzuzufügen.

Jetzt kommen die Transferoptionen an die Reihe. Dabei legen die Mitarbeiter die Sprache für die Benachrichtigungs-Mail fest und definieren, wie lang der Download verfügbar sein soll. Darüber hinaus haben die Anwender an dieser Stelle unter anderem Gelegenheit, sich Benachrichtigungen schicken zu lassen, wenn die Dateien vom Empfänger heruntergeladen wurden und festzulegen, ob die Dateinamen der heruntergeladenen Files in diesen Benachrichtigungs-Mails erscheinen sollen, oder nicht. Zu guter Letzt lässt sich die Übertragung bei

Bedarf auch noch mit einem generierten oder selbst eingegebenen Passwort sichern. Falls gewünscht haben die Anwender auch die Option, an dieser Stelle die bereits erwähnte QUICK-Technologie zu aktivieren, über Datenübertragungen mit QUICK später mehr.

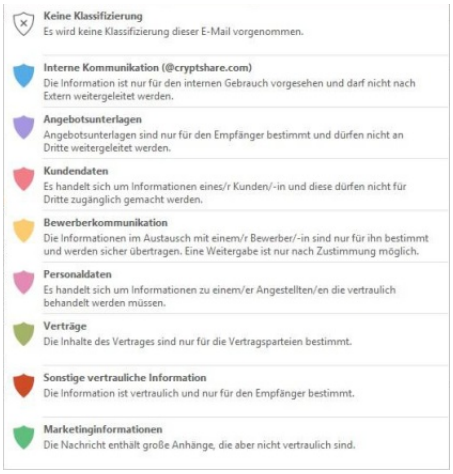
Im nächsten Schritt zeigt das System den Anwendern die Nachricht an, die der Empfänger zu sehen bekommen wird und ermöglicht es, den Transfer zu starten. Danach lädt die Software die zu übertragenen Files auf den Server hoch und verschlüsselt sie. Parallel dazu stellt das System die Empfänger-Mail zu. Über einen Klick auf den darin enthaltenen Download-Link haben die Empfänger dann Zugriff auf die verschlüsselte Nachricht und die Dateien. Ist kein QUICK aktiv und wurde ein Passwort vergeben, so müssen sie dieses allerdings zuerst – beispielsweise telefonisch – in Erfahrung bringen. Im Test ergaben sich bei der Arbeit mit dem Cryptshare Web-Interface keine Probleme.

Das Outlook-Add-In im Einsatz

Nachdem wir erfolgreich über das Web-Interface die ersten Datenübertragungen vorgenommen hatten, nahmen wir im Test das Outlook-Add-In unter die Lupe. Dieses stellt innerhalb des Outlook-Mail-Clients die gleichen Cryptshare-Funktionen bereit, die auch das Web-Interface bietet und ermöglicht es so, dabei zum Beispiel die Outlook-Notizbücher mit zu benutzen und alle von Cryptshare versendeten Mails im Postfach zu archivieren. Der Leistungsumfang des Add-Ins geht sogar noch über den des Web-Interfaces hinaus, denn das Add-In ist zusätzlich dazu in der Lage, Passwörter per SMS zu verschicken und Mails zu klassifizieren.

Im Test luden wir zunächst die Installationsdatei für das Add-In von der Webseite des Herstellers herunter, die dieser im MSI-Format bereitstellt. Die Installation läuft Wizard-gesteuert ab und wird niemanden vor unüberwindbare Schwierigkeiten stellen.

Nachdem wir die Software eingespielt und Outlook gestartet hatten, fand sich im Ribbon-Bereich



Die Klassifizierungsfunktion des Outlook-Add-Ins

des Mail-Clients unter "Start" ein Cryptshare-Eintrag, der es ermöglicht, den Support zu kontaktieren, QUICK zu aktivieren und den Transfermanager einzublenden, der am rechten Fensterrand über Benachrichtigungen, verwendete Passwörter und verfügbare Up- und Downloads informiert. Außerdem haben die Mitarbeiter an dieser Stelle auch die Option, Einstellungen vorzunehmen. Dazu gehören die Server-Adresse des Cryptshare-Servers, die Proxykonfiguration sowie Daten wie Name, Vorname und Telefonnummer des Benutzers. Dazu kommen noch diverse Add-In-Einstellungen, die es beispielsweise möglich machen, Passwörter zu speichern, eine Transferhistorie anzulegen und ähnliches.

Um nun eine Datei mit Hilfe des Add-Ins via Cryptshare zu versenden, müssen die Anwender lediglich ganz normal unter Outlook eine neue Mail erstellen und ihre Attachments anhängen. Danach gehen sie aber nicht auf den Button "Senden", sondern auf den Button "Mit Cryptshare senden", der nun neu oben links im Fenster erscheint.

Danach öffnet sich auf der linken Fensterseite eine Seitenleiste, über die sich bei Bedarf weitere Dateien zu der Nachricht hinzufügen lassen, auch große Files, die die Anwender über das Büroklammer-Symbol von Outlook nicht anhängen könnten. Anschließend genügt ein Klick auf "Senden", um den Transferdialog zu öffnen, über den die Nutzer die bekannten Transfereinstellungen wie Passwörter, Ablaufdatum und Empfängersprache vornehmen können. Im Outlook-Add-In ist es zudem auch möglich anzugeben, dass die Nachricht und auf Wunsch sogar die Betreffzeile mit verschlüsselt werden. Ein Klick auf "Transfer starten" sorgt dann für das Verschicken der Nachricht.

Wenn der Empfänger ebenfalls über das Outlook-Add-In verfügt, muss er zum Dateiempfang nicht auf die Web-Oberfläche von Cryptshare zurückgreifen. Eingehende Transferbenachrichtigungen landen in diesem Fall in der Transfer-Manager-Übersicht und lassen sich dort direkt anzeigen. Es ist auch möglich, dort den Download der Dateien zu starten. Im Test gestaltete sich die Arbeit mit dem Outlook-Add-In unpro-

blematisch und die Integration in die Office-Umgebung ließ keine Wünsche offen.

Gehen wir an dieser Stelle noch kurz auf die E-Mail-Klassifizierungsfunktion ein, die das Add-in bietet. Diese dient dazu, die E-Mails vor dem Versand vom Absender in eine bestimmte Schutzklasse einordnen zu lassen, wie beispielsweise "öffentlich", "vertraulich" oder "streng vertraulich". Die Schutzklassen kommen dann wiederum zum Einsatz, um die Zahl der Empfänger einzuschränken und so zu verhindern, dass Nachrichten versehentlich an nicht befugte Adressaten gelangen. Außerdem sind die IT-Verantwortlichen damit in der Lage, bestimmte Voreinstellungen für die oben genannten Transferoptionen festzulegen. Auf diese Weise stellen sie sicher, dass für bestimmte Inhaltstypen immer gleiche Sicherheitseinstellungen Verwendung finden. Insgesamt lassen sich 25 verschiedene Klassifizierungsstufen einrichten, die die zuständigen Mitarbeiter beliebig benennen können.

QUICK: Sichere Datenübertragungen ohne Passworttausch

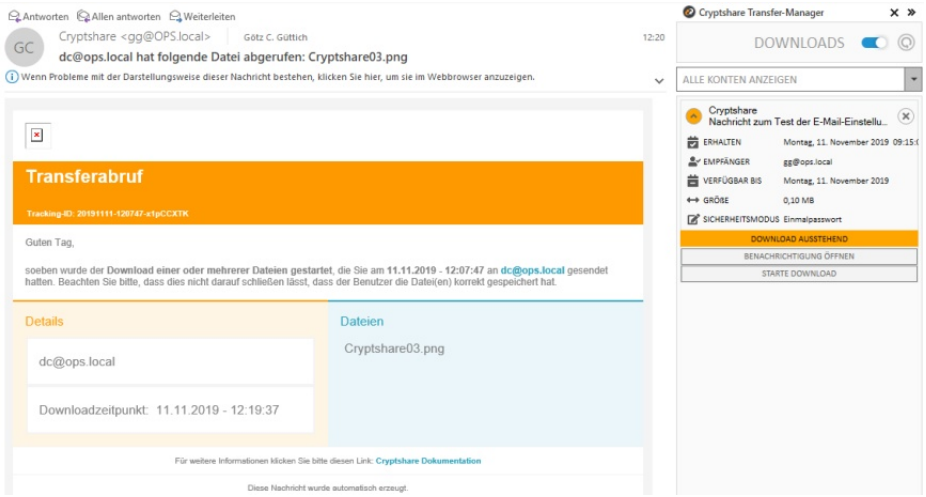
Um die bereits erwähnte QUICK-Technologie, die den manuellen Austausch der Passwörter zwischen den Kommunikationsteilnehmern überflüssig macht, zu aktivieren, muss man lediglich eine Datenübertragung anstoßen, die Schaltfläche "QUICK aktivieren" auswählen und ein „erstes“ Passwort vergeben. Wenn der Empfänger anschließend mit dem Passwort auf die Übertragung zugreift, hat er die Option, ebenfalls QUICK zu aktivieren. Dann erhält er eine Verifizierungs-E-Mail vom System. Nachdem diese eingegeben wurde, ist QUICK aktiv und kann genutzt werden.

Konkret bedeutet das, dass das System alle späteren Datenübertragungen zwischen den beiden Kommunikationspartnern, die ja beide verifiziert wurden, automatisch mit Einmalpasswörtern schützt, ohne dass die Benutzer dazu in irgendeiner Form aktiv werden müssen. Im Test funktionierte das einwandfrei und diese Technologie ist wirklich absolut empfehlenswert, da sie den Anwendern viel Arbeit spart und darüber hinaus eine große Zahl an Fehlerquellen ausschließt. Vor allem auf mobilen Geräten, auf denen keine richtige Tastatur zur Verfügung steht, ist QUICK ein echter Pluspunkt.

Geht die QUICK-Verbindung verloren, lässt sie sich mit Hilfe eines zweiten für QUICK aktivierten Clients oder mit Hilfe eines Administrators aktivieren. Dieser erhält dann eine Nachricht und kann dem betroffenen User anschließend einen Code generieren und zur Verfügung stellen, mit dem dieser dann in die Lage versetzt wird, QUICK auf seinem Endgerät zu nutzen. Dieses Vorgehen ergibt beispielsweise Sinn, wenn es darum geht, weitere Endpoints (wie etwa mobile Geräte) zu einer bestehenden QUICK-Verbindung hinzuzufügen oder wenn eine QUICK-Verbindung wiederbelebt werden soll, für die keine Endgeräte mehr existieren, da alle diesbezüglichen Token gelöscht wurden.

Hintergründe zu QUICK

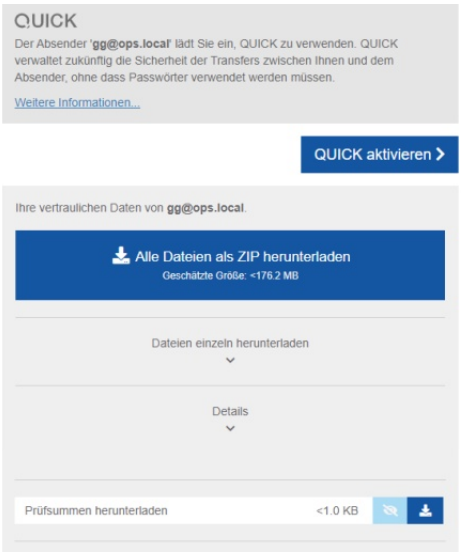
Gehen wir an dieser Stelle noch kurz etwas konkreter auf die Funktionsweise von QUICK ein. Sobald die Benutzer ihren Verifizierungscode in ihrem Client eingeben, erzeugt das System ein Verifizierungs-Token und speichert dieses in dem selben Client. Stößt ein Anwender nun die erste Dateiübertragung mit QUICK an, so generiert das System einen geteilten Schlüssel für die Kommunikation zwischen Absender und Empfänger. Dieser geteilte Schlüssel wird für den Absender verschlüsselt auf dem Server abgelegt. Zum Schutz dient ein automatisch erzeugter persönlicher Schlüssel, der ebenfalls verschlüsselt auf dem Server abgelegt wird. Auf diesen wiederum wird der Zugriff nur über das lo-



Eine Transferbenachrichtigung in Qutlook mit aktivem Add-In

kal gespeicherte Verifizierungstoken gewährt.

Wenn der Empfänger nun auf den Transfer zugreift, so generiert das System auch einen persönlichen



Die Einladung zu QUICK auf dem Client des Empfängers

Schlüssel für den Empfänger. Anschließend wird der geteilte Schlüssel mit Hilfe des persönlichen Schlüssels des Empfängers verschlüsselt und auf dem Cryptshare-Server gespeichert.

Damit wurde QUICK eingerichtet. Wenn es nun darum geht, Datenübertragungen über bestehende QUICK-Verbindungen abzuwickeln, so verwendet das System beim Erstellen einer Datenübertragung den persönlichen Schlüssel des Absenders, um den geteilten Schlüssel, der auf dem Server liegt, zu entschlüsseln. Anschließend erzeugt die Lösung unter Verwendung des gemeinsamen Schlüssels und eines Zufallsfaktors ein Einmalpasswort mit 64 Zeichen Länge und verschlüsselt damit den Datentransfer.

Wenn der Empfänger nun die Datei herunterlädt, so greift das System mit Hilfe des Verifizierungstokens auf dem Client auf dessen persönlichen Schlüssel zu. Dieser kommt dann zum Einsatz, um den geteilten Schlüssel auf dem Server lesbar zu machen. Der geteilte Schlüssel findet dann Verwendung, um in Kombination mit dem Zufallsfaktor das Transferpasswort zu ermitteln und damit auf die Daten zuzugreifen. Der Empfänger leitet sich das Verschlüsselungspasswort also selbst her und es ist nicht erforderlich, das Passwort in irgendeiner Form zu verschicken oder zu speichern. Zudem kommt für jeden Datentransfer automatisch ein anderes Passwort zum Einsatz.

Die Optionen zum Anpassen der Benutzeroberfläche

Da Cryptshare üblicherweise eng integriert in die Mail- und Web-Umgebungen der Kunden zum Einsatz kommt, spielen die Funktionen zum Anpassen des Aussehens des Systems eine besonders wichtige Rolle. Deswegen lassen sich über das Konfigurations-Interface der Lösung nicht nur verschiedene Sprachen einrichten, sondern auch Unternehmenslogos in die Web-Oberfläche einbinden sowie deren Farben und Hintergründe ändern. Es besteht bei Bedarf sogar die Option, CSS-Codes einzubinden. Auch das Layout der E-Mails lässt sich jederzeit mit Logo und Farben anpassen und es ist auch möglich, benutzerdefinierte Links zum Anwendungsmenü hinzuzufügen.

Fazit

Die Cryptshare-Lösung ist extrem flexibel. Dank der Automatisierung lässt sie sich auch für die Machine to Machine- und Application to Application-Kommunikation nutzen. Auf Seiten des Empfängers müssen keine besonderen technischen Voraussetzungen erfüllt sein, er muss nur E-Mails empfangen können. Das hilft dabei, Schatten-IT zu verhindern.

Umfassende Protokollierungsfunktionen sorgen dafür, dass stets klar ist, welche Dateien wann von wem wohin verschickt wurden und alle Transfers lassen sich optional auf Viren und Malware prüfen. Bei Bedarf können die Verantwortlichen auch Löschfristen für die Dateien auf dem Server setzen und das Einhalten der Vorgaben durch die DSGVO stellt kein Problem dar.

QUICK nach der erfolgreichen Aktivierung

Für den Betrieb der Lösung sind zudem keine Benutzerkonten und speziellen Zertifikate erforderlich und die Einbindung mobiler Geräte (im Test verwendeten wir Smartphones und Tablets unter Android und iOS) gestaltet sich nahtlos. Das gleiche gilt für die Qutlook-Integration, bei der uns besonders die Funktion zur Klassifizierung von E-Mails positiv auffiel. Cryptshare ist damit auf jeden Fall für alle Administratoren einen Blick wert, die sich mit der sicheren Übertragung großer Dateien an beliebige Empfänger auseinandersetzen müssen.