SOPHOS
Security made simple.

次世代型暗号化 - ソフォスのアプローチ

情報漏えいは、事業規模や業種、場所にかかわらず、あらゆる企業のリスクとなっており、その懸念は高まり続けています。Privacy Rights Clearing House の報告によると、2014年に発生したデータ漏えいのうち半数はハッキングやマルウェアによるもので、第 2位にランクインしたのは、過失による流出でした (16%)。

この事実に加え、業務環境はここ数年間で大きく変化しています。今日のビジネスにはデータ漏えい対策のほか、さまざまなデータ保護規制に沿ったデータの取り扱いが求められる一方、競争の激しい今日のビジネス環境では、業務の効率性も追求しなくてはなりません。

ソフォスの次世代型暗号化ソリューションは、特にこのようなニーズに合わせて設計されました。このホワイトペーパーでは、ソフォスの次世代型暗号化とその仕組みを概説するとともに、あらゆる規模の企業に対応するソフォスのソリューションを使用して、業務効率を損なうことなく、シンプルに企業データを保護する方法について説明していきます。

最新動向

今日の業務環境は、5年～10年前と比べて大きく変わっています。特に、デバイスや脅威を巡る状況は著しい変化を遂げました。ここでは、これらの変化のうち、データ保護に大きな影響を及ぼした 2点について考察します。

モバイルなのは、デバイスではなく従業員

企業の従業員は、平均して 3つのデバイスを所有しています。以前は、デスクトップに加えてノート PC が時々使用されるくらいでしたが、現在では、タブレットやその他のモバイルデバイスの使用が一般的になっています。貴社の従業員の例を考えてみてください。ノート PC や携帯電話を所有しているのはもちろんのこと、タブレットを 2つ以上所有しているケースも珍しくないでしょう。

モバイルデバイス上には、大抵、ノート PC に劣らない量の機密情報が保存されています。また、ノート PC と同様、紛失しやすいという特徴があります。そのため、従業員が所有するデバイスの数が増えるに従って、企業データが攻撃に晒される可能性も増します。

モバイルワーカーが増えている現在、これらの従業員は移動中でも業務をこなす必要に迫られています。業務を効率良くこなせるかどうかは、究極的には、場所や時間、デバイスを問わず、いつどこからでも企業データにアクセスできるかどうかにかかっています。

企業データの保存場所

企業データがどこに保存されているか把握していますか？その保存場所は、サーバーからデスクトップ、ノート PC、モバイルデバイス、タブレット、リムーバブルメディア、クラウドまで、多岐にわたります。企業の機密データは、企業の従来のネットワーク境界線を越えて遍在しています - これは、そもそも「企業のネットワークの境界線」という概念が消滅したからです。

企業データが多様なモバイルデバイスやストレージに保存されている状況においては、企業のネットワークの境界線を定義することは困難です。これらのデバイスは、まったく管理下にないか、企業ネットワークの外にあることがほとんどです。クラウドストレージに至っては、企業データが物理的にどこに保存されているのか、誰がアクセスすることができるのかも不明です。こういうった状況においては、データの保存場所に関わらず、データを保護する手段が必要になってきます。

次世代型暗号化戦略の定義

ソフォスでは、次世代型暗号化戦略を定義するにあたり、企業においてデータ漏えいが起こったと想定し、その原因や影響をいくつかの分野にわたって考察しました。その際、特に以下のポイントに着目しました。

1. デバイスが紛失や盗難に遭った場合の影響
2. 従業員によるデータの扱い
3. 過失によるデータ流出
4. ハッキングやマルウェア攻撃
5. 使いやすさ

標的型攻撃は、マルウェアやフィッシングなどを使った無差別攻撃とは異なり、中小企業を狙う可能性は非常に低いため、このリストからは省きました。標的型攻撃は膨大な労力を要するため、Sony や Target 社などの大企業や、非常に特殊な機密情報を抱える組織を除いては、犯罪組織に標的にされることは少ないでしょう。

デバイスが紛失や盗難に遭った場合の影響

従業員が平均して所有するデバイスの数は 3つで、これらはどれも紛失したり盗難に遭いやすいものです。通勤電車に携帯電話を置き忘れたり、空港のセキュリティチェックで慌ててノート PC を置き去りにするなどのミスが考えられます。デバイスは小さく、アクシデントを免れることはできません。データを保護するためには、ディスクを完全に暗号化することが、有効かつ基本的な防御策と言えます。しかし、今日の従業員がどのように企業データを使用しているかという点を見ていくと、ディスクの暗号化だけでは十分ではないことがわかります。

従業員によるデータの扱い

まずは、従業員がデータをどのように使用しているのかを、1時間だけでも観察してみましょう。従業員は、文書やプレゼン資料にデータを挿入し、これらのファイルをネットワーク上の共有フォルダや、USB スティック、クラウドストレージにコピーしたりします。業務にはファイルがつきもので、これらのファイルはさまざまなデバイスやストレージ間でやりとりされます。このようなシチュエーションでは、データを保護することは必須であると言えます。

過失

従業員は皆、人間であり、人は必ずミスを犯します。メールに間違った添付ファイルを付けて送信してしまうこともあれば、間違った宛先に送信してしまうこともあるでしょう。過失によるデータ流出の例は、数限りなくあります。Web ブラウザやメールクライアントは、効率良く仕事をこなしたり、データを共有するために欠かせないツールですが、同時に、企業データを誤ってクラウド上にコピーしてしまったり、誤った宛先に送ってしまうといったアクシデントの原因にもなります。

ハッキングやマルウェア攻撃

2014年、Privacy Rights Clearinghouse が行ったデータ漏えいの種別に関するレポートによると、データ漏えいの 51% がハッキングやマルウェアによるものでした。マルウェアは増え続けているだけでなく、その巧妙性も増しています。この分類には、無差別なデータ搾取も含まれます。マルウェアによるデータアクセスは必ず阻止する必要があります。

使いやすさ

暗号化技術は、エンドユーザーに存在を気付かれないものが最適です。つまり、エンドユーザーにまったく負荷を与えることなく、バックグラウンドでデータを保護するようなものです。たとえば、HTTPS がそうです。「S」は Secure (安全) を表し、ブラウザと Web サイト間のやりとりがすべて暗号化されていることを意味しますが、ほとんどのユーザーは URL にこの S が付いていても気が付きません。

暗号化技術は、エンドユーザーはもちろんのこと、管理者にとっても使いやすいものであることが、広く受け入れられるかどうかの鍵を握ります。

ソフォスの次世代型暗号化ソリューションの紹介

ソフォスの次世代型暗号化ソリューション は、以下の 2つの前提に基づいています。

1. 従業員が作成するデータはすべて重要なものであり、保護 (暗号化) する必要がある。これは、「常時オン」型の暗号化であり、デフォルトで暗号化するということを意味します。
2. ファイルがどこに保存 / コピー / 移動されても、常に暗号化する。

暗号化は、データを保護する最善の手法として、広く認知されています。特許につながる新しいアイディアを記した文書や、新しいビジネスコンセプトを説明するスプレッドシートなど、その内容はさまざまですが、従業員が作成するデータはすべて重要データであり、自動的かつ透過的に暗号化するべきです。従業員がデータの重要度に基づいていちいち暗号化するかどうかを決めるべきではありません。そもそも、データが暗号化されていることを意識しないで済むのが理想的です。そのような状況を作り出せば、従業員はただ既存のワークフローに従って業務を進めればよく、一方で、データを確実に保護することができます。

ファイルはいったん暗号化されれば、その状態が保持されます。たとえば、ファイルが移動・コピーされたり、名前が変更された場合はもちろん、デバイスの外に送信された場合であっても、常に暗号化された状態を保ちます。ユーザーが誤ってファイルを紛失してしまった場合でも、暗号化されているため、許可されていないユーザーがそのファイルを解読したり使用したりすることはできません。

DLP について

データ保護といえば、DLP (Data Loss/Leakage Prevention)、つまり「データ流出防止」が連想されがちです。DLP と暗号化技術は、従来、共用される技術でした。DLP は優れたテクノロジーですが、一方で、DLP に多大な時間と費用を投資したあげく、うまく実用化できなかったケースが数多く報告されています。これは、DLP が複雑であることに起因します。DLP では、データの保護ルールをゼロから作り上げ、定着させる必要があります。よくあるのは、管理者が作ったルールが厳しすぎて、何も問題のないケースまで報告されてしまい、後処理に時間がかかるというものです。一方、ルールが緩すぎると、DLP システムをすり抜けてデータが社外に流出する恐れがあります。ソフォスは、データを分類する必要性を省き、DLP の概念を覆しました。これにより、エンドユーザーと管理者の双方の手間が大幅に省かれます。

DLP が重要でないと主張しているわけではありません。DLP は、次世代型暗号化においても、引き続き役割を果たし続けます。しかし、これは例外的なケースにのみ適用され、基本ルールとはなりません。たとえば、従業員がデータの暗号解除を意識的にリクエストしたとします。こういったケースでは、DLP ルールを使用します。DLP ルールと照らし合わせ、機密データが含まれないと判断されれば、暗号を解除することが許可されます。一方、問題ありと判断された場合は、暗号解除のリクエストは拒否されます。このアプローチは、重要ファイルを確実に保護されたままにすることができるので、二重の安全機構と言えます。また、ファイルの暗号解除リクエストがすべて確認・記録されるのも特徴です。

このアプローチにより、DLP ルールは例外的な場合 (暗号を解除する場合) にのみチェックすればよく、処理が大幅に簡易化されます。

Synchronized Encryption

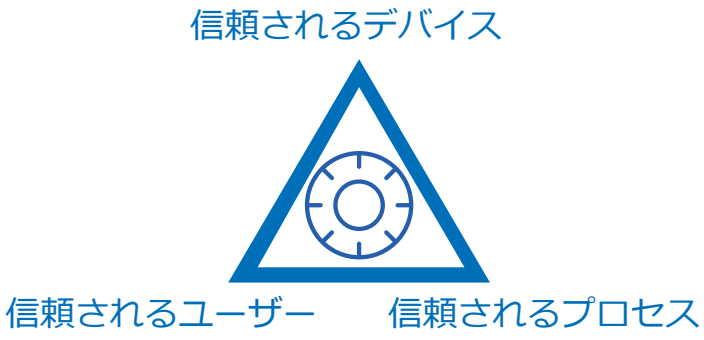
暗号データにアクセスするには、信頼されるデバイス、信頼されるユーザー、信頼されるプロセス / アプリケーションという 3つの条件をすべて満たす必要があります。

従業員のデータをすべて暗号化したと仮定して、次に保護する必要があるのは、データの暗号化に使用する暗号鍵です。

暗号鍵の基本的な考え方は、信頼されるデバイス、アプリケーション、およびユーザーにのみ、暗号化されているデータへのアクセスを許可するというものです。

これを実現するために、ソフォスでは、Sophos Endpoint および Sophos SafeGuard Encryption (SafeGuard) の両製品のノウハウと機能を統合して、暗号化を脅威対策テクノロジーのレベルにまで引き上げました。エンドポイント製品は、機器のセキュリティ状態を調べたり、プロセスが信頼されるかどうかを判断することを得意としており、これらの処理を担当します。一方、データ保護製品は、データを保護したり、鍵へのアクセスを制御する処理を行います。

鍵をリリースするタイミングや、暗号化されたコンテンツへのアクセスを許可するかどうかを判断するにあたっては、ユーザー、デバイス、アプリケーション / プロセスの 3つを同時に判断したうえで決定します。



これらの条件をすべて満たすことによって、暗号鍵にアクセスして暗号データを表示できるようになります。

実際のケースでは、社内の正規ユーザーが、信頼されるデバイスから (会社から支給されたデバイスなど)、信頼されるアプリケーションを使用してアクセスすることがほとんどで、この場合は、データに透過的にアクセスできます。ただし、条件が 1つでも欠けていると、暗号鍵にアクセスできず、たとえファイルを見れたとしても、暗号化されたままです。マルウェアがファイルをこっそり盗み出したような場合も同様で、暗号鍵がなければ、解読することはできません。

信頼されるデバイス

デバイスが信頼されるかどうかを判断する方法は、多数あります。その 1つとして、ソフォス製品がインストールされていれば、信頼されると見なすことができます。また、ソフォスのエンドポイントエージェントによって、安全 (グリーン Heartbeat™ ステータスがグリーン) と評価された場合も、信頼される根拠となります。EMM ソリューションで管理されているモバイルデバイスの場合は、企業のセキュリティポリシーに従っているかどうかが、信頼されるかどうかの分かれ目となります。契約社員が使用しているデバイスなどは、管理者が信頼しないと明示的に定義することもできます。

Windows や Mac のノート PC が感染し、マルウェアを削除処理中の場合は、信頼すべきではありません。iPhone や Android などのモバイルデバイスについては、企業のコンプライアンスポリシーに従っていない場合は (Jailbreak したものや、ロックスクリーンのパスワードがないものなど)、信頼すべきではありません。

信頼されるユーザー

デバイスと同様、ユーザーが信頼されるかどうかを判断する方法も多数あります。ユーザー ID から判断する方法や、システムにログインできたユーザーを信頼されると見なす方法などがあります。退職する従業員に対しては、暗号データへのアクセスを許可するべきではありませんが、デバイスに引き続きログインできてしまうことがあるため、そういったユースケースも想定しておく必要があります。

信頼されるプロセス

プロセスが信頼されるかどうかを判断するにあたっては、ソフォスのエンドポイント製品が中心的な役割を果たします。ソフォスのエンドポイント製品がインストールされているかどうかによっても違ってきますが、この仕組みの詳細については、この文書の範疇ではないので割愛します。

一般的に言って、業務上不要なアプリケーション (PUA) や、マルウェア、ウイルス、Web ブラウザ、メールクライアントは信頼されないと見なされます。その他にも、torrent のようなプログラムなど、企業にとって直感的に信頼されないと感じるアプリケーションも存在します。Web ブラウザやメールクライアントは、エンドユーザーがうっかりデータを共有・流出する経路となる恐れがあるため、デフォルトでは信頼されないと見なされます。これにより、過失によるデータ流出を防ぐことができます。

ここまでのところ、プロセスについてのみ見てきましたが、アプリケーションについてはどうでしょうか。基本的には、エンドユーザーが効率良く作業できる状況を確保するということが最優先されます。不正な処理を実行しているプロセスのみをブロックするという考え方に基づけば、その他のプロセスはすべて信頼されるとして、妨害されることなく実行することができます。

それでは、マルウェア / ウイルス以外のプロセスの例を 3つあげ、それぞれ信頼されるかどうかを考察していきましょう。

1. **メモ帳**

   メモ帳は、単独で機能する非常にシンプルなアプリケーションです。構造がシンプルであり、悪質なアクティビティが付随ません。信頼されると見なされると、メモ帳からの暗号鍵へのアクセスは許可されます。すると、メモ帳で作成した文書はデフォルトで暗号化され、それらのファイルをメモ帳で平文ドキュメントとして表示することもできます。

2. **Internet Explorer**

   Internet Explorer は、過去にエクスプロイトの被害を受けてきた経緯があり、マルウェアの感染経路として現在もよく利用されます。そのため、Internet Explorer はデフォルトでは信頼されず、暗号鍵にアクセスすることはできません。よって暗号ファイルにアクセスすることはできますが、ファイルを解読することはできません。暗号化されたファイルを Internet Explorer 経由でクラウドベースのファイル共有サービスにアップロードすることは可能です (開いたり表示したりすることはできません)。

3. Microsoft Word

Microsoft Word は、信頼されるか否かのグレ-ゾーンに位置するアプリケーションです。Word の動作にはまったく問題がなく、信頼されるアプリケーションなので、ユーザーは Word を使って文書を作成します。これらのファイルはデフォルトで暗号化されます。この暗号化されたファイルは、ダブルクリックするだけで参照・編集することができ、このプロセスは完全に透過的です。これは、Word が信頼されたアプリケーションであるため、バックグラウンドで暗号鍵にアクセスしたり、暗号化 / 暗号解除を実行することができるためです。しかし、Word はマクロウイルスのようなものに感染する恐れがあり、いったん感染したら、暗号鍵へのアクセスを許可するべきではありません。

以上の 3つの簡単な例を見ただけでも、Synchronized Encryption で継続的に、総合的な安全性をチェックする必要があることがわかります。

総合的な安全性を常時チェック

ここまでをまとめると、データ保護テクノロジーには、システムのセキュリティ状態と、総合的な安全性、アプリケーション / プロセスの信頼性を常にチェックする機能が必要とされることがわかります。最終的な目標は、従業員の業務を妨げることなく、データを安全に保つことです。すでに述べたように、信頼されないプロセスは、暗号鍵を取得できないため、ファイルにアクセスできても解読することはできません。ほとんどのケースでは、これらの処理が行われていることにエンドユーザーが気付くことはありません。しかし、マルウェアをはじめとする悪質なプロセスが見つかった場合は、明らかに実行を許可すべきではありません。また、感染システムも、信頼すべきではありません。総合的な安全性を判断するにあたっては、プロセスが信頼されるかどうかということは大前提ですが、システムの全体的なセキュリティ状態をチェックすることも重要な役割を担います。

それでは、ユーザーの業務を妨げないという点について、あらためて考察していきましょう。信頼されないプロセスは、平文のテキストデータへのアクセスを許可してはならず、実行も阻止しなければなりません。ここで、Word 文書を 2つ開いている場合を想定してみましょう - 1つ目は、自分で編集している重要文書で、2つ目は、同僚や友人から送られてきたファイルです。この 2つ目の文書が悪質だった場合は、その 2つ目の Word プロセスのみをブロックし、1つ目の Word 文書については、引き続き作業を続けられるような仕組みが求められます。

次の例として、システムが深刻な感染状態に陥ったとしましょう。感染源のマルウェアは、現在駆除作業の真っ最中です。このような場合、Synchronized Encryption では最終手段として、クライアント上の暗号鍵のを一時的に無効にします。鍵を無効化すると、そのシステム上では、ファイルもデータもいっさい復号化できなくなります。このシステム上では暗号データにアクセスできなくなり、業務の進行がいったん妨げられますが、この場合、この処置は的を射ていると言えます。感染システム上で、ユーザー (またはユーザーが使用するアプリケーション / プロセス) が暗号データへアクセスすることを許可すべきかどうか、考えてみてください。もちろん、許可すべきではありません。この場合は、マルウェアが駆除されて、システムの安全性が確認された後、暗号鍵が元のシステムに返されて、作業を続行することができます。

信頼されないプロセスは悪いプロセス？

プロセスが信頼されないということは、悪いプロセスということでしょうか？そうとは限りません。実際のケースでは、暗号ファイルを暗号化されたまま処理したいことがよくあります。たとえば、Outlook などのメールクライアントを使って、添付ファイルを送信する場合を考えてみましょう。Outlook クライアント自体は信頼されないと見なされますが、暗号化された状態のファイルを、添付したり、送信することはできます。宛先に届くと、Outlook から Word や Excel などの信頼されるアプリケーションが呼び出され、これらのアプリケーションでファイルが開かれます。つまり、エンドユーザーがまったく意識することなく、添付ファイルが暗号化・保護され、やりとりされるというわけです。

これらの例を考えると、Sophos Synchronized Encryption のコンセプトが、アプリケーションのホワイトリスティングとは異なることは明らかです。ホワイトリストに指定されたアプリケーションは、実行すること自体は問題ありませんが、これらのアプリケーションから暗号データへのアクセスを必ずしも許可してよいとは限りません。Synchronized Encryption は、実行を許可されたアプリケーションが、暗号データを平文テキストとして参照してよいかどうかを判断する役割を担います。

Synchronized Encryption - Sophos Endpoint を使用しない場合

ここまでで見てきたように、Sophos Synchronized Encryption の特長を最大限に生かすためには、Sophos Endpoint と Sophos SafeGuard の両製品が必要です。それでは、Sophos Endpoint 製品がインストールされていない場合はどうでしょうか。基本的な理屈は同じですが、システムのセキュリティ状態やプロセスが信頼されるかの判断が、動的ではなく静的に行われるようになります。SafeGuard 製品には、マルウェアを検出する機能はありません。そのため、システムのセキュリティ状態を検証するための機能が別途、必要になります。この場合は、信頼されるプロセスリストを管理者が作成し、このリストに基づいて判断することになります。デフォルトでは、このリストに指定されていないプロセスは、信頼されないと見なされます。

次世代型暗号化におけるコラボレーションのあり方

日々の業務を効率良くこなすためには、社内・社外に関わらず、エンドユーザー同士でコラボレーションすることが求められます。ここまでで見てきたとおり、次世代型暗号化テクノロジーでは、従業員が作成したデータはすべて保護され、信頼されたものだけがこのデータにアクセスすることができます。このような環境において、コラボレーションはどのように実現されるのでしょうか？繰り返しになりますが、ポイントは、従業員のワークフローを妨げず、スムーズな業務進行を維持するという点です。それでは、以下の 2点に的を絞って、詳しく見ていきましょう。

社内でのコラボレーション

社内でのコラボレーションは、もっとも簡単かつ、シームレスに行われます。社内にいる従業員は、誰もが暗号鍵にアクセスすることができます。作成されたデータはすべて暗号化され、暗号化されたまま共有され、誰でもアクセスすることができます。

1. **ジョンが Word 文書を作成し、保存するとしましょう。**ジョンはジュディに文書を確認してもらいたいと思っています。ジョンが文書を保存すると、自動的に暗号化された状態で保存されます (デフォルト暗号化)。Word 文書を暗号化するために、ジョンは何も特別な操作をする必要はありません。
2. **ジョンは、Outlook を開いて新規メールを作成し、**宛先にジュディを指定します。通常の手順に従って、このメールに Word 文書を添付します。メッセージに本文を打ち込み、「送信」をクリックします。Outlook はメールクライアントなので、一般的に、信頼されないと見なされます。信頼されないプロセスであるため、3つの必要条件のうちの 1つが欠けることになります。Outlook で Word 文書を添付すると、この文書は暗号化されたまま添付されます。
3. **メールがジュディに送信されました。**ジュディは、ジョンから届いたメールを開きます。ジョンの「送信済みメール」フォルダに入っている添付ファイルは、暗号化された状態です。ジュディの「受信メール」フォルダに入っている添付ファイルも、暗号化された状態です。つまり、ジョンからジュディのもとに届くまで、添付ファイルは暗号化された状態を保ちます。
4. **ジュディが Word 文書をダブルクリックすると、**自動的に Word から文書が開かれ、ジュディは文書を読んだり、コメントを追加することができます。Outlook は信頼されないと見なされるため、文書は一時的な場所に、暗号化されたまま保存されます。次に、Outlook は Word を起動し、Word に対して、この一時的な場所に作成されたファイルを開くようにリクエストします。Word は信頼されるアプリケーションなので、鍵にアクセスすることができます。ジュディは信頼されるユーザーであり、信頼されるデバイスとアプリケーション (MS Word) を使用しています。これらの条件がすべて満たされているため、暗号鍵によって暗号文書が平文に変換され、正しく表示されます。

   仮に、ジュディが Sophos Mobile Control の管理下にある安全なモバイルデバイス上でメールを読んだとしましょう。この場合、ジュディは暗号化された添付ファイルを Secure WorkSpace (暗号化されたコンテナ) に保存することができます。この暗号化されたコンテナでは、同じ暗号鍵が共有されるため、ジュディは安全に文書を参照することができます。

この例では、ジョンもジュディも何も特別な操作を行っていませんが、すべてのやりとりは暗号化された状態で行われ、シームレスに何の問題もなく、コラボレーション作業できていることがわかります。

社外でのコラボレーション

データがすべて暗号化されている場合、社外ユーザーとのコラボレーションの様子は変わってきます。社外ユーザーとコラボレーションするには、以下の 2通りの方法があります。

1. パスワードで保護する (HTML5 ファイルに変換)
2. 暗号を解除する

社外とのコラボレーション - ファイルの暗号を解除する場合

暗号を解除してデータを共有しても、妥当と言えるケースがあります。たとえば、パンフレットなど、一般公開情報がこれにあたります。一般公開情報は、誰もがアクセスできる状態にしておく必要があり、暗号化しなくてもまったく問題ありません。データの暗号を解除するには、次世代型暗号化製品を使用します。このときだけは、エンドユーザーが意識的に、ファイルの復号化処理を確認・実行する必要があります。

エンドユーザーがファイルを外部に送信する前に、意識的に暗号を解除した場合は、すでに説明したように、実際に暗号解除する前に、DLP によって本当に安全かどうかチェックすることもできます。暗号 / 平文は、いったんその状態に変換されると、その状態を保ちます。これらの処理はすべて記録されるため、管理者は従業員が不正な行為をしていないかどうか、監視することができます。ファイルの暗号が解除されると、その後は通常のワークフローが続行されます。

社外とのコラボレーション - パスワードを使用する場合

次に、社外ユーザーと安全に共有したい契約書があるとしましょう。この契約書は暗号化されており、相手に暗号解除してもらう必要がありますが、送り先の環境に暗号ソフトウェアがインストールされているかどうかは不明です。

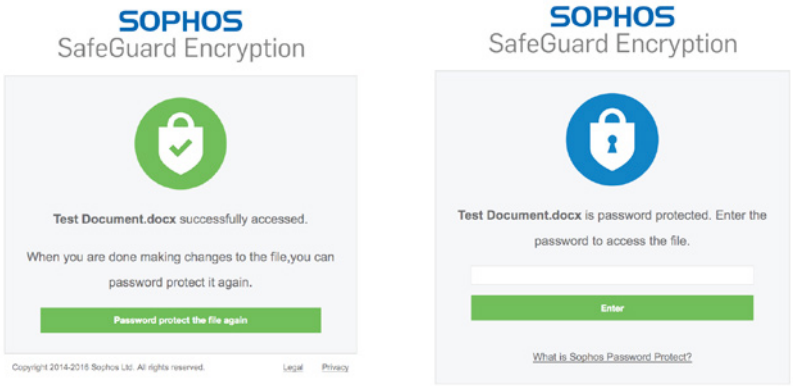
このような場合は、ユーザーがパスワードを作成して、ファイルを保護することができます。基本的には、契約文書 (contract.doc とします) は暗号化し直され、パスワードがかけられて、HTML5 wrapper に挿入されます。これにより、contract.html という名前のファイルが生成されます。パスワードは、相手に伝えておきます。この処理により、HTML5 対応のブラウザや OS で処理できる単一の HTML ファイルが出来上がります。この単一の HTML ファイルは、3つの部分から構成されています。

1. 表示レイヤー (受信者がファイルを開いたときに、Web ブラウザに表示される部分)
2. 添付された暗号データを解除するコード
3. 暗号ファイル (この例では、contract.doc)

準備ができたら、contract.doc ファイルの代わりに contact.html をメールで送信します。受信者がメールクライアント上でこの HTML ファイルをダブルクリックすると、ブラウザが開き、パスワードを入力する画面が表示されます。パスワードを正しく入力すると、ファイルの暗号を解除するコードが実行され、受信者のコンピュータに暗号解除された状態のファイルが保存されます。

この方法によって、機密ファイルを暗号化した状態で送信し、受け取った受信者がスムーズにファイルの暗号を解除して開くことが可能になります。

受信者がファイルを更新して送り返したい場合は、同じ HTML wrapper を再びコンテナとして使用することができます。このためには、受け取ったファイルを更新して、同じ HTML 画面にドロップするだけです。これにより、Sophos SafeGuard Encryption を持っていない外部のユーザーとでも、双方向の安全なコラボレーションが可能になります。



ユーザーの利便性を向上するプラグイン

ソフォス製品では、エンドユーザーの利便性のため、添付ファイル付きで社外に送信されるメールを検出するアイテム (Outlook プラグインなど) を提供しています。これを使えば、従業員が暗号ファイルを社外に送信しようとしたときに、その方法を選択する画面を表示することができます。または、管理者がポリシーにデフォルトのアクションを指定し、自動的にデフォルト処理を適用することもできます。

クロスプラットフォーム環境でのデータアクセス

従業員がスムーズに業務を進めるためには、一般的に使用されるすべてのデバイス上でソフォスの次世代型暗号化機能を実行しておく必要があります。ソフォスの次世代型暗号化は、Windows、OS X、iOS、Android に対応しています。

冒頭で、従業員は平均して 3つのデバイスを所有していると述べました。もしも Windows 機器がマルウェアに深刻に感染した場合は、この機器は信頼されないとしていったんロックされますが、Mac や iPad を持っていれば、それらを使って社内外で引き続き作業することができます。複数の機器を持っていれば、そのうちの 1つが感染したとしても、代わりに別のデバイスを使えるので問題ありません。

次世代型の脅威対策＆データ保護

ソフォスの次世代型暗号化と Synchronized Security を組み合わせて利用すれば、より高いレベルのセキュリティを実現することができます。Sophos Endpoint と Sophos UTM / Firewall、Sophos SafeGuard の 3つソリューションをすべて連係させれば、脅威を効果的に検出・駆除できるのはもちろんのこと、脅威による暗号データへのアクセスを確実に阻止できるようになります。これが、「次世代型」の保護製品と呼ばれる理由です。

まとめ

ソフォスの次世代型暗号化は、データ保護のパラダイムを転換させます。従来のファイル / フォルダごとの暗号化に代わり、あらゆるデータを暗号化するアプローチによって、エンドユーザーは、どのデータが重要であり、暗号化する必要があるかどうかを判断する必要がなくなりました。その結果、エンドユーザーのワークフローをまったく変えることなく、使いやすく、透過的・自動的に暗号化 / 復号化する仕組みが実現しました。Synchronized Encryption のデータ保護方法は、感染システムが発生した場合にその鍵を無効化したり、信頼されないアプリケーションや悪質なアプリケーションからのアクセスを制限するという考え方に基づいています。この仕組みにより、データと企業を安全に保護する一方で、従業員がスムーズに業務を続けることが可能になりました。

ソフォス株式会社営業部
Tel: 03-3568-7550
Email: sales@sophos.co.jp

2016/08/01 WP-JA (NP)

SOPHOS