SOPHOS

Cybersecurity made simple.

SafeGuard Enterprise

Erste Schritte und Praxistipps

Produktversion: 8.3

Inhalt

1 Über diese Anleitung

In diesem Handbuch erhalten Sie Tipps zu den neuen Funktionen in SafeGuard Enterprise.

- Synchronized Encryption mit Unterstützung mehrerer Schlüssel
- Verbesserungen bei der Erstellung von kennwortgeschützten Dateien
- Outlook Add-in für pfadbasierte Verschlüsselung

Er enthält einen Überblick über die neuen Funktionen und wie Sie das Modul in Ihrer Umgebung implementieren. Weiterführende Informationen zum Synchronized Encryption Modul finden Sie in der SafeGuard Enterprise Administratorhilfe.

Es handelt sich hierbei um keine umfassende Installationsanleitung, sondern richtet sich hauptsächlich an Benutzer, die bereits mit dem Produkt vertraut sind. Weitere Informationen zu Installation und Administration finden Sie in der SafeGuard Enterprise Administratorhilfe.

2 Best Practice: Synchronized Encryption mit Unterstützung mehrerer Schlüssel

Mit SafeGuard Enterprise Synchronized Encryption können Sie zusätzliche Schlüssel für die Verschlüsselung an bestimmten Speicherorten konfigurieren.

Beispiel:

- Ihr Unternehmen verwendet **Anwendungsbasierend (Synchronized Encryption)** um alle Dateien, die mit gemeinsam genutzten Applikationen erstellt werden, standardmäßig mit dem **Synchronized Encryption-Schlüssel** zu verschlüsseln.
- Dateien im Benutzer-Ordner `Dokumente` werden mit dem **Persönlichen Schlüssel** verschlüsselt.
  - Der Benutzer-Ordner `Dokumente` sollte den Ordner `/unencrypted` enthalten, wo Benutzer unverschlüsselte Dateien speichern können.
- Um sicherzustellen, dass alle Dateien auf Endpoints entsprechend der Richtlinien Ihres Unternehmens verschlüsselt werden, sollten Sie die Initialverschlüsselung aktivieren.

2.1 File Encryption Richtlinie für mehrere Schlüssel erstellen

1. Wählen Sie im Management Center **(Default) File Encryption** und wählen Sie unter **Verschlüsselungstyp** die Option **Anwendungsbasierend (Synchronized Encryption)**.
2. Wählen Sie unter **Applikationenlisten** die Option **Template**.

   Die standardmäßig vordefinierte Applikationenliste heißt **Template**. Sie enthält die meist verwendeten Anwendungen.
3. Wählen Sie unter **Umfang der Verschlüsselung** die Option **Überall**. Dies ist die sicherste Option und wird üblicherweise für Windows-Endpoints verwendet.

   Es wird eine Regel erzeugt, nach der Dateien an allen Speicherorten mit dem **Synchronized Encryption Schlüssel** verschlüsselt werden. Die Regel wird zur Liste der Speicherorte hinzugefügt, wo anwendungsbasierte Verschlüsselung gilt.

   Nun können Sie bestimmte Regeln für Speicherorte hinzufügen, die Sie mit anderen Schlüsseln verschlüsseln möchten. Dies können lokale Speicherorte oder Orte im Netzwerk sein. Sie können vordefinierte Werte verwenden, um sie zu definieren.

   In unserem Beispiel möchten wir den Ordner `Dokumente` des Benutzers verschlüsseln.
4. Um eine Regel zu erstellen, klicken Sie in das Feld **Pfad** und wählen Sie in der Auswahlliste **<Documents>** aus.

   Hinweis
   Sie können den Umfang der Verschlüsselung nicht verändern.

   Standardmäßig ist der **Synchronized Encryption-Schlüssel** ausgewählt, aber Sie können jeden beliebigen Schlüssel auswählen. Zum Beispiel den Domänenschlüssel oder den Schlüssel einer Organisationseinheit. Sie können auch den **Persönlichen Schlüssel** auswählen, der für jeden Benutzer einzigartig ist.

5. Klicken Sie auf das **Persönlicher Schlüssel** Symbol im Feld **Schlüssel**, um den persönlichen Schlüssel des Benutzers zum Verschlüsseln des `Dokumente`-Ordners zu verwenden. Sie können den Mauszeiger über die Schlüssel-Symbole bewegen, um ihre Funktion anzuzeigen.

   Um einen Ordner von der Verschlüsselung auszunehmen, müssen Sie für diesen Ordner eine Ausnahmeregel definieren.
6. Klicken Sie in das Feld **Pfad**, wählen Sie **<Documents>** aus der Auswahlliste und geben Sie `\unencrypted` nach dem **<Documents>** Platzhalter ein.
7. Wählen Sie in der Spalte **Modus** die Option **Ausschließen** aus der Auswahlliste.
8. Um die Initialverschlüsselung auf den Endpoints zu aktivieren, setzen Sie die Option **Auf lokalen Laufwerken** unter **Initialverschlüsselung: Bestehende Dateien automatisch verschlüsseln** auf **Ja**.
9. Speichern Sie die Richtlinie und übertragen Sie sie an die relevanten Endpoints.

Hinweis
Wenn Sie eine solche Richtlinie mit nur spezifischen Regeln für Speicherorte und verschiedene Schlüssel Endpoints zuweisen, auf denen SafeGuard Enterprise 8.0 installiert ist, werden diese Regeln korrekt angewendet. Alle angegebenen Speicherorte werden mit den ausgewählten Schlüsseln verschlüsselt. Wenn jedoch eine Regel mit der Einstellung **Überall** für **Umfang der Verschlüsselung** Teil der Richtlinie ist, wird nur der **Synchronized Encryption -Schlüssel** verwendet. Dateien an allen spezifischen Speicherorten werden ebenfalls mit dem **Synchronized Encryption -Schlüssel** verschlüsselt.

2.2 Anwendungsbasierte Verschlüsselung mit mehreren Schlüsseln auf Endpoints

Auf dem Endpoint ist die SafeGuard Enterprise Encryption Software installiert, aber es kommt keine Richtlinie zur Anwendung.

Wenn Sie mit der rechten Maustaste auf das SafeGuard Enterprise Taskleistensymbol klicken und auf **Synchronisieren** klicken, erhält der Endpoint die aktualisierten Richtlinien. Die Richtlinienänderungen enthalten die Liste der Anwendungen, für die alle neuen Dateien verschlüsselt werden müssen. Diese Liste enthält Microsoft Office, daher werden alle neuen Microsoft Office Dokumente verschlüsselt.

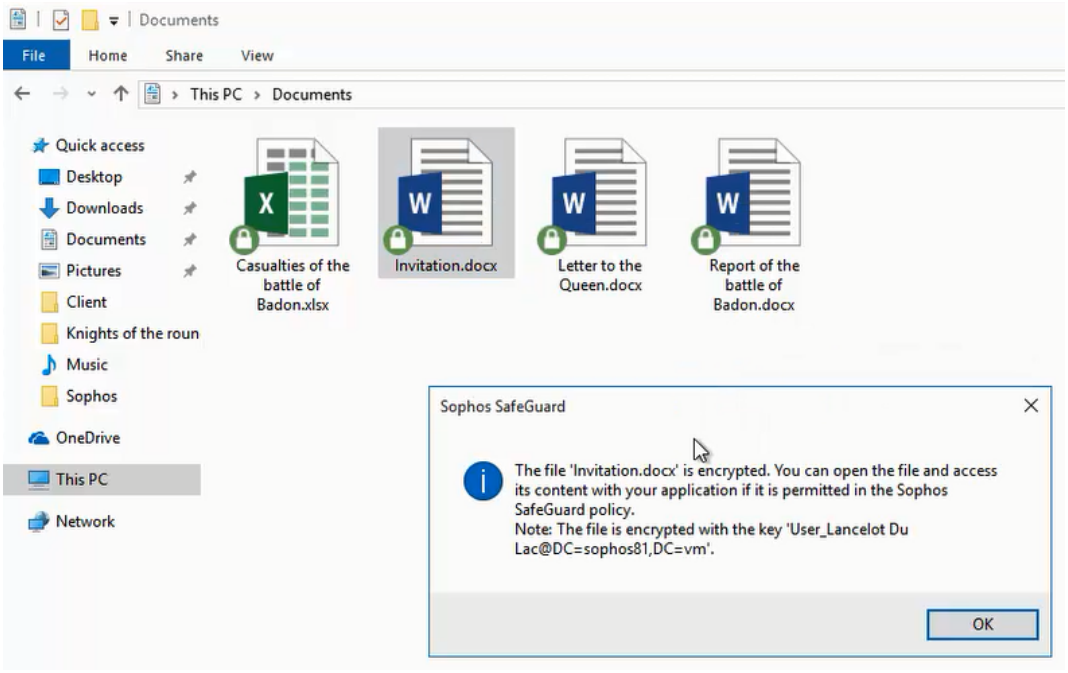
Da Sie die Initialverschlüsselung für alle lokalen Laufwerke eingeschaltet haben, werden auch alle Dateien verschlüsselt, die sich auf dem Computer befinden.

Hinweis
Beim Erstellen einer Applikationenliste müssen Sie explizit angeben, welche Dateien mit welchen Dateiendungen von der initialen Verschlüsselung verarbeitet werden sollen. Die **Template** Applikationenliste enthält die gebräuchlichsten Dateiendungen für jede Anwendung.

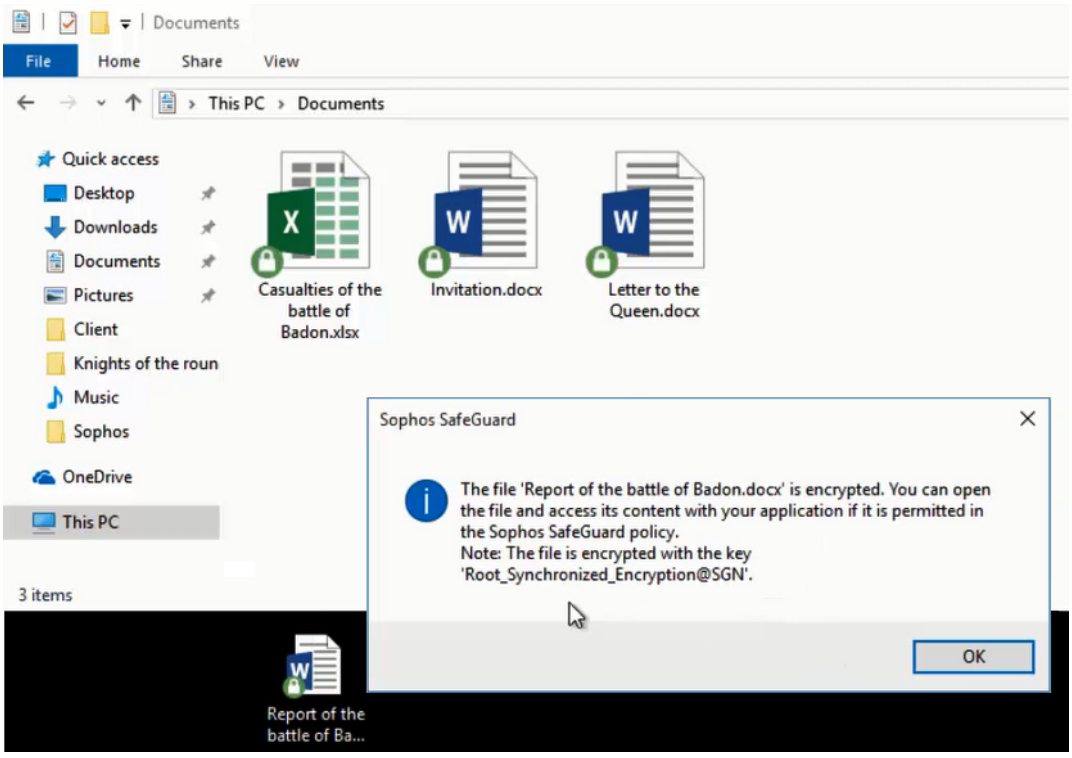
- Dateien im Ordner `Dokumente` werden mit dem **Persönlichen Schlüssel** des Benutzers verschlüsselt.
- Alle anderen Dateien, die gemäß Applikationenliste verschlüsselt werden müssen, werden mit dem **Synchronized Encryption Schlüssel** verschlüsselt.

Umfang der Verschlüsselung - Überall oder Definierte Speicherorte

Sie haben festgelegt, dass überall der **Synchronized Encryption Schlüssel** verwendet werden soll und haben eine Ausnahme für den **<Documents>** Ordner definiert, wo der **Persönliche Schlüssel** des Benutzers verwendet werden soll.



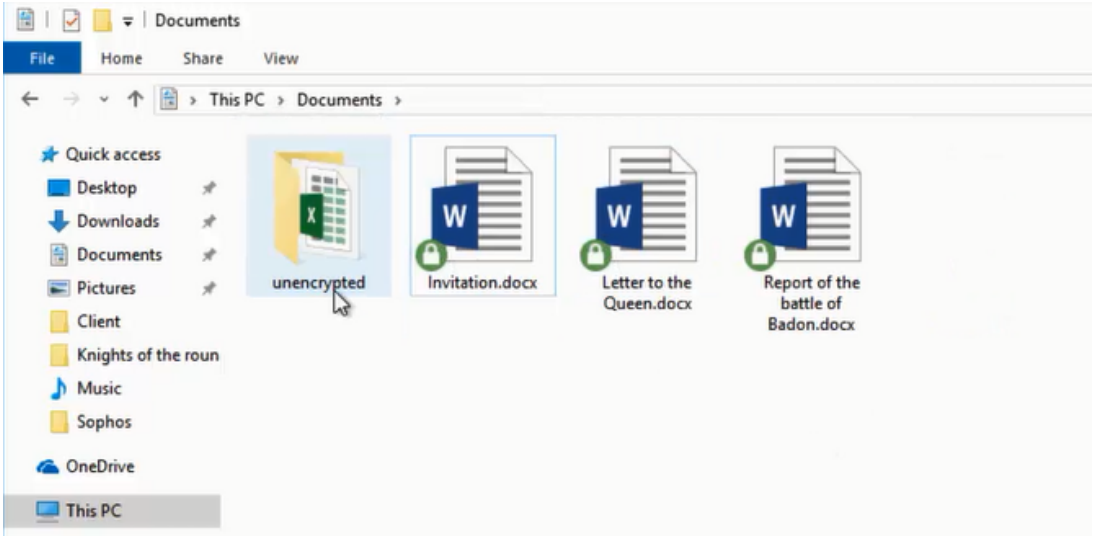
Das Verschieben oder Kopieren einer Datei ändert den für die Verschlüsselung verwendeten Schlüssel. Der neue Speicherort ist Teil der **Überall** Regel, daher wird der **Synchronized Encryption Schlüssel** verwendet.



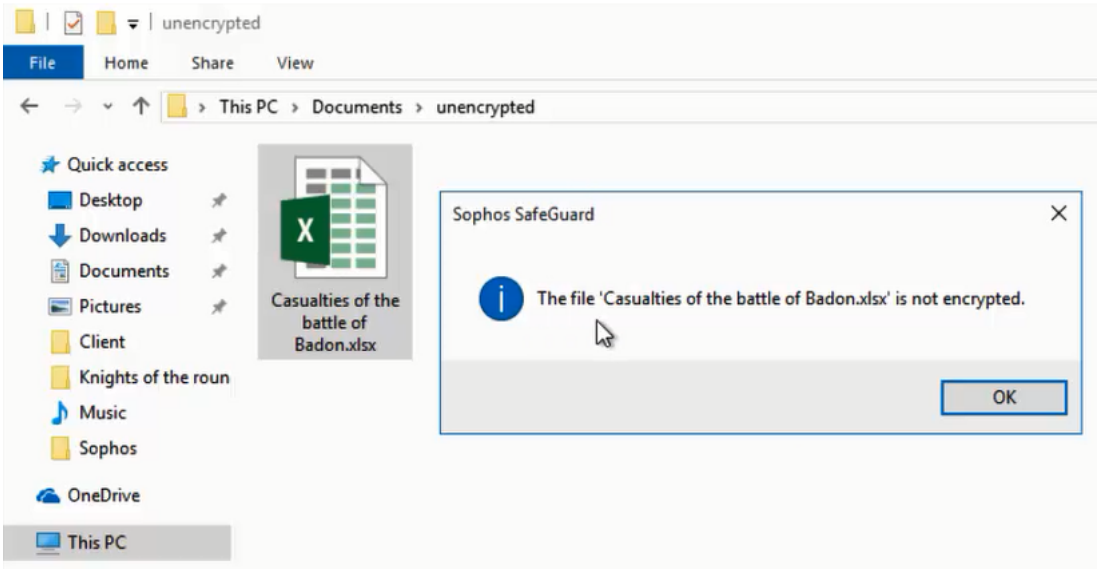
Wenn Sie eine Datei (verschlüsselt oder unverschlüsselt) in den Ordner **<Documents>** verschieben, wird sie mit dem **Persönlichen Schlüssel** des Benutzers verschlüsselt.

Ordner ohne Verschlüsselung

In der Richtlinie legen Sie fest, dass im Ordner **<Documents>**`\unencrypted` keine Dateien verschlüsselt werden.



Wenn Sie eine Datei in den Ordner unencrypted verschieben, wird sie entschlüsselt.



SafeGuard Enterprise entschlüsselt Dateien nur dann, wenn Sie eine oder mehrere einzelne Dateien an einem Ort ohne Verschlüsselung speichern. Wenn Sie einen Ordner an einen von der Verschlüsselung ausgenommenen Ort verschieben oder wenn Sie einen Ordner mit dem Namen eines ausgenommenen Ordners umbenennen, werden keine Dateien entschlüsselt, um einer versehentlichen Entschlüsselung vorzubeugen. Sie können dann die Dateien manuell entschlüsseln oder die Funktion Gemäß Richtlinie verschlüsseln aus dem SafeGuard File Encryption Kontextmenü des entsprechenden Ordners verwenden.

3 Outlook Add-In für pfadbasierte Verschlüsselung

Ab Version 8.1 ist das SafeGuard Enterprise Outlook Add-In für Windows auch für pfadbasierte Dateiverschlüsselung verfügbar. Es ist auf Endpoints verfügbar sobald Sie eines der Module für die pfadbasierte Dateiverschlüsselung installieren.

Generell funktioniert das Senden von E-Mails an externe Empfänger gleich wie bei der anwendungsbasierten Dateiverschlüsselung. Beim Senden von E-Mails mit Anhängen an Domänen auf Whitelists gibt es aufgrund der Natur der pfadbasierten Verschlüsselung und des Multi-Key Features allerdings einige Dinge zu beachten.

In der Richtlinie **(Default) Allgemeine Einstellungen** können Sie konfigurieren, was mit E-Mail-Anhängen passiert, die an (meist interne) Domänen auf Whitelists gesendet werden. Für das **Verhalten bei Domänen auf Whitelists** sind folgende Optionen verfügbar:

- **Verschlüsselt**
- **Keine Verschlüsselung**
- **Immer fragen**
- **Unverändert (Synchronized Encryption)**

Keine Verschlüsselung und **Immer fragen** verhalten sich bei allen File Encryption Modulen gleich.

Die Optionen **Verschlüsselt** und **Unverändert (Synchronized Encryption)** verhalten sich bei Synchronized Encryption anders als bei pfadbasierter Verschlüsselung.

Verschlüsselt

- Synchronized Encryption

  Verschlüsselte Dateien bleiben verschlüsselt; der Schlüssel wird nicht verändert. Unverschlüsselte Dateien werden mit dem **Synchronized Encryption-Schlüssel** verschlüsselt, wenn die Dateierweiterung in der Liste der In-Apps definiert ist.

- Pfadbasierte Verschlüsselung

  Alle angehängten Dateien werden mit dem **Synchronized Encryption Schlüssel** verschlüsselt - unabhängig von ihrer Dateierweiterung und ihrem Verschlüsselungsstatus.

Unverändert (Synchronized Encryption)

- Synchronized Encryption

  Verschlüsselte Dateien werden verschlüsselt gesendet; unverschlüsselte Dateien werden unverschlüsselt gesendet.

- Pfadbasierte Verschlüsselung

  Alle Dateien werden mit dem **Synchronized Encryption Schlüssel** verschlüsselt.

4 Kennwortgeschützte Dateien

Mit Synchronized Encryption wurde das Konzept der kennwortgeschützten Dateien eingeführt, wobei Benutzer verschlüsselte HTML-Dateien erzeugen, die zum Entschlüsseln ein Kennwort benötigen.

Mit SafeGuard Enterprise 8.1 ist diese Funktion auch im Modul zur pfadbasierten Dateiverschlüsselung auf Windows Endpoints verfügbar.

Hinweis
Auf macOS Endpoints ist diese Funktion bereits seit Version 8 verfügbar.

4.1 Datei mit Kennwort schützen

Wenn Sie E-Mails an Empfänger außerhalb Ihres Firmennetzwerks senden, empfehlen wir, die Datei mit einem Kennwort zu verschlüsseln. Das erlaubt den Empfängern ohne SafeGuard Enterprise auf verschlüsselte Dateien zuzugreifen.

Gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf die Datei, die Sie versenden möchten, und wählen Sie **Kennwortgeschützte Datei erstellen**.
2. Klicken Sie dazu mit der rechten Maustaste auf die Datei, die Sie versenden möchten, und wählen Sie **Kennwortgeschützte Datei erstellen**.
   Wenn eine Fehlermeldung angezeigt wird, wählen Sie im Finder **Darstellung > Vorschau ausblenden** und versuchen Sie es erneut.
3. Folgen Sie den Anweisungen auf dem Bildschirm und erzeugen Sie ein Kennwort. Wählen Sie ein sicheres Kennwort und senden Sie es nicht in derselben E-Mail wie die Dateien.
   Ihre Datei wird verschlüsselt und als HTML-Datei gespeichert. Sie können die HTML-Datei nun sicher per E-Mail versenden.

   Hinweis
   - Für die Verschlüsselung benötigen Sie freien Platz auf der Festplatte.
   - Die verschlüsselte HTML-Datei ist größer als die Originaldatei.
   - Die maximal unterstützte Dateigröße beträgt 50 MB.
   - Um mehrere Dateien auf einmal zu verschlüsseln, können Sie sie in eine .zip-Datei packen und die .zip-Datei verschlüsseln.

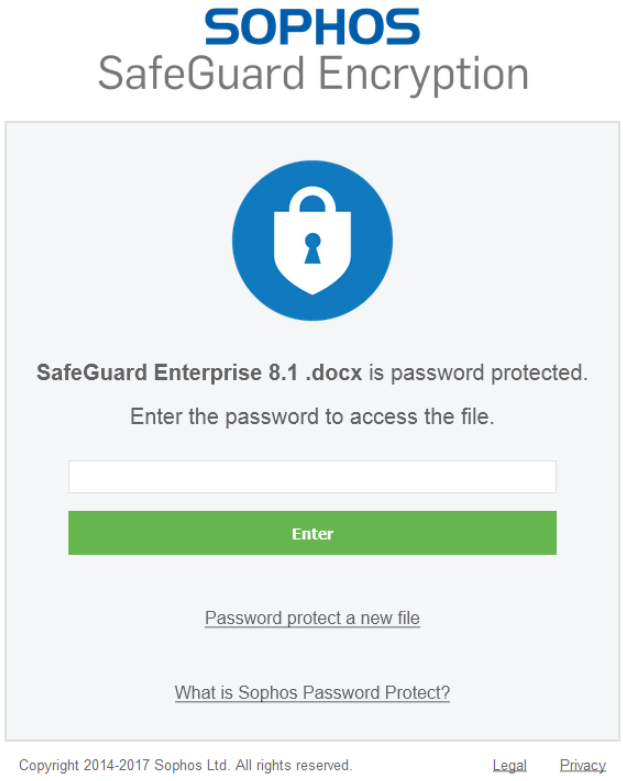
4. Übermitteln Sie Ihren Empfängern das Kennwort am Telefon oder persönlich.
   Empfänger können einen der folgenden Browser verwenden, um den kennwortgeschützten Anhang zu öffnen:
   - Mozilla Firefox
   - Google Chrome
   - Microsoft Internet Explorer 11
   - Microsoft Edge
5. Weisen Sie Ihre Empfänger an, auf die Datei doppelzuklicken und den Anweisungen auf dem Bildschirm zu folgen, um Folgendes zu tun:

- Das Kennwort eingeben und auf **Entschlüsseln** klicken, um auf die Datei zuzugreifen
- Auf **Neue Datei mit Kennwort schützen** klicken, um eine andere Datei mit einem Kennwort zu schützen.

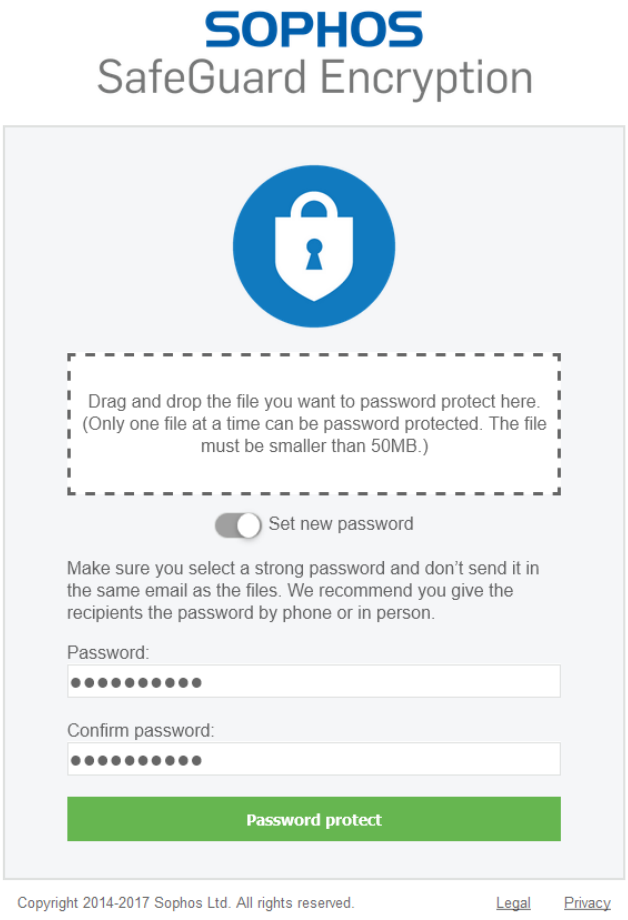
Empfänger können die Datei öffnen, die Sie mit einem Kennwort geschützt haben. Sie können die Datei mit einem Kennwort schützen, bevor sie sie an Sie zurücksenden. Dabei können sie dasselbe oder ein neues Kennwort verwenden. Sie können sogar eine neue Datei mit einem Kennwort schützen.

4.2 Eine neue Datei mit einem Kennwort schützen

Empfänger einer Datei, die mit SafeGuard Enterprise 8.1 kennwortgeschützt wurde, können auch eine neue Datei mit einem Kennwort schützen. Sie müssen dazu nicht die Originaldatei entschlüsseln. Dies spart Zeit und funktioniert auch ohne das ursprüngliche Kennwort einzugeben.



Benutzer müssen nur auf eine verschlüsselte HTML-Datei doppelklicken und dann auf **Neue Datei mit Kennwort schützen** klicken.



Benutzer müssen eine Datei in das gekennzeichnete Feld ziehen, ein sicheres Kennwort wählen und auf **Mit Kennwort schützen** klicken.

5 Synchronized Encryption

Synchronized Encryption ist das anwendungsbasierte Dateiverschlüsselungsmodul von SafeGuard Enterprise. Die Unterschiede zur pfadbasierten Dateiverschlüsselung sind:

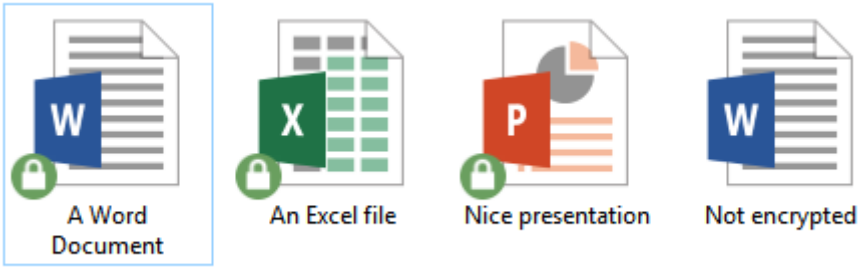
- Automatische Verschlüsselung von Dateien, die mit definierten Anwendungen (In-Apps) erzeugt oder bearbeitet wurden.
- Nur definierte Anwendungen können Dateien lesen.
- Die Verschlüsselung ist nicht vom Speicherort der Datei abhängig.
- Schlüssel können automatisch von den Geräten der Benutzer entfernt werden, wenn eine Bedrohung der Sicherheit erkannt wurde.

Hinweis
Dieses Feature ist nur verfügbar, wenn Sie web-basierte Sophos Central Endpoint Protection gemeinsam mit SafeGuard Enterprise verwenden. Sie benötigen eine SafeGuard Enterprise Richtlinie um Schlüssel entfernen zu können. Dieses Feature ist sowohl für Windows als auch für Mac Endpoints verfügbar.

5.1 Arbeiten mit Standardanwendungen

Mit Synchronized Encryption können Sie wie gewohnt arbeiten und brauchen sich nicht um Verschlüsselung zu sorgen. Nur wenn Sie Informationen mit Empfängern außerhalb Ihres Unternehmens teilen, müssen Sie einschätzen, welches Sicherheitsniveau angebracht ist.

Zum Beispiel: Sie erstellen wie gewohnt Inhalte in Excel oder PowerPoint. Beim Speichern werden die Dateien automatisch verschlüsselt. Verschlüsselte Dokumente werden mit einem kleinen Vorhängeschloss-Symbol am Dateisymbol gekennzeichnet.



5.2 Informationen innerhalb des Unternehmens teilen

Die Verwendung des SafeGuard Enterprise **Synchronized Encryption** Schlüssels erleichtert den internen Informationsaustausch. Jeder Benutzer von SafeGuard Enterprise in Ihrem Unternehmen kann die Informationen lesen.

Diese Version von SafeGuard Enterprise (SGN 8.1) ermöglicht Ihnen, zusätzliche Schlüssel für die Verschlüsselung bestimmter Speicherorte zu konfigurieren. Damit Benutzer Dateien lesen können, die mit einem anderen Schlüssel als dem Synchronized Encryption Schlüssel verschlüsselt sind, muss der Benutzer diesen Schlüssel in seinem Schlüsselring haben, siehe Best Practice: Synchronized Encryption mit Unterstützung mehrerer Schlüssel (Seite 2).

Hinweis
Benutzer können ihren Schlüsselring anzeigen indem sie mit der rechten Maustaste auf das SafeGuard Enterprise Taskleistensymbol klicken und dann auf **Anzeigen > Schlüsselring** klicken.

Sie können mit den verschlüsselten Dateien in gewohnter Weise verfahren: per E-Mail senden, auf eine Netzwerkfreigabe stellen oder auf einen Wechseldatenträger kopieren.

Sie müssen Synchronized Encryption auf den Rechnern aller Benutzer installieren, die Zugriff auf die innerhalb des Unternehmens geteilten Informationen benötigen.

Hinweis
Stellen Sie sicher, dass Sie SafeGuard Enterprise sowohl für Windows als auch für Mac Benutzer installieren.

5.3 Informationen mit externen Parteien austauschen

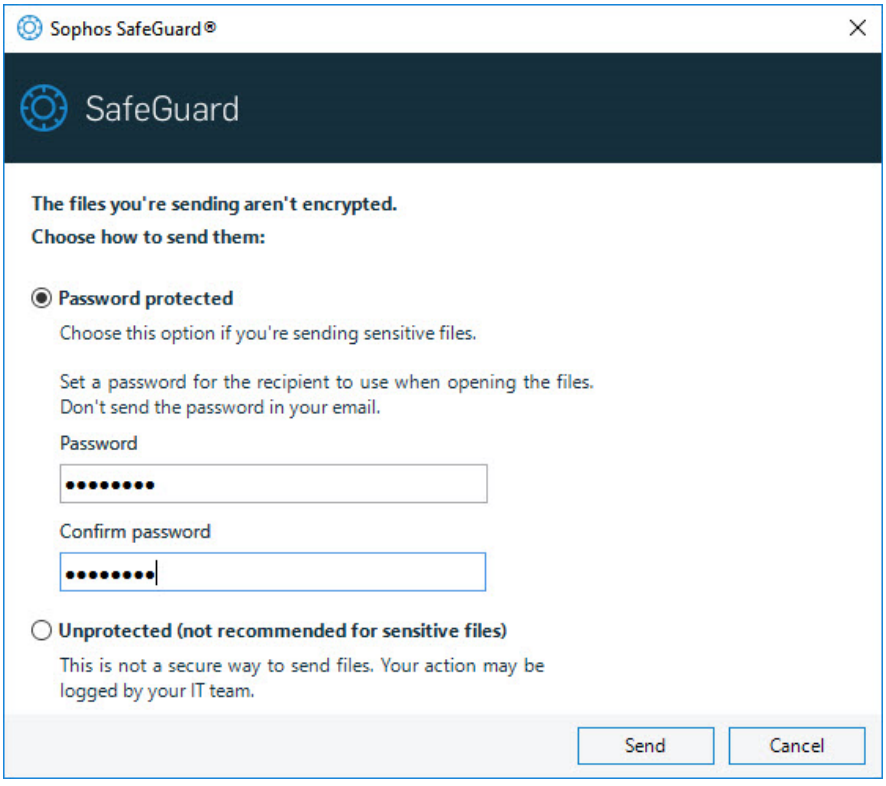
Die Verschlüsselung von Daten dient dazu, den Zugang zu sensiblen Daten einzuschränken. Dokumente mit Finanzdaten oder neuestem geistigen Eigentum sind üblicherweise nicht für die Öffentlichkeit gedacht. Dennoch gibt es oft Fälle, wo Sie derartige Informationen mit jemandem außerhalb Ihres Unternehmens teilen möchten. Manchmal sollen die Dokumente weiterhin verschlüsselt sein, manchmal handelt es sich auch nicht um vertrauliche Daten.

Für Benutzer von Outlook gelten andere Arbeitsabläufe wie für Benutzer anderer Mail-Clients.

Tipp
Geben Sie Ihren Benutzern Zugriff auf die SafeGuard Enterprise Benutzerhilfe.

Outlook-Benutzer

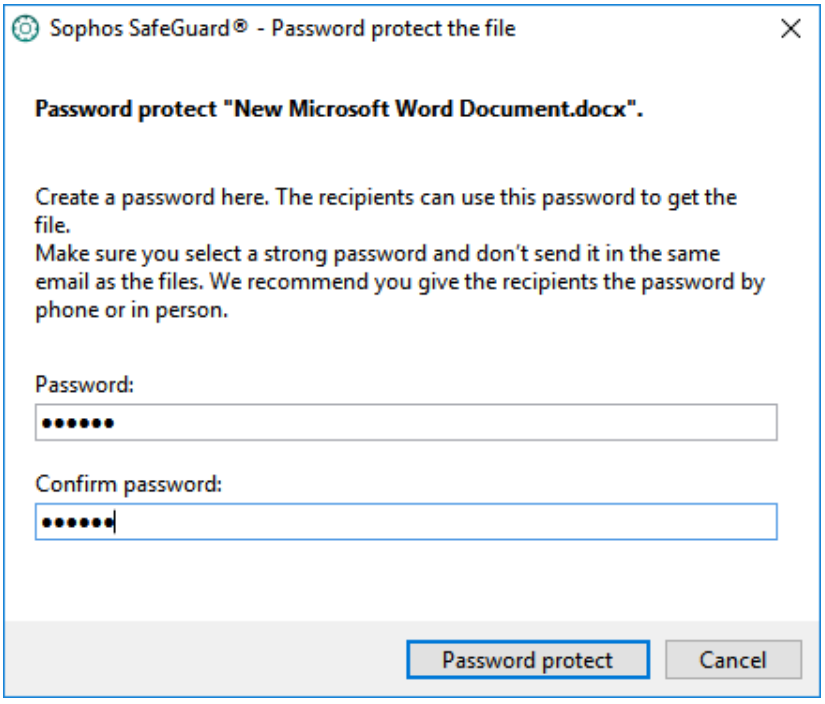
Benutzer mit einem Windows Computer mit Microsoft Outlook (32-Bit-Version von Office) müssen sich nicht weiter um Verschlüsselung kümmern. Sie können Synchronized Encryption so konfigurieren, dass immer wenn eine E-Mail mit einem Anhang an einen externen Empfänger gesendet wird, Benutzer mittels Pop-up gefragt werden, wie mit dem Anhang verfahren werden soll.



Weitere Benutzer

Windows und Mac Benutzer können eine Datei entweder entschlüsseln, um sie unverschlüsselt zu versenden, oder eine kennwortgeschützte Datei erzeugen, um Inhalte sicher zu teilen.

Sie können mit der rechten Maustaste auf eine Datei klicken und **SafeGuard Dateiverschlüsselung** > **Ausgewählte Datei entschlüsseln** wählen. Oder sie wählen **SafeGuard Dateiverschlüsselung** > **Kennwortgeschützte Datei erstellen**. In diesem Fall wird eine neue Datei mit der Endung HTML erzeugt und der Empfänger kann mit dem vom Sender definierten Kennwort auf die Datei zugreifen.



Weitere Informationen finden Sie in der SafeGuard Enterprise Benutzerhilfe im Kapitel Mailanhänge sicher versenden.

5.4 Definieren von In-Apps

In-Apps sind Anwendungen, die verschlüsselte Inhalte erzeugen und lesen können. Diese Anwendungen werden von einem Sicherheitsbeauftragten anhand von vollständigen Pfaden sowohl für Windows als auch für Mac OS X definiert.

Tipp
Stellen Sie sicher, dass die Anwendungen auf allen Computern am selben Ort installiert sind oder beziehen Sie alle möglichen Installationsverzeichnisse in die Definition der In-Apps mit ein.

5.4.1 Welche Anwendungen soll ich als In-App definieren?

In-Apps sind die einzigen Anwendungen, die verschlüsselte Inhalte erzeugen und lesen können. Sie müssen alle Anwendungen einbeziehen, die Sie zum Erstellen oder Lesen von verschlüsselten Dateien verwenden möchten.

Typische Anwendungen für die Erstellung von Inhalten:

- Office Suites (Microsoft Office, OpenOffice, FreeOffice, ...)
- Design Suites (Adobe Creative Suite, ...)

Typische Anwendung zum Betrachten von Inhalten:

- Office-Betrachter
- PDF-Betrachter
- Bildbetrachter

Hinweis
Sie können keine Windows Store Apps zur Liste der In-Apps hinzufügen.

Tipp
Berücksichtigen Sie alle Dateitypen, die von Anwendungen zum Erstellen von Inhalten verwendet werden. Sie müssen zum Beispiel für Microsoft Word neben .docx auch .rtf, .odt etc. hinzufügen.

In einigen Fällen müssen Sie auch Anwendungen einbeziehen, die nur von einzelnen Benutzern verwendet werden. Das bedeutet aber nicht, dass Sie die entsprechende Richtlinie nur bestimmten Benutzern zuweisen müssen; wenn Benutzer eine Richtlinie für eine Anwendung erhalten, die sie nicht haben, so wird dieser Teil der Richtlinie ignoriert.

5.4.2 Welche Anwendungen soll ich NICHT als In-App definieren?

Verschlüsselung verhindert, dass sensible Informationen nach außen dringen; daher sollen Anwendungen, die dazu dienen, Informationen zu versenden, niemals als In-Apps definiert werden.

Andernfalls würden alle Inhalte vor dem Senden entschlüsselt und es bestünde keinerlei Schutz der Daten.

Definieren Sie daher nie Anwendungen wie E-Mail-Clients, Internet Browser, Backup-Software und dergleichen als In-Apps.

Hinweis
Für Mac OS X kann es jedoch sinnvoll sein, E-Mail-Programme einzubeziehen, da kein Outlook Add-In verfügbar ist.

5.5 Aspekte, die vor der Bereitstellung beachtet werden müssen

Stellen Sie Synchronized Encryption vorerst nur einer eingeschränkten Anzahl von Personen (Testgruppe) zur Verfügung. Statten Sie alle anderen Benutzer mit einer Richtlinie aus, mit der sie keine verschlüsselten Inhalte erzeugen, jedoch auf die verschlüsselten Dateien ihrer Kollegen zugreifen können, siehe Erstellen von Lesezugriff-Richtlinien (Seite 17).

Beachten Sie außerdem vor der Bereitstellung von Synchronized Encryption die folgenden Aspekte.

5.5.1 Öffnen von Dateien in einer anderen App als der mit der sie erstellt wurden

Viele Anwendungen können Dateien in unterschiedlichen Formaten erzeugen. Zum Beispiel kann Microsoft Word auch PDF-Dateien erzeugen. Ist Microsoft Word als In-App (Anwendung, die Dateien verschlüsselt) definiert, werden die erzeugten PDF-Dateien verschlüsselt. Dies ist erwartetes Verhalten, da es sich um sensiblen Inhalt handeln könnte.

Jedoch müssen Sie auch die Anwendung berücksichtigen, mit der die Datei geöffnet und gelesen werden soll. In unserem Beispiel ist dies wahrscheinlich ein PDF-Betrachter, und obwohl PDF-Betrachter normalerweise nicht zum Erstellen von Dateien verwendet werden, müssen sie doch als In-Apps definiert werden. Andernfalls können die Dateien nicht mit dem PDF-Betrachter gelesen werden. Aus diesem Grund haben wir die häufigsten PDF-Betrachter schon in die Applikationenlisten-Vorlage aufgenommen, die im SafeGuard Management Center zur Verfügung steht.

Andere Beispiele:

- In-Apps, die Bilder exportieren
- In-Apps, die Text in unterschiedlichen Formaten exportieren, zum Beispiel .txt, .rtf oder .csv.

Tipp
Berücksichtigen Sie für alle Dateien, die Sie mit den definierten In-Apps erzeugen können, Anwendungen zum standardmäßigen Öffnen der Dateien. Stellen Sie sicher, dass diese Anwendungen auf allen Computern installiert sind und definieren Sie sie ebenfalls als In-Apps, um auf die verschlüsselten Inhalte zugreifen können.

Windows 10 PDF

Der standardmäßige PDF-Betrachter für Windows 10 ist der neue Internet-Browser Edge. Sie könnten Edge zur In-App machen, das würde aber bedeuten, dass Dateien beim Hochladen über Edge entschlüsselt werden.

Wichtig
Statten Sie daher Ihre Windows 10 Geräte mit einem anderen PDF-Betrachter als Edge aus, zum Beispiel Adobe Acrobat Reader oder Foxit Reader.

5.5.2 Java-Anwendungen

Java-Anwendungen verwenden häufig dieselbe ausführbare Datei `java.exe` gemeinsam. Es ist daher nicht möglich, zwischen unterschiedlichen Java-Anwendungen anhand des Pfades der laufenden `java.exe` zu unterscheiden. Wenn Sie `java.exe` als In-App definieren, müssen Sie bedenken, dass alle Anwendungen, die diese ausführbare Datei verwenden, verschlüsselte Inhalte erstellen und darauf zugreifen können.

5.5.3 Webbasierte Anwendungen

Benutzer müssen häufig mit Dokumenten arbeiten und sie dann in eine webbasierte Anwendung hochladen. Verschlüsselte Dateien bleiben verschlüsselt und können vom zugrunde liegenden System nicht gelesen werden. Dies bedeutet:

- Die Dateien können nicht aufgrund ihres Inhalts indexiert werden.
- Werden Dateien von außen aufgerufen, sind sie nicht lesbar.

Möglicherweise benötigen Sie extern Zugriff auf diese Dateien. Benutzer können dazu die Dateien vor dem Hochladen entschlüsseln. Alternativ können Sie einen Ordner erstellen, wo Dateien unverschlüsselt gespeichert werden.

Dieser von der Verschlüsselung ausgenommene Ordner sollte nur für diesen Zweck verwendet werden. Stellen Sie sicher, dass Ihre Benutzer darüber informiert werden.

Tipp
Erstellen Sie eine Ausnahme für die Dateiverschlüsselung; entweder über einen direkten Pfad wie `c:\unencrypted`, oder definieren Sie einen relativen Pfad (nur auf Windows Endpoints möglich). Wenn Sie einen relativen Pfad verwenden, müssen Benutzer nur einer Ordner mit einem vereinbarten Namen erstellen. Lautet der Name des Ordners beispielsweise `\unencrypted`, so werden Dateien und Unterordner in allen Ordnern mit dem Namen `\unencrypted` auf dem Computer nicht verschlüsselt.

5.5.4 Austausch von Informationen mit Plattformen, die nicht über SafeGuard Verschlüsselung verfügen

Zuweilen erstellen Benutzer Dateien, die zur Verwendung in einer anderen Umgebung gedacht sind. Zum Beispiel können Dateien auf einem Windows oder Mac Endpoint erstellt werden aber in einer Terminal Server Umgebung verwendet werden. Da SafeGuard Enterprise in Terminal Server

Umgebungen nicht unterstützt wird, bleiben verschlüsselte Dateien dort verschlüsselt und können von keiner Anwendung gelesen werden.

Die Lösung besteht darin, den gewünschten Speicherort per Verschlüsselungsrichtlinie von der Verschlüsselung auszuschließen.

5.5.5 Was passiert mit meinen Vorschauen?

Dateibrowser (Windows Explorer oder Finder) können Vorschauen für unterschiedliche Dateitypen wie Bilder, Textdokumente, Tabellenkalkulationen und PDF-Dateien anzeigen. Diese Vorschauen werden üblicherweise beim Speichern oder Ändern der Datei erzeugt. Um eine Vorschau erzeugen zu können, muss die entsprechende Anwendung auch Zugriff auf den unverschlüsselten Inhalt der Datei haben. Daher muss die Anwendung zur Liste der In-Apps hinzugefügt werden. Bei Mac OS X handelt es sich um eine separate Anwendung, die standardmäßig in der Liste enthalten ist.

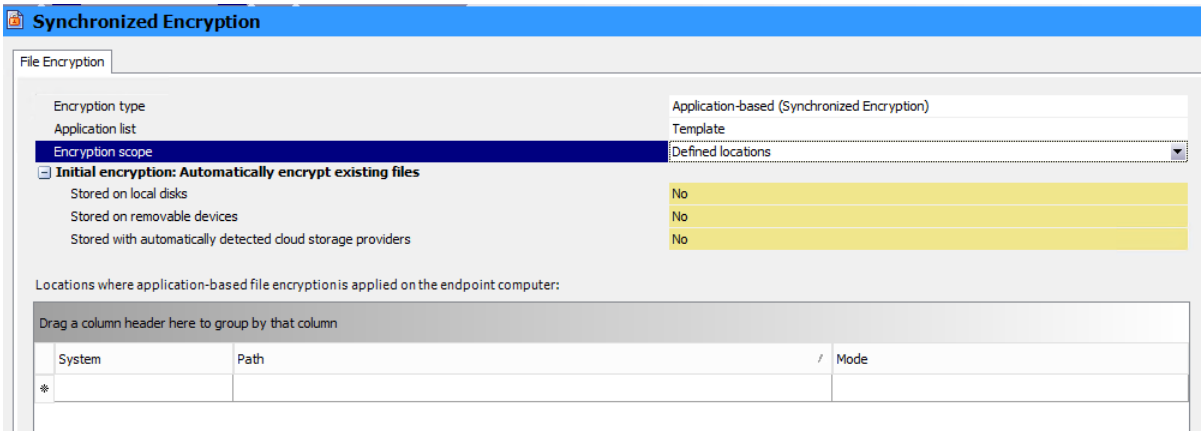
5.6 Erstellen von Lesezugriff-Richtlinien

Am Beginn des Rollouts von Synchronized Encryption sollen Benutzer in der Lage sein, verschlüsselte Dokumente zu lesen, aber nicht selbst zu erstellen. Sie können dann nach und nach die Verschlüsselung für bestimmte Gruppen und schließlich für alle Benutzer aktivieren.

Die erste Richtlinie ist eine Lesezugriff-Richtlinie.

Windows

Für Windows Benutzer erstellen Sie eine Synchronized Encryption Richtlinie mit allen benötigten Anwendungen und definieren **Definierte Speicherorte** als **Umfang der Verschlüsselung**, definieren jedoch keine Speicherorte.



Weitere Informationen finden Sie in der SafeGuard Enterprise Administratorhilfe im Kapitel Erstellen von Lesezugriff-Richtlinien für Windows Endpoints.

Mac OS X

Mac OS X verhält sich anders als Windows. Auf Mac OS X Computern können verschlüsselte Dateien nur in definierten Speicherorten gelesen werden.

Das bedeutet, dass die Lesezugriff-Richtlinie für Windows-Nutzer nicht für Mac-Nutzer verwendet werden kann.

Für Mac-Nutzer erstellen Sie eine Richtlinie vom Typ **Dateiverschlüsselung** und wählen **Pfadbasiert** als Verschlüsselungstyp. Sie müssen zumindest einen Speicherort hinzufügen, ihn von der Verschlüsselung **Ausschließen** und den Pfad den Mac-Nutzern mitteilen. Der Pfad lautet beispielsweise `<Documents>/Verschlüsselt`. Benutzer, die ein verschlüsseltes Dokument lesen möchten, müssen das Dokument zuerst an diesen Speicherort kopieren oder verschieben.

Weitere Informationen finden in der SafeGuard Enterprise Administratorhilfe im Kapitel Erstellen von Lesezugriff-Richtlinien für Mac Endpoints.

5.7 Informieren der Endbenutzer

In vielen Fällen ist das Thema Verschlüsselung neu für Benutzer. Wir empfehlen daher, dass Sie Benutzer über Ihre Vorgehensweise und Regeln hinsichtlich Verschlüsselung aufklären. Besonders bei Synchronized Encryption ist es wichtig für Benutzer zu erfahren, was sie zu erwarten haben. Zum Beispiel: Welche Anwendungen werden als In-Apps definiert? Dieses Wissen ermöglicht Benutzern, fehlende Anwendungen zu identifizieren und dem SafeGuard Enterprise Sicherheitsbeauftragten Feedback zu geben. Dieser kann dann die benötigte Anwendung zur Liste der In-Apps hinzufügen.

Empfohlene Vorgehensweise:

- Senden Sie eine E-Mail an alle Benutzer in der Sie erklären, welche Verschlüsselungsregeln implementiert werden und welche Auswirkungen sie haben. Idealerweise stellen Sie einen Link auf eine interne Website bereit, die Sie jederzeit leicht anpassen können wenn beispielsweise neue In-Apps hinzugefügt werden.
- Geben Sie eine Mail-Adresse an, an die Benutzer Feedback senden können.
- Wenn Sie SafeGuard Enterprise bereits auf allen Endpoints ausgerollt haben (eventuell nur Lesezugriff), können Sie ein Dokument anfügen, das mit dem Synchronized Encryption Schlüssel verschlüsselt ist, und ihre Benutzer prüfen lassen, ob sie das Dokument lesen können. Ist dies nicht der Fall, so wissen Sie, dass ein Problem bei der Installation oder bei der Kommunikation zwischen Endpoint und dem SafeGuard Backend vorliegt bevor Sie die Verschlüsselung für alle Benutzer aktivieren.

5.7.1 Beispielnachricht

Dies ist ein Beispiel für eine E-Mail, mit der Sie Ihre Benutzer informieren können. Sie enthält bereits die wichtigsten Informationen, aber Sie können selbstverständlich weitere Punkte hinzufügen, etwa wenn Sie eine Regel zum Ausnehmen von Ordnern mit dem Namen "Unencrypted" verwenden oder wenn Sie andere Anwendungen in Gebrauch haben. Der Text geht von dem Fall aus, dass mit der E-Mail ein mit Synchronized Encryption verschlüsseltes Dokument als Anhang gesendet wird.

= =

Sehr geehrte Kolleginnen und Kollegen,

die IT-Abteilung hat nun auf allen Rechnern SafeGuard Enterprise installiert. Dabei handelt es sich um ein Produkt zur Datenverschlüsselung von Sophos, das zukünftig von allen verwendet wird, um unsere Dokumente zu schützen. In der Regel wird dies keinen Einfluss auf Ihre tägliche Arbeitsweise haben, jedoch möchten wir Sie auf einige Ausnahmen hinweisen.

Wir werden Synchronized Encryption nächste Woche aktivieren. Sobald die Software aktiviert ist, werden Sie auf Ihrem Computer verschlüsselte Dateien erzeugen. Wir haben einiges an Informationen für einen leichten Einstieg auf unserer Intranet-Seite unter "Verschlüsselung" zusammengestellt, siehe https://firma.intern/verschluesselung.

Um zu prüfen, ob Ihr Gerät bereit für die Verschlüsselung ist, öffnen Sie bitte die angefügte Datei.

- **Windows und Mac OS X:** Wenn Sie das Dokument öffnen und den Inhalt lesen können, sind Sie startklar. Wenn die Nachricht in der Datei nicht korrekt angezeigt wird, kontaktieren Sie bitte den IT Service Desk.
- **iOS und Android:** Öffnen Sie den Anhang in der Sophos Secure Workspace App auf Ihrem Gerät. Der systemeigene Betrachter kann die Datei nicht öffnen, weil sie verschlüsselt ist. Wenn Sie Sophos Secure Workspace noch nicht auf Ihrem Mobilgerät installiert haben, kontaktieren Sie bitte den IT Service Desk.

Anwendungen

Die folgenden Anwendungen werden automatisch verschlüsselte Inhalte auf Ihrem Computer erzeugen. Wenn Sie unterschiedliche Anwendungen verwenden, um auf verschlüsselte Dateien zuzugreifen, werden Sie nur den verschlüsselten Inhalt sehen.

Windows:

- Adobe Reader
- MS Office 2010 (Excel, PowerPoint, Word)
- MS Office 2013 (Excel, PowerPoint, Word)
- MS Office 2016 (Excel, PowerPoint, Word)
- Office-Betrachter
- Foxit Reader für PDF

Mac OS X

- Adobe Reader
- Apple Produktivität (Keynote, Numbers, Pages, Preview)
- MS Office 2011 (Excel, PowerPoint, Word)
- MS Office 2016 (Excel, PowerPoint, Word)

Wie verhält es sich mit dem Senden von Dateien?

Beachten Sie, dass beim Senden von E-Mails an externe Empfänger die Datei in verschlüsselter Form gesendet wird. Das bedeutet, dass Ihr Empfänger den Inhalt nicht lesen kann. Ist der Inhalt nicht vertraulich, können Sie die Datei vor dem Senden entschlüsseln. Wenn es sich um vertraulichen Inhalt handelt oder Sie nicht sicher sind, erstellen Sie eine kennwortgeschützte Datei. Klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie "SafeGuard Dateiverschlüsselung". Wählen Sie dann entweder "Ausgewählte Datei entschlüsseln" oder "Kennwortgeschützte Datei erstellen".

Wenn Sie **Windows** verwenden und die Datei über **Microsoft Outlook** versenden, müssen Sie diese Schritte nicht manuell vornehmen. Wenn das System feststellt, dass Sie eine verschlüsselte Datei an einen externen Empfänger versenden, werden Sie zu einer Entscheidung aufgefordert, wie mit der Datei verfahren werden soll.

Was passiert mit Dateien, die auf unsere Web-Anwendungen hochgeladen werden?

Dateien, die Sie verschlüsselt hochladen, werden nicht entschlüsselt. Das bedeutet, sie bleiben sowohl in SharePoint als auch in allen anderen Web-Anwendungen stets verschlüsselt. Eventuell möchten Sie Dateien vor dem Hochladen manuell entschlüsseln. Beachten Sie, dass keine Vorschauen angezeigt werden und dass die Indexierung nicht funktioniert.

Probleme? Vorschläge?

Wenn Sie Probleme mit SafeGuard Enterprise oder generell mit Ihrem Computer haben seit die Verschlüsselung aktiviert wurde, erstellen Sie bitte ein IT-Ticket beim IT Service Desk.

Mit freundlichen Grüßen

6 Support

Vollständiger Release

Technische Unterstützung zu Sophos-Produkten erhalten Sie auf folgende Weise:

- Tauschen Sie sich in der Sophos Community unter community.sophos.com/ mit anderen Benutzern aus, die dasselbe Problem haben.
- Besuchen Sie die Sophos Support-Knowledgebase unter www.sophos.com/de-de/support.aspx.
- Lesen Sie die Produktdokumentation unter www.sophos.com/de-de/support/documentation.aspx.
- Stellen Sie eine Support-Anfrage unter https://secure2.sophos.com/de-de/support/contact-support/support-query.aspx.

7 Rechtliche Hinweise