SOPHOS
Security made simple.

# Next-Gen Encryption: Datenschutz mit Sophos

Fast täglich gibt es Schlagzeilen über neue Datenpannen in Unternehmen. Kein Unternehmen ist davor gefeit, unabhängig von Standort, Größe und Branche.

Wie können sich Unternehmen schützen und Datenverluste verhindern? Eine effektive Lösung muss dafür sorgen, dass geltende Datenschutzgesetze eingehalten werden. Gleichzeitig muss sie jedoch auch sicherstellen, dass die Mitarbeiter weiterhin effektiv arbeiten können.

Die Next-Gen-Encryption-Strategie von Sophos ist speziell auf diese Anforderungen ausgerichtet. In diesem Whitepaper erfahren Sie, wie eine effektive Next-Gen Encryption funktioniert und welche Vorteile Sie Ihnen bringt. Außerdem zeigen wir Ihnen, wie Sie Ihre Daten mit Sophos ganz einfach schützen können, ohne Ihre Mitarbeiter bei der Arbeit zu behindern.

# Die neue Realität

Unsere Arbeitsumgebung hat sich in den letzten Jahren komplett verändert. Wir arbeiten mit Geräten, die vor wenigen Jahren noch völlig unbekannt waren, und werden gleichzeitig mit immer raffinierteren Bedrohungen konfrontiert. Zwei entscheidende Veränderungen haben sich ganz besonders auf den Datenschutz ausgewirkt:

**Nicht das Gerät ist mobil, sondern Sie**

Ein durchschnittlicher Enduser besitzt heute drei Geräte. Früher wurden vor allem Desktop-PCs und gelegentlich auch Laptops genutzt. Inzwischen gehören auch Tablets und mobile Geräte zum Standardrepertoire. Nehmen Sie Ihre Mitarbeiter. Mit hoher Wahrscheinlichkeit haben sie einen Laptop und ein Mobiltelefon; manche nutzen vielleicht auch ein oder zwei Tablets.

Auf mobilen Geräten befinden sich oft genauso viele oder sogar noch mehr sensible Daten als auf einem Laptop. Sie gehen auch leichter verloren. Die potenzielle Angriffsfläche wächst also, weil Benutzer Unternehmensdaten auf mehr Geräten speichern.

Mitarbeiter von heute sind mobil und müssen auch unterwegs produktiv bleiben. Produktives Arbeiten wiederum ist untrennbar mit der Möglichkeit verknüpft, von beliebigen Geräten auf Unternehmensdaten zugreifen zu können – jederzeit und überall.

**Wissen Sie, wo Ihre Daten sind?**

Wissen Sie, wo sich Ihre Unternehmensdaten befinden? Sie sind auf Servern, Desktop-PCs, Laptops, mobilen Geräten, Tablets und Wechselmedien oder in der Cloud gespeichert. Sensible Unternehmensdaten befinden sich außerhalb der traditionellen Unternehmensgrenzen, weil es diese Unternehmensgrenzen schlichtweg nicht mehr gibt.

Wie definieren Sie eine Unternehmensgrenze für Ihre Daten, wenn die Daten sich auf einer Vielzahl von mobilen Geräten und in verschiedenen Speicherlösungen befinden? Diese Geräte sind oft nicht verwaltet oder befinden sich außerhalb eines Unternehmensnetzwerks. Und im Falle eines Cloudspeicher-Anbieters wissen Sie unter Umständen gar nicht, wo Ihre Daten genau liegen oder wer tatsächlich Zugriff erhält. Sie benötigen deshalb unbedingt eine Lösung, die Daten dort schützt, wo Benutzer sie abspeichern.

# Definition einer Next-Gen-Encryption-Strategie

Bei der Aufstellung unserer Next-Gen-Encryption-Strategie haben wir mehrere Punkte berücksichtigt. Bei all diesen Punkten kann es zu Datenverlusten oder -diebstählen kommen, die Auswirkungen auf Kunden haben, was rechtliche Konsequenzen nach sich ziehen kann. Folgende 5 Punkte haben wir definiert:

1. Verlorene oder gestohlene Geräte
2. Nutzung und Speicherung von Daten
3. Versehentliche Weitergabe von Daten
4. Hacking- oder Malware-Angriffe
5. Wunsch nach einfacher Bedienung

**Verlorene oder gestohlene Geräte**

Ein Benutzer hat heute durchschnittlich drei Geräte, von denen jedes leicht verloren gehen oder gestohlen werden kann. Mobiltelefone werden nicht selten auf dem Weg zur Arbeit im Zug vergessen und Laptops bleiben in der Eile versehentlich bei der Sicherheitskontrolle am Flughafen liegen. Viele Geräte haben heute Handtaschenformat und gehen schnell verloren. Eine Festplattenverschlüsselung ist zum Schutz von gespeicherten Daten sinnvoll und eine gute erste Verteidigungslinie. Sie reicht jedoch heute nicht mehr aus, um Unternehmensdaten zuverlässig zu schützen.

**Nutzung und Speicherung von Daten**

Mitarbeiter erstellen Daten in Form von Dokumenten, Präsentationen usw. Sie kopieren Dateien in Netzlaufwerke, auf USB-Sticks oder zu Cloudspeicher-Anbietern. Oft arbeiten mehrere Personen gemeinsam an Dateien und verschieben diese zwischen verschiedenen Geräten und Speicherorten. Hier muss sichergestellt sein, dass die Daten die gesamte Zeit geschützt sind.

**Versehentliche Weitergabe von Daten**

Wir sind alle nur Menschen. Und wir alle machen Fehler. Jeder von uns hat schon mal eine E-Mail geschrieben, die falsche Datei angehängt und abgeschickt (oder die richtige Datei an den falschen Empfänger geschickt). Es gibt viele Beispiele, bei denen menschliches Versagen zu Datenverlusten und -diebstählen führen kann. Web-Browser und E-Mail-Clients sind nützliche Tools zum produktiven Arbeiten und Austauschen von Daten, bergen jedoch die Gefahr, dass Unternehmensdaten versehentlich in der Cloud offengelegt oder an Unbefugte weitergegeben werden.

**Hacking- oder Malware-Angriffe**

Die Zahl der Malware-Angriffe auf Unternehmen steigt und immer häufiger erbeuten die Angreifer wichtige Kundendaten. Sollten Sie Opfer eines Malware-Angriffs werden, hilft eine Verschlüsselung. Denn sind die Daten verschlüsselt, kann die Malware mit ihnen nichts anfangen.

**Wunsch nach einfacher Bedienung**

Eine Verschlüsselung funktioniert am besten, wenn niemand bemerkt, dass sie überhaupt da ist. Sie schützt lautlos und ohne den Enduser zu beeinträchtigen. Denken Sie zum Beispiel an HTTPS. Das „S“ steht für „secure“ (sicher) und bedeutet, dass alle Kommunikationen zwischen Ihrem Browser und der Website verschlüsselt sind. Die meisten Benutzer bemerken jedoch gar nicht, dass die URL der Seite, die sie besuchen, anders aussieht.

Eine Verschlüsselung muss bedienerfreundlich sein – sowohl für den Administrator als auch für den Enduser – nur so lässt sich ein hoher Akzeptanzgrad erreichen. Ist die Bedienung einer Verschlüsselung zu kompliziert, werden Ihre Mitarbeiter sie mit hoher Wahrscheinlichkeit nicht nutzen – damit bleibt das Risiko für Datenverluste.

# Die neue Sophos Next-Gen Encryption

Die Next-Gen-Encryption von Sophos basiert auf zwei Grundsätzen:

1. Alle Daten, die ein Enduser erstellt, sind wichtig und müssen geschützt (verschlüsselt) werden. Hierunter verstehen wir „immer aktive" Verschlüsselung oder Standardverschlüsselung.

2. Eine Verschlüsselung sollte permanent sein, egal, wo eine Datei sich befindet oder wohin sie kopiert oder verschoben wird.

Die Verschlüsselung von Daten gilt weithin als beste Datenschutzmethode. Egal,ob ein Benutzer ein Dokument erstellt, in dem er seine neue Patentidee erklärt, oder eine Tabellenkalkulation anlegt, um eine neue Geschäftsidee zu begründen – es handelt sich um wichtige Daten, die automatisch und transparent verschlüsselt werden müssen. Ein Benutzer sollte dabei nicht selbst entscheiden müssen, ob eine Datei wichtig genug ist, um eine Verschlüsselung zu rechtfertigen. Tatsächlich müssen sich Benutzer nicht mal darüber bewusst sein, dass Daten verschlüsselt sind. So können sie weiterhin produktiv und wie gewohnt arbeiten, während ihre Daten geschützt bleiben.

Sobald eine Datei verschlüsselt ist, muss sie dies auch bleiben. Egal, was mit der Datei geschieht – ob sie verschoben, kopiert oder umbenannt wird bzw. auf dem Gerät verbleibt oder nicht – die Verschlüsselung muss permanent sein. Wenn ein Benutzer versehentlich eine Datei verliert, geht diese in verschlüsselter Form verloren und ist demzufolge für Unbefugte wertlos/unleserlich.

**Welche Rolle spielt DLP?**

Beim Thema Datenschutz denken wir oft an Data Loss/Leakage Prevention (DLP). DLP und Verschlüsselung sind seit jeher eng miteinander verknüpft. DLP ist eine leistungsstarke Technologie. Viele Unternehmen scheitern jedoch daran, ihre DLP-Strategie erfolgreich umzusetzen, obwohl sie bereits viel Geld und Zeit in das Projekt investiert haben. Das Problem ist die Komplexität der Aufgabe. Es müssen Regeln für Daten vorhanden sein, die Sie vielleicht noch gar nicht erstellt haben. Ein häufiges Problem besteht zudem darin, dass Administratoren die Regeln zu streng gestalten und anschließend mit einer Flut von False Positives zu kämpfen haben. Oft lockern Administratoren die Regeln dann und Daten können trotz DLP-System aus dem Unternehmen gelangen. Bei Sophos revolutionieren wir DLP, indem wir die Notwendigkeit abschaffen, Daten klassifizieren zu müssen. Diese Vereinfachung hilft sowohl dem Enduser als auch dem Administrator.

Das soll nicht heißen, dass DLP unwichtig ist. DLP hat bei Next-Gen Encryption nach wie vor seine Daseinsberechtigung. DLP sollte jedoch die Ausnahme und nicht die Regel sein. Wenn ein Benutzer Daten entschlüsseln möchte, ist dies eine bewusste Entscheidung, den Schutz einer Datei herabzusetzen. In dieser Situation ist eine optionale Ausführung von DLP-Regeln sinnvoll. Wenn keine Auffälligkeiten erkannt werden, darf der Benutzer die Datei entschlüsseln, da diese keine als sensibel eingestuften Daten enthält. Werden jedoch Auffälligkeiten entdeckt, wird die Anfrage auf Entschlüsselung der Datei abgelehnt. Dieser Ansatz ist ausfallsicher, um zu gewährleisten, dass Dateien verschlüsselt bleiben. Zusätzlich wird jede Anfrage zur Entschlüsselung einer Datei überwacht und protokolliert.

Dieser Ansatz führt zu einer erheblichen Vereinfachung von DLP sowie zur Reduzierung der Verarbeitungsanforderungen, da die Anwendung von DLP-Regeln zur Ausnahme wird (wird nur bei der Entschlüsselung von Daten verwendet).

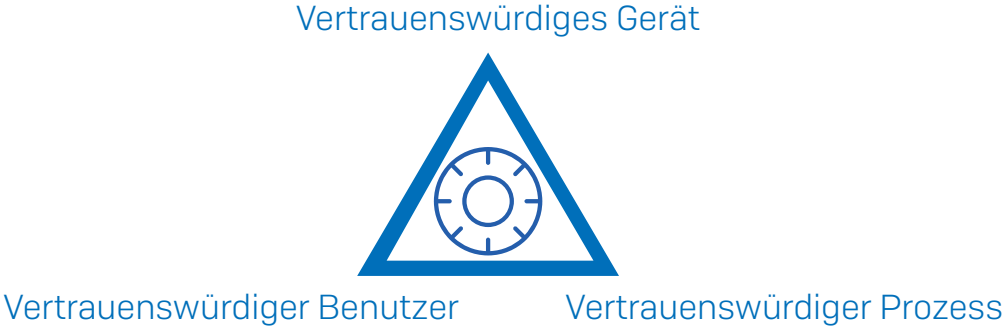
# Synchronized Encryption

Wenn wir davon ausgehen, dass alle Daten eines Benutzers verschlüsselt sind, besteht der nächste Schritt darin, die Schlüssel zu schützen, mit denen die Daten verschlüsselt wurden.

Die Kernidee von Schlüsseln ist, dass nur vertrauenswürdige Geräte, Anwendungen und Benutzer Zugriff auf verschlüsselte Daten erhalten.

Um dies zu erreichen, kombiniert Sophos das Know-how und die Funktionalität von Sophos Endpoint mit Sophos SafeGuard Encryption (SafeGuard) und verwandelt Verschlüsselung damit in eine Threat-Protection-Technologie. Das Endpoint-Produkt tut das, was es schon immer gut konnte: Es ermittelt den Sicherheitsstatus des betreffenden Geräts und entscheidet, ob die ausgeführten Prozesse vertrauenswürdig sind. Auch das Datenschutzprodukt tut, was es am Besten kann: Daten verschlüsseln und den Zugriff auf Schlüssel schützen.

Um zu entscheiden, wann Schlüssel freigegeben werden sollten und wann der Zugriff auf verschlüsselte Inhalte gewährt werden darf, triangulieren und synchronisieren wir Benutzeridentität, Gerät und Anwendung/Prozess:




*Um als vertrauenswürdig eingestuft zu werden und auf verschlüsselte Daten zugreifen zu können, muss der Benutzer ein vertrauenswürdiges Gerät verwenden, ein vertrauenswürdiger Benutzer sein und für den Datenzugriff einen vertrauenswürdigen Prozess bzw. eine vertrauenswürdige Anwendung nutzen.*

Alle drei dieser Bedingungen müssen erfüllt sein, bevor der Zugang zum Schlüssel freigegeben wird und Daten eingesehen werden können.

In fast allen Fällen ist ein legitimer Unternehmens-Enduser in der Lage, mit einem vertrauenswürdigen Gerät (z. B. einem vom Unternehmen ausgegebenen Gerät) und vertrauenswürdigen Anwendungen transparent auf Daten zuzugreifen. Sollten eine oder mehrere der obengenannten Bedingungen nicht erfüllt sein, wird der Schlüsselzugriff verweigert. Der Enduser kann in diesem Fall zwar die verschlüsselte Datei, nicht jedoch den Inhalt der Datei sehen. So kann datenstehlende Malware eine geschützte Datei zwar abschöpfen, mit dieser ohne den Zugriffsschlüssel jedoch nichts anfangen.

**Vertrauenswürdiges Gerät**

Die Vertrauenswürdigkeit eines Geräts lässt sich auf viele verschiedene Arten ermitteln. Zum Beispiel, indem festgestellt wird, ob die geeigneten Sophos-Produkte installiert sind. Oder indem der Sophos-Endpoint-Agent das System überprüft und ihm einen „Healthy State“ (einen grünen Heartbeat™-Status) bescheinigt.

Ein vertrauenswürdiges Gerät kann auch ein mobiles Gerät sein, das von der EMM-Lösung des Unternehmens verwaltet wird und demzufolge mit den Sicherheitsrichtlinien des Unternehmens konform ist. Gleichzeitig kann ein Administrator ein System auch explizit als nicht vertrauenswürdig einstufen (z. B. ein von einem externen Mitarbeiter genutztes Gerät).

Wenn sich ein Windows- oder Mac-Laptop in einem aktiven Infektionszustand befindet, da der Endpoint gerade Malware entfernt, sollte das System aller Wahrscheinlichkeit nach nicht als vertrauenswürdig eingestuft werden. Ein mobiles Gerät (z. B. iPhone oder Android), das gegen die Unternehmensrichtlinien verstößt (z. B. ein Gerät mit Jailbreak oder ohne Passwort zur Bildschirmsperre), sollte ebenfalls nicht als vertrauenswürdig kategorisiert werden.

**Vertrauenswürdiger Benutzer**

Genau wie es mehrere Methoden gibt, um zu ermitteln, ob ein Gerät als vertrauenswürdig eingestuft werden sollte, gibt es auch viele verschiedene Methoden, um festzustellen, ob ein Benutzer als vertrauenswürdig gelten sollte. Die Vertrauenswürdigkeit kann auf Grundlage der Identität oder einfach dadurch ermittelt werden, dass der Benutzer sich auf seinem System erfolgreich anmelden konnte. Es gibt Anwendungsfälle, bei denen Benutzer trotz erfolgreichem Login auf ihrem Gerät keinen Zugriff auf verschlüsselte Daten erhalten sollten (z. B. wenn ein Mitarbeiter das Unternehmen verlässt).

**Vertrauenswürdiger Prozess**

Sophos Endpoint spielt eine zentrale Rolle bei der Entscheidung, ob ein Prozess vertrauenswürdig ist oder nicht.

Generell vertraut die interne Logik keinen PUAs (potenziell unerwünschten Anwendungen), Malware-Elementen, Viren, Web-Browsern und E-Mail-Clients. Es gibt jedoch auch andere Arten von Anwendungen (z. B. Torrent-Programme), denen Unternehmen eventuell instinktiv nicht vertrauen und denen sie demzufolge keinen Zugriff auf verschlüsselte Daten gewähren. Web-Browser und E-Mail-Clients sind grundsätzlich nicht vertrauenswürdig, da Enduser über sie versehentlich Daten austauschen oder verlieren können. Auf diese Weise wird menschlichen Fehlern vorgebeugt.

Warum sprechen wir über Prozesse und nicht über Anwendungen? Das primäre Ziel besteht darin, dem Enduser ein produktives Arbeiten zu ermöglichen. Wenn ausschließlich der schädliche Prozess blockiert wird, können alle vertrauenswürdigen Prozesse weiterhin ungehindert ausgeführt werden.

Sehen wir uns nun drei Beispiele von Prozessen an, bei denen es sich nicht um Malware/Viren handelt. Die Frage ist, ob diese Prozesse als vertrauenswürdig eingestuft werden können.

1. **Notepad**

   Notepad ist eine eigenständige, einfache Anwendung. Sie ist vertrauenswürdig, weil sie einfach ist und keine Schadaktivitäten enthält. Da Notepad als vertrauenswürdig eingestuft wird, kann diese Anwendung auf Schlüssel zugreifen. Auf diese Weise können mit Notepad erstellte Dokumente standardmäßig verschlüsselt und verschlüsselte Klartextdokumente angezeigt werden.

2. **Internet Explorer**

   Internet Explorer ist für seine Sicherheitslücken bekannt und stellt einen beliebten Übertragungsweg von Malware auf Geräte dar. Daher wird Internet Explorer standardmäßig als nicht vertrauenswürdig eingestuft. Weil Internet Explorer nicht vertrauenswürdig ist, erhält er keinen Schlüsselzugriff und kann demzufolge nur auf Dateien in ihrer verschlüsselten Form zugreifen. Er kann Inhalte weder öffnen noch anzeigen, kann eine verschlüsselte Datei jedoch in einen Cloud-Speicher hochladen.

3. **Microsoft Word**

   Microsoft Word befindet sich in einer Grauzone zwischen vertrauenswürdig und nicht vertrauenswürdig. Word kann sich völlig unbedenklich verhalten und vertrauenswürdig sein. Wenn ein Benutzer also mit Word ein Dokument erstellt, kann dieses standardmäßig verschlüsselt werden. Der Benutzer kann einfach auf verschlüsselte Dateien doppelklicken und diese anschließend lesen und bearbeiten. Der Prozess ist komplett transparent. Dies liegt daran, dass Word als vertrauenswürdig gilt und auf Schlüssel zugreifen darf, um im Hintergrund Verschlüsselungs-/Entschlüsselungsprozesse zu vollziehen. Word kann jedoch auch mit einer Art Macro-Virus infiziert sein. Es ist dann nicht mehr vertrauenswürdig genug, um auf den Schlüssel zugreifen zu dürfen, und kann verschlüsselte Daten demzufolge nicht lesen.

Die drei Beispiele zeigen deutlich, wie wichtig eine Synchronized Encryption ist, damit die Integrität kontinuierlich überprüft und sichergestellt werden kann.

**Kontinuierliche Kontrolle der Integrität, bevor Vertrauen gewährt wird**

Vorwiegend möchten Sie erreichen, dass Ihre Datenschutztechnologie den Sicherheitsstatus, die Integrität und die Vertrauenswürdigkeit der Systemanwendung/des Systemprozesses konstant kontrolliert. Das Ziel besteht darin, Endusern ein produktives Arbeiten zu ermöglichen und gleichzeitig die Sicherheit der Daten zu gewährleisten. Wie bereits beschrieben, können als nicht vertrauenswürdig eingestufte Prozesse nur auf Dateien in verschlüsselter Form zugreifen, nicht jedoch auf den zur Entschlüsselung erforderlichen Schlüssel. In den meisten Fällen bemerken die Benutzer davon gar nichts. Wenn der Prozess jedoch schädlich ist (z. B. Malware), sollte er selbstverständlich überhaupt nicht ausgeführt werden. Falls sich Ihr System zudem im Zustand einer aktiven Infektion befindet, darf das System nicht als vertrauenswürdig eingestuft werden. Prozessvertrauen ist die erste Reaktion auf Integrität, der übergreifende Sicherheitsstatus des Systems spielt jedoch bei der Reaktion auf die Integrität ebenfalls eine Rolle.

Widmen wir uns nun wieder dem Konzept der Benutzerproduktivität. Sie müssen verhindern, dass nicht vertrauenswürdige Prozesse auf Klartextdaten zugreifen, und deren Ausführung unterbinden. Wenn Sie jedoch beispielsweise zwei Word-Dokumente geöffnet haben – das erste mit wichtiger Dokumentation, an der Sie gerade arbeiten, und das zweite eine Datei, die Ihnen ein Freund oder Kollege geschickt hat – und sich das zweite Dokument als schädlich herausstellt, sollte nur der zweite Word-Prozess blockiert werden. Der Benutzer muss das erste Word-Dokument weiter produktiv bearbeiten können.

Sollte das System des Benutzers mit einem oder mehreren Malware-Elementen infiziert worden sein, die gerade entfernt werden, kann die Synchronized Encryption als letzte Möglichkeit die lokalen Kopien der Schlüssel vorübergehend entziehen. Mit einer Schlüsselsperrung wäre sichergestellt, dass auf dem System keine Dateien oder Daten mehr entschlüsselt werden können. Dies beschränkt die Produktivität des Endusers, da er nicht mehr auf verschlüsselte Daten zugreifen kann, aber genau das ist der Punkt. Möchten Sie, dass ein Benutzer (und die von ihm genutzten Anwendungen/Prozesse) Zugriff auf verschlüsselte Daten hat, obwohl sein System infiziert ist? Mit Sicherheit nicht. Sobald die Malware-Infektion(en) beseitigt und der Sicherheitsstatus des Systems als unbedenklich bestätigt ist, werden die Schlüssel wieder freigegeben und der Benutzer kann weiterarbeiten.

**Ist ein nicht vertrauenswürdiger Prozess etwas Schlechtes?**

Ist ein nicht vertrauenswürdiger Prozess automatisch gefährlich? Nicht zwangsläufig. Es gibt viele Anwendungsfälle, bei denen Sie einem Prozess Zugang zu Dateien gewähren möchten – jedoch nur verschlüsselt. Benutzer können beispielsweise einen E-Mail-Client wie Outlook verwenden, um einen Anhang zu senden. Der Outlook-Client ist nicht vertrauenswürdig, kann jedoch auf Dateien in ihrer verschlüsselten Form zugreifen, um ein Dokument an eine E-Mail anzuhängen und zuzustellen. Sobald das Dokument jedoch beim Empfänger eintrifft, ist Outlook zum Öffnen der Datei auf eine vertrauenswürdige Anwendung wie Word oder Excel angewiesen. In den Augen des Endusers ist der Prozess vollständig transparent. Gleichzeitig sind die Anhänge verschlüsselt und während ihrer Übertragung demzufolge geschützt.

Dies macht auch deutlich, warum sich das Sophos-Synchronized-Encryption-Konzept vom Application Whitelisting unterscheidet. Nur weil Sie die Ausführung einer Whitelist-Anwendung erlauben, muss das nicht bedeuten, dass diese auch Zugriff auf verschlüsselte Daten erhalten darf. Mit Synchronized Encryption entscheiden Sie, ob eine vertrauenswürdige ausgeführte Anwendung vertrauenswürdig genug ist, um eine Klartextversion der verschlüsselten Daten zu sehen.

**Synchronized Encryption ohne Sophos Endpoint**

Um die Vorteile von Sophos Synchronized Encryption vollständig nutzen zu können, benötigen Kunden sowohl Sophos-Endpoint- als auch Sophos-SafeGuard-Produkte. Was geschieht jedoch, wenn das Sophos-Endpoint-Produkt nicht vorhanden ist? Dieselbe Logik gilt auch hier: Allerdings erfolgt die Überprüfung des Systemstatus und der Prozessvertrauenswürdigkeit dann nicht dynamisch, sondern statisch. Das SafeGuard-Produkt kann keine Malware erkennen. Der Sicherheitsstatus des Systems muss daher auf andere Weise festgestellt werden. Die Prozessvertrauenswürdigkeit wird in diesem Fall auf Grundlage einer Liste explizit benannter Prozesse ermittelt, die der Administrator als vertrauenswürdig definiert hat. Alle Prozesse, die nicht auf der Liste stehen, werden standardmäßig als nicht vertrauenswürdig eingestuft.

# Möglichkeiten der Zusammenarbeit mit Next-Gen Encryption

Enduser müssen zusammenarbeiten – sowohl innerhalb als auch außerhalb des Unternehmens – um ihr Tagesgeschäft zu erledigen und produktiv arbeiten zu können. Next-Gen Encryption stellt sicher, dass alle von den Endusern erstellten Daten geschützt sind und nur von vertrauenswürdigen Instanzen aufgerufen werden können. Wie funktioniert die Zusammenarbeit in diesem Fall? Das Hauptaugenmerk liegt nach wir vor darauf, Benutzern weiterhin ein produktives Arbeiten zu ermöglichen, ohne dass diese ihre gewohnten Arbeitsabläufe ändern müssen. Sehen wir uns die zwei Kategorien des Zusammenarbeitens – interne und externe Zusammenarbeit – einmal genauer an.

**Interne Zusammenarbeit**

Die interne Zusammenarbeit gestaltet sich bei der Implementierung einer Next-Gen Encryption besonders einfach und nahtlos. Alle Benutzer innerhalb eines Unternehmens haben Zugang zu den Schlüsseln. Alle Daten, die erstellt werden, sind verschlüsselt. Sie werden verschlüsselt ausgetauscht und jeder kann auf sie zugreifen.

1. **Ein Mitarbeiter erstellt ein Word-Dokument und speichert es.** Er möchte, dass eine Kollegin ihm Feedback zu dem Dokument gibt. Sobald er das Dokument speichert, wird es automatisch verschlüsselt (Standard-Verschlüsselung). Er muss nichts Spezielles tun, um das Word-Dokument zu verschlüsseln.
2. **Der Mitarbeiter öffnet Outlook und erstellt eine neue E-Mail,** die er an seine Kollegin adressiert. Er hängt seine Word-Datei wie gewohnt an die E-Mail an. Er schreibt seine Nachricht und klickt auf „Senden". Outlook ist ein E-Mail-Client und wird daher im Allgemeinen nicht als vertrauenswürdig eingestuft. Da Outlook nicht vertrauenswürdig ist, ist eine der drei Voraussetzungen nicht gegeben (kein vertrauenswürdiger Prozess). Wenn Outlook das Word-Dokument liest, um es anzuhängen, wird die Datei in verschlüsseltem Zustand angehängt.
3. **Die E-Mail wird dann an die Kollegin gesendet.** Diese erhält die E-Mail und öffnet sie. Der Dateianhang in der E-Mail ist dabei an allen Orten die gesamte Zeit verschlüsselt: Im "Gesendet"-Ordner des Mitarbeiters, im Posteingang der Kollegin und während des Sendevorgangs.
4. **Die Kollegin doppelklickt auf das Word-Dokument** in der E-Mail und öffnet die Datei problemlos in Word, wo sie die Datei lesen und Kommentare einfügen kann. Outlook ist nicht vertrauenswürdig. Wenn es das Dokument an einem temporären Speicherort speichert, bleibt die Datei daher weiterhin verschlüsselt. Outlook startet anschließend Word, um die gerade erstellte temporäre Datei zu öffnen. Word ist vertrauenswürdig und hat Zugriff auf den Schlüssel. Da die Kollegin, ihr Gerät und MS Word vertrauenswürdig sind, kann Word das Dokument entschlüsseln, lesen und es der Kollegin im Klartext präsentieren.

   Wenn die Kollegin die E-Mail auf einem mit Sophos Mobile Control geschützten mobilen Gerät liest, kann sie den verschlüsselten Anhang zudem im Secure WorkSpace (einem verschlüsselten Container) speichern. Dieser Container nutzt denselben Schlüssel, sodass sich die Kollegin den Inhalt sicher anzeigen lassen kann.

Keiner der beiden musste sein gewohntes Verhalten ändern und alle Interaktionen zwischen den beiden sind verschlüsselt. Sie profitieren von einem nahtlosen Workflow und können problemlos zusammenarbeiten.

# Externe Zusammenarbeit

Die externe Zusammenarbeit verändert sich, wenn Ihr gesamter Datenbestand verschlüsselt ist. Benutzer können auf zwei Arten extern zusammenarbeiten:

1. Passwortgeschützt (verpackt in einer HTML5-Datei)
2. Entschlüsselt

### Externe Zusammenarbeit mit einer entschlüsselten Datei

Es gibt durchaus Fälle, in denen der Austausch von Daten in entschlüsselter Form sinnvoll ist. Zum Beispiel, wenn es sich um öffentliche Informationen wie eine Broschüre handelt. Öffentliche Informationen sollten für jeden zugänglich sein. Eine Entschlüsselung solcher Daten ist also unbedenklich und explizit gewollt. Die Entschlüsselung von Daten ist die einzige Situation, in der die Next-Gen Encryption für den Enduser sichtbar wird. Der Benutzer muss nämlich bestätigen, dass er die Datei wirklich entschlüsseln möchte.

Der Benutzer trifft hiermit die bewusste Entscheidung, die Datei vor dem Senden zu entschlüsseln. Wie oben beschrieben, kann der Inhalt der Datei anschließend optional von der DLP-Technologie geprüft werden und wird entschlüsselt, falls keine Auffälligkeiten festgestellt werden. Darüber hinaus ist die Verschlüsselung, oder in diesem Fall die Entschlüsselung, permanent. Der gesamte Vorgang wird protokolliert und überwacht, sodass der Administrator erkennen kann, wenn Mitarbeiter sich nicht richtlinienkonform verhalten. Sobald die Datei entschlüsselt ist, kann der normale Benutzer-Workflow fortgesetzt werden.

**Externe Zusammenarbeit mit passwortgeschützter Datei**

Was geschieht, wenn Sie einen Vertrag mit einem externen Empfänger sicher austauschen möchten, dem Empfänger jedoch ermöglichen müssen, diesen zu entschlüsseln und zu verwenden, ohne dass Sie wissen, ob auf Seiten des Empfängers eine Verschlüsselungssoftware vorhanden ist?

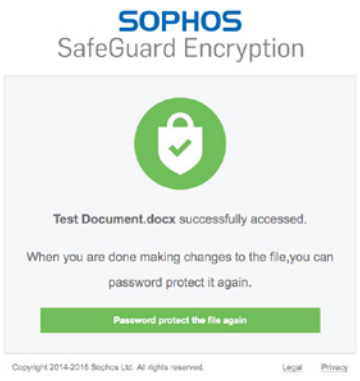
Der Benutzer kann einfach eine passwortgeschützte Datei erstellen und ein Passwort festlegen. Die Software verschlüsselt das Vertragsdokument (z. B. „Vertrag.doc“) mit dem vom Benutzer zugewiesenen Passwort erneut und verpackt es in einem HTML5-Wrapper. Auf diese Weise wird eine Datei namens „Vertrag.html“ erstellt. Das Passwort muss dem Empfänger mitgeteilt werden. Das Ergebnis ist eine einzelne HTML-Datei, die von HTML5-fähigen Browsern und jedem Betriebssystem interpretiert werden kann. Die HTML-Datei besteht aus drei verschiedenen Komponenten:

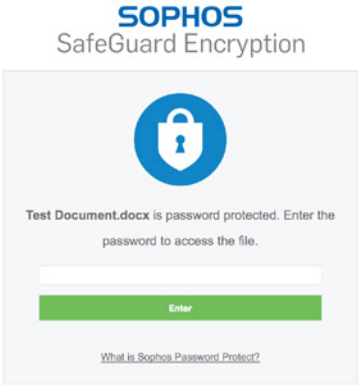
1. Der Darstellungsschicht (das, was dem Empfänger in seinem Web-Browser angezeigt wird, wenn er die Datei öffnet)
2. Code zur Entschlüsselung des angehängten Payloads
3. Der verschlüsselten Datei (in diesem Fall „Vertrag.doc“)

Der Benutzer schickt anschließend die HTML-Datei „Vertrag.html“ und nicht die Word-Datei „Vertrag.doc“ an den Empfänger. Wenn der Empfänger in seinem E-Mail-Client auf die HTML-Datei doppelklickt, öffnet sich sein Browser und er wird aufgefordert, das Passwort einzugeben. Vorausgesetzt, dass das Passwort korrekt eingegeben wird, führt der Browser den Code zum Entschlüsseln der Datei aus und diese wird anschließend lokal und unverschlüsselt auf dem Computer des Empfängers gespeichert.

Auf diese Weise kann die vertrauliche Datei verschlüsselt versendet und nahtlos entschlüsselt werden, wenn der Empfänger die Datei öffnet.

Falls der Empfänger eine aktualisierte Datei zurücksenden möchte, kann der HTML-Wrapper auch als Container genutzt werden. Der Empfänger kann die Datei einfach aktualisieren und die aktualisierte Datei wieder im HTML-Bildschirm ablegen. So wird eine bidirektionale, sichere Kommunikation mit einem externen Benutzer ermöglicht, der selbst keine Sophos SafeGuard Encryption installiert hat.




**Mehr Komfort für Ihre Benutzer**

Um Ihren Endusern das Leben zu erleichtern, bietet Sophos Features wie z. B. unser Outlook-Plugin an, das erkennen kann, wenn E-Mails mit einem Dateianhang an einen Empfänger außerhalb des Unternehmens gesendet werden. Der Benutzer kann in diesem Fall informiert werden, dass er gerade dabei ist, eine verschlüsselte Datei zu versenden, und ihn auffordern, die gewünschte Option zur externen Zusammenarbeit auszuwählen sowie anschließend die geeigneten Maßnahmen zu treffen. Alternativ kann der Administrator über eine Richtlinie auch eine Standardaktion festlegen, die automatisch ausgeführt wird.

# Plattformübergreifender Datenzugriff

Um Endusern weiterhin ein produktives Arbeiten zu ermöglichen, muss die Next-Gen-Encryption-Funktionalität auf allen Geräten aktiv sein, die von Endusern in der Regel genutzt werden. Sie funktioniert auf Windows, OS X, iOS und Android.

Wir haben bereits erwähnt, dass Benutzer heute durchschnittlich drei Geräte im Einsatz haben. Sollte der Windows-Computer des Benutzers mit Malware infiziert, gesperrt oder als nicht vertrauenswürdig eingestuft sein, kann der Benutzer immer noch mit seinem Mac oder iPad arbeiten und produktiv bleiben – egal, ob im Büro oder unterwegs. Ein kompromittiertes Gerät ist ärgerlich, aber der Benutzer kann in diesem Fall einfach auf ein anderes Gerät ausweichen.

# Next-Gen Threat and Data Protection

Mit Sophos können Kunden ihre Sicherheit noch weiter optimieren, indem sie Next-Gen Encryption mit unserem breiteren Synchronized-Security-Angebot kombinieren. Wenn ein Kunde Sophos Endpoint, eine Sophos UTM/Firewall und Sophos SafeGuard nutzt, arbeiten alle drei Lösungen zusammen und erkennen und entfernen Bedrohungen nicht nur effektiver. Sie verhindern auch, dass Bedrohungen auf verschlüsselte Daten zugreifen können. Sie erhalten Next-Generation Protection für Ihr Unternehmen, die ihrem Namen gerecht wird.

# Fazit

Next-Gen Encryption definiert Datenschutz komplett neu. Eine immer aktive Verschlüsselung anstelle der herkömmlichen Datei-/Ordnerverschlüsselung nimmt Endusern die Entscheidung ab, welche Daten wichtig sind und verschlüsselt werden müssen. Die Enduser können Dateien transparent und automatisch verschlüsseln/entschlüsseln und ihre gewohnten Arbeitsabläufe beibehalten. Synchronized Encryption schützt Daten vor Bedrohungen, indem sie infizierten Systemen Schlüssel entzieht und den Zugriff auf nicht vertrauenswürdige und schädliche Anwendungen verweigert. Auf diese Weise wird sichergestellt, dass Benutzer produktiv arbeiten können, ohne die Sicherheit Ihrer Daten und Ihres Unternehmens zu gefährden.

*Mehr als 100 Millionen Anwender in 150 Ländern vertrauen auf Sophos. Wir bieten den besten Schutz vor komplexen IT-Bedrohungen und Datenverlusten. Unsere umfassenden Sicherheitslösungen lassen sich einfach bereitstellen, bedienen und verwalten. Dabei bieten sie die branchenweit niedrigste Total Cost of Ownership. Das Angebot von Sophos umfasst preisgekrönte Verschlüsselungslösungen, Sicherheitslösungen für Endpoints, Netzwerke, mobile Geräte, Server, E-Mails und Web. Dazu kommt Unterstützung aus den SophosLabs, unserem weltweiten Netzwerk eigener Analysezentren. Weitere Informationen unter www.sophos.de*

Sales DACH (Deutschland, Österreich, Schweiz):
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de



18.10.2016 WP-DE (NP)

SOPHOS