SOPHOS
Security made simple.

Chiffrement Next-Gen : l'approche Sophos

La perte des données reste une préoccupation majeure de toutes les entreprises. Personne n'en est à l'abri, peu importe la taille de l'entreprise ou l'endroit où elle se situe, ni le secteur professionnel. Selon Privacy Rights Clearinghouse (États-Unis), tandis que la moitié des violations de données produites en 2014 sont dues au piratage ou à un malware, 16 % d'entre-elles résultent d'une divulgation involontaire.

Parallèlement à cela, l'environnement de travail a énormément changé ces dernières années. Aujourd'hui, les entreprises ont besoin de se protéger contre la perte de données et se conformer aux législations en matière de protection des données, tout en assurant la productivité de leurs employés.

La stratégie de chiffrement Next-Gen de Sophos est conçue pour répondre spécifiquement à ces besoins. Le présent document explique pourquoi le chiffrement Next-Gen est indispensable et comment il fonctionne, et démontre comment Sophos simplifie la protection des données pour les entreprises de toutes tailles, tout en renforçant la productivité des utilisateurs.

La situation actuelle

L'environnement de travail actuel est très différent de ce qu'il était il y a 5 ou 10 ans. L'environnement des systèmes et des menaces a énormément évolué. Examinons deux des changements principaux ayant eu des effets sur la protection des données.

Votre système n'est pas mobile, c'est vous qui l'êtes

Un utilisateur ordinaire possède en moyenne trois systèmes. Auparavant, il s'agissait essentiellement d'un ordinateur de bureau et parfois d'un ordinateur portable, mais le paysage s'est depuis développé et inclut désormais des tablettes et smartphones. Mettez-vous à la place de vos utilisateurs. Il y a de grandes chances qu'ils utilisent un ordinateur portable, ainsi qu'un téléphone mobile, voire une ou deux tablettes.

Bien souvent, les smartphones contiennent tout autant de données sensibles qu'un ordinateur portable, si ce n'est plus, et il est beaucoup plus facile de les perdre. Plus les utilisateurs possèdent d'appareils mobiles plus la surface d'attaque potentielle des données de l'entreprise augmente.

Le personnel est habituellement mobile et l'on attend de chaque employé qu'il reste productif pendant ses déplacements. Pour cela, il doit avoir accès aux données de l'entreprise depuis l'appareil mobile de son choix, peu importe quand et où il se trouve.

Il est minuit, savez-vous où sont vos données ?

Savez-vous où sont les données de votre entreprise ? Elles sont stockées sur des serveurs, des ordinateurs de bureau ou portables, des mobiles, des tablettes et des supports de stockage amovibles, sans oublier les plateformes de stockage en ligne. Les données professionnelles sensibles se situent en dehors des frontières traditionnelles de l'entreprise, principalement du fait de la disparition de cette notion de frontière professionnelle.

Comment définir cette frontière pour les données, si elles se trouvent stockées sur de multiples appareils et lieux de stockage ? Ces appareils ne sont pas administrés ou passent très peu de temps à l'intérieur du réseau de l'entreprise. Et dans le cas d'une plateforme de stockage dans le Cloud, il est fort probable que vous ne sachiez pas où vos données sont physiquement stockées ni qui y a réellement accès. Toutes ces raisons démontrent pourquoi vous avez besoin de protéger vos données là où vos utilisateurs les stockent.

Définir la stratégie pour un chiffrement Next-Gen

En développant notre stratégie de chiffrement Next-Gen, nous avons pris en compte plusieurs domaines où les clients pourraient subir une perte ou une violation de leurs données. Notre stratégie prend en compte les domaines suivants :

1. Les répercussions liées à la perte ou le vol d'appareils
2. La manière dont les personnes utilisent les données
3. La divulgation involontaire liée à une erreur humaine
4. Les attaques de cyber-pirates ou de malwares
5. La simplicité

Nous pourrions inclure les attaques ciblées dans cette liste (qui sont à l'opposé des attaques opportunistes de malwares ou de phishing), mais les statistiques démontrent qu'une PME a peu de chances d'en être victime. À moins d'être une grande société, comme Sony ou Orange, ou d'être en possession d'informations très spécialisées et sensibles, les pirates ne se donneront pas la peine de lancer une attaque ciblée.

Les répercussions liées à la perte ou le vol d'appareils

Chacun des appareils mobiles de chaque utilisateur peut potentiellement être volé ou perdu. Il n'est pas rare d'oublier son téléphone dans le train en allant au travail ou son ordinateur portable lors d'un contrôle à l'aéroport. Les systèmes sont petits et les accidents peuvent survenir. C'est pourquoi le chiffrement intégral du disque, utile pour protéger les données stockées, est une première ligne de défense efficace. Mais se limiter à prévenir le comportement des utilisateurs ne suffit pas à protéger les données de votre entreprise.

Comment les employés utilisent-ils les données ?

Observez un moment vos utilisateurs et examinez comment ils utilisent les données. Ils les manipulent sous forme de documents, de présentations, etc. Ils copient des fichiers sur des serveurs partagés, des clés USB ou des plateformes de stockage en ligne. Ils travaillent avec des fichiers qui migrent d'un appareil à l'autre selon différentes options de stockage. Dans ce genre de situation, la protection des données est fondamentale.

Simple erreur humaine

Nous sommes tous des êtres humains, et nous faisons tous des erreurs. Chacun d'entre nous a déjà créé un email, attaché la mauvaise pièce jointe puis envoyé cet email (ou envoyé le bon fichier au mauvais destinataire). Il existe de nombreux exemples d'erreurs humaines simples qui conduisent à la perte ou la violation de données. Les navigateurs Web et les clients de messagerie sont de bons exemples d'outils de production utilisés par les utilisateurs pour partager des données, mais qui peuvent accidentellement exposer des données professionnelles sur le Cloud ou les envoyer à la mauvaise personne.

Les attaques des cyber-pirates ou des malwares

L'analyse réalisée en 2014 par Privacy Rights Clearinghouse sur les violations de données classe différentes catégories de violations et a déterminé que le piratage ou les malwares représentent 51 % des violations de données. Les malwares sont en constante évolution, tant en taille qu'en complexité. Cela inclut également le vol de données opportuniste. Les malwares ne sont évidemment pas dignes de confiance et ne devraient donc jamais avoir accès aux données chiffrées.

La simplicité

Le chiffrement fonctionne mieux lorsque personne ne s'en rend compte. Il offre une protection invisible, sans effet sur les utilisateurs. C'est par exemple le cas du protocole HTTPS. Le « S » veut dire sécurisé, et signifie que toutes les communications entre votre navigateur et le site Web sont chiffrées. La plupart des utilisateurs ne remarquent aucune différence dans l'URL qu'ils visitent.

Le chiffrement doit être un moyen simple à utiliser pour l'administrateur tout comme l'utilisateur final, afin de garantir l'adhésion totale de ces deux acteurs.

Présentation de Sophos Next-Gen Encryption

La stratégie de chiffrement Next-Gen de Sophos se fonde sur deux affirmations :

1. Toutes les données créées par un utilisateur sont importantes et doivent être protégées (chiffrées). C'est ce que nous appelons le chiffrement « always-on », c'est-à-dire actif en permanence, ou le chiffrement par défaut.

2. Le chiffrement doit être persistant, peu importe où le fichier est stocké, copié ou déplacé.

Le chiffrement est considéré comme l'une des meilleures façons de protéger des données. Que l'utilisateur crée un document expliquant sa nouvelle idée de brevet ou une feuille de calcul pour démontrer un nouveau concept commercial, il s'agit de données importantes qui doivent être chiffrées. Un utilisateur ne devrait pas avoir à décider lui-même si telle ou telle données doit être chiffrée ou non. En réalité, les utilisateurs ne réaliseront même pas que les données sont chiffrées. Cela leur permet de rester productifs tout en gardant les données protégées.

Une fois le fichier chiffré, il doit le rester. Peu importe que ce fichier soit déplacé, copié ou renommé, et indépendamment du fait que le fichier sorte ou non de l'appareil, le chiffrement doit être permanent. Si un utilisateur perd accidentellement un fichier, il sera perdu sous sa forme chiffrée, le laissant indéchiffrable/illisible à toute personne n'ayant pas la permission de le lire.

Qu'en est-il du DLP ?

La protection des données sous-entend souvent les techniques de prévention des fuites de données (DLP pour Data Leak Prevention). Le DLP et le chiffrement ont toujours été étroitement associés. Bien que le DLP soit une formidable technologie, il existe de nombreux exemples d'entreprises n'ayant pas mis en place une stratégie DLP, même après y avoir consacré beaucoup d'argent et d'énergie. Le problème réside dans la complexité de la tâche. Des règles appliquées aux données, que vous n'avez peut-être pas encore créées, doivent être mises en place. Un des problèmes récurrents est que les administrateurs sont trop stricts avec certaines règles et font ensuite face à un nombre conséquent de faux positifs. À l'inverse, certains administrateurs assouplissent les règles, et les données finissent par sortir de l'entreprise malgré les systèmes DLP. Sophos a repensé complètement le DLP en enlevant la nécessité de classifier les données. Cette simplification facilite le travail des administrateurs et des utilisateurs.

Mais cela ne veut pas dire que le DLP n'est pas important. Il a toujours un rôle à jouer dans le chiffrement Next-Gen. Mais cela doit rester l'exception et non la règle. Lorsque l'utilisateur veut déchiffrer les données, retirer la protection d'un fichier est un choix délibéré. C'est le seul moment où les règles de DLP peuvent être suspendues. Si aucune alerte n'est déclenchée, l'utilisateur est autorisé à déchiffrer le fichier car il ne contient pas de données jugées sensibles. En revanche, si une alerte se déclenche, la demande de déchiffrement du fichier est refusée. Cette approche de sécurité intégrée garantit que les fichiers restent chiffrés. En outre, toute requête pour déchiffrer un fichier est analysée et enregistrée.

Cette approche simplifie grandement le DLP, puisque l'évaluation des règles de DLP devient l'exception (utilisé uniquement lorsque les données sont déchiffrées), et réduit considérablement les exigences du processus.

Synchronized Encryption

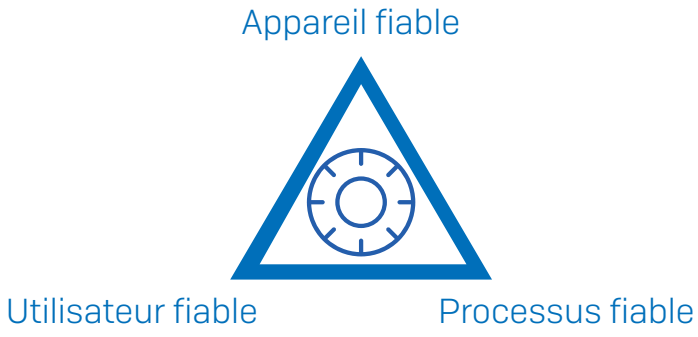
Si nous partons du principe que toutes les données des utilisateurs sont chiffrées, les seconds éléments les plus importants à protéger sont les clés de chiffrement.

Le principe fondamental des clés de chiffrement repose sur le fait que seuls les appareils, applications et utilisateurs fiables ont accès aux données chiffrées.

Pour y parvenir, Sophos fusionne le savoir-faire et les fonctions des produits Sophos Endpoint avec Sophos SafeGuard Encryption (SafeGuard) pour transformer le chiffrement en une technologie de protection contre les menaces. Le produit Endpoint analyse l'état de santé de la sécurité de la machine afin de déterminer si les processus en cours sont fiables, tandis que le produit de protection des données chiffre les données et protège l'accès aux clés.

Pour prendre la décision de livrer les clés et d'autoriser l'accès au contenu chiffré, nous triangulons et synchronisons les informations sur l'identité de l'utilisateur, l'appareil et les applications/processus.

Pour être considéré comme fiable et pouvoir accéder aux données chiffrées, l'utilisateur doit utiliser un appareil fiable, être un utilisateur fiable et utiliser une application ou un processus fiable.



Ces trois conditions doivent être validées afin d'accéder à la clé de chiffrement et de voir les données.

Dans quasiment tous les cas, un utilisateur légitime de l'entreprise sera capable d'accéder en toute transparence aux données en utilisant un appareil fiable (c'est-à-dire un appareil de l'entreprise) et des applications fiables. Si l'une ou plus de ces trois conditions n'est pas remplie, l'utilisateur ne pourra pas accéder à la clé et ne pourra pas lire le contenu chiffré. Grâce à cela, les malwares voleurs de données qui réussiront à exfiltrer des fichiers protégés ne pourront pas les lire sans la clé de chiffrement.

Système fiable

Il existe plusieurs façons de déterminer si un système est fiable. Par exemple, un système est considéré comme fiable si les produits Sophos appropriés y sont installés. Ou bien si l'agent Sophos Endpoint a évalué le système et le considère comme sain (avec un Heartbeat™) vert). Un appareil fiable peut être un mobile administré par la solution EMM de l'entreprise et ainsi se conformer à sa politique de sécurité. Alternativement, un administrateur peut explicitement demander qu'un système ne soit pas considéré comme fiable, par exemple lors de l'utilisation par un sous-traitant.

Si un ordinateur portable Windows ou Mac est dans un état d'infection active, la solution Endpoint étant en cours de nettoyage du malware, le système ne devrait pas être considéré comme fiable. Dans le cas d'un mobile, comme un iPhone ou un Android, s'il ne répond pas aux exigences de conformité de l'entreprise (s'il a été jailbreaké par exemple, ou si l'écran n'est pas verrouillé par un mot de passe), il ne devrait pas être considéré comme fiable.

Utilisateur fiable

De la même manière qu'il existe de multiples façons de déterminer si un appareil est fiable, il existe de nombreuses façons de déterminer si un utilisateur est fiable. Cela peut être basé sur son identité ou simplement sur le fait qu'il se soit connecté sans problème au système. Dans certains cas, comme lorsqu'un utilisateur quitte une entreprise, les utilisateurs pourront se connecter à leur système mais ne pourront pas accéder aux fichiers chiffrés.

Processus fiable

Sophos Endpoint prend les devants pour déterminer si un processus est fiable ou non. Les détails précis du fonctionnement de Sophos Endpoint n'entrent pas dans le cadre de ce document.

D'une manière générique, la logique interne ne fait pas confiance aux PUA (applications potentiellement indésirables), malwares, virus, navigateurs Web et clients de messagerie. Il existe cependant d'autres types d'applications, dont les programmes Torrent, auxquelles les entreprises ne font instinctivement pas confiance pour accéder aux données chiffrées. Les navigateurs Web et les clients de messagerie ne sont pas considérés comme fiables par défaut, car ces deux processus facilitent le partage ou la perte accidentelle de données. C'est une protection contre les erreurs humaines simples.

Pourquoi parlons-nous de processus et non d'applications ? Tout d'abord, notre objectif premier est de garantir la productivité des utilisateurs. En bloquant uniquement le processus au comportement suspect, cela permet aux processus fiables de fonctionner librement.

Regardons plus en détail trois exemples d'un processus, autre qu'un malware/virus, et s'il peut être considéré comme fiable ou non.

1. **Notepad**

   Notepad est une application autonome simpliste. Elle est fiable car elle est simple et ne contient aucune activité malveillante. Notepad étant considéré comme fiable, il peut accéder à la clé de chiffrement. Les documents créés avec Notepad sont chiffrés par défaut et le texte de ces documents chiffrés peut être affiché.

2. **Internet Explorer**

   Internet Explorer a un historique lourd et est couramment utilisé pour transmettre des malwares. C'est pour cela qu'il n'est pas considéré comme fiable. Par conséquence, il ne peut pas accéder à la clé de chiffrement et ne peut accéder aux fichiers que sous leur forme chiffrée. Il ne peut pas ouvrir ou voir le contenu des fichiers, mais peut toutefois les télécharger sur une plateforme de stockage en ligne.

3. **Microsoft Word**

   Microsoft Word se situe dans une zone floue, où il est considéré comme fiable et non fiable. Lorsque Word fonctionne normalement, un document créé par un utilisateur sera chiffré par défaut. Il suffit de double-cliquer sur le fichier chiffré pour le lire et le modifier. Le processus est totalement transparent, car Word est considéré comme fiable et peut dès lors accéder aux clés de chiffrement pour chiffrer/déchiffrer les fichiers en arrière-plan. En revanche, Word peut également être infecté par quelque chose se rapprochant d'un macrovirus, et dans ce cas, Word n'est plus considéré comme fiable, ne peut plus accéder aux clés de chiffrement et ne peut plus lire les données chiffrées.

Cela illustre trois exemples du processus de décision de la fiabilité, démontrant la nécessité du chiffrement synchronisé pour contrôler en permanence l'intégrité du système.

Contrôle permanent de l'intégrité avant d'accorder la confiance

Avant tout, vous voulez que votre technologie de protection des données contrôle en permanence la santé de la sécurité, l'intégrité et la fiabilité des applications/processus du système. Le but est de garder vos utilisateurs productifs tout en gardant vos données sécurisées. Comme mentionné ci-dessus, si un processus n'est pas fiable, il n'aura accès qu'aux fichiers dans leur format chiffré et ne pourra pas obtenir la clé de chiffrement. La plupart du temps, les utilisateurs ne s'en rendront pas compte. En revanche, si le processus est malveillant, s'il s'agit d'un malware par exemple, il est évident qu'il ne devrait pas du tout fonctionner. Et si votre système est infecté, il ne devrait pas être considéré comme fiable. Le processus de décision de la fiabilité est la première réaction pour préserver l'intégrité, mais le système global de la santé de la sécurité joue également un rôle dans cette réaction.

Mais revenons au concept consistant à garder les utilisateurs productifs. Le but recherché est d'empêcher les processus non fiables d'accéder aux données en texte brut et de les bloquer. Par exemple, si vous ouvrez deux documents Word, où le premier contient des informations importantes sur lesquelles vous travaillez et le second est un fichier envoyé par un ami ou un collègue, et si le second document s'avère être malveillant, seul ce second processus Word devrait être bloqué. Nous souhaitons permettre à l'utilisateur de rester productif sur le premier document Word.

Si le système de l'utilisateur se révèle être hautement infecté avec un ou plusieurs malwares qui sont en cours de nettoyage, Synchronized Encryption peut, en dernier recours, révoquer les copies locales des clés de chiffrement. La révocation des clés évite que tout code malveillant ne puisse déchiffrer les fichiers ou les données sur le système. Cela a pour effet de diminuer la productivité de l'utilisateur, car il ne peut plus accéder aux données chiffrées, mais c'est justement l'effet recherché. Souhaitez-vous qu'un utilisateur (et les applications/processus qu'il utilise) puisse accéder aux données chiffrées sachant que le système est infecté ? Non, vous ne le souhaitez pas. Une fois le(s) infection(s) de malware nettoyée(s) et l'état de santé du système revenu à la normale, les clés de chiffrement seront réintroduites dans le système et l'utilisateur pourra continuer de travailler.

Un processus non fiable est-il forcément mauvais ?

Si un processus n'est pas fiable, cela veut-il dire qu'il est mauvais ? Non, pas nécessairement. Il existe de nombreux cas où vous avez besoin qu'un processus accède à vos fichiers, mais uniquement dans leur état chiffré. Par exemple, les utilisateurs peuvent utiliser un client de messagerie comme Outlook pour envoyer des pièces jointes. Outlook n'est pas fiable, mais il peut accéder aux fichiers chiffrés pour joindre des pièces et les envoyer à une autre personne. Une fois dans la boîte de réception du destinataire, Outlook fait appel à une application fiable, telle que Word ou Excel, pour ouvrir le fichier. Aux yeux de l'utilisateur final, le processus est totalement transparent, mais en arrière-plan les pièces jointes sont chiffrées et donc protégées durant la phase de transmission.

Cela montre également pourquoi le concept Sophos Synchronized Encryption est différent d'une mise sur liste blanche des applications. Vous pouvez faire confiance à une application mise sur liste blanche, mais cela ne veut pas dire qu'elle devrait forcément avoir accès aux données chiffrées. Avec Synchronized Encryption, vous décider si une application fiable est suffisamment fiable pour l'autoriser à lire les textes bruts des données chiffrées.

Synchronized Encryption sans Sophos Endpoint

Pour profiter au maximum de Sophos Synchronized Encryption, les clients ont besoin des produits combinés Sophos Endpoint et Sophos SafeGuard. Mais que se passe-t-il si le produit Sophos Endpoint n'est pas présent ? La même logique s'applique, mais en revanche la validation de l'état de santé du système et du processus n'est alors plus dynamique mais statique. Le produit SafeGuard ne peut pas détecter les malwares, donc une évaluation de la santé du système différente doit être établie. La fiabilité des processus est alors basée sur quelque chose se rapprochant d'une liste de processus avec un nom fort, que l'administrateur peut ensuite choisir de définir comme fiable. Par défaut, tout ce qui n'apparait pas dans cette liste est considéré comme non fiable.

Options de collaboration avec le chiffrement Next-Gen

Dans le cadre de leur travail, les utilisateurs ont besoin de collaborer avec des personnes internes ou externes à l'entreprise. Le chiffrement Next-Gen garantit que toutes les données créées sont protégées, et que seuls des applications/processus fiables peuvent y accéder. Comment la collaboration fonctionne-t-elle ? L'objectif principal est de permettre aux utilisateurs de rester productifs et de conserver leur flux de travail. Regardons maintenant plus en détail les deux cas de figure de la collaboration.

Collaboration interne

La collaboration interne est en réalité l'expérience la plus simple et la plus transparente. Tous les utilisateurs d'une entreprise ont accès aux clés de chiffrement et toutes les données créées sont chiffrées. Ces dernières restent chiffrées lorsqu'elles sont partagées et tout le monde peut y accéder.

1. **Jean crée un document Word et l'enregistre.** Il souhaite avoir l'avis de Justine. Lorsque Jean enregistre le document, il est automatiquement chiffré (chiffrement par défaut). Jean n'a rien d'autre à faire pour chiffrer son document Word.
2. **Jean ouvre Outlook et crée un nouvel email**, qu'il destine à Justine. Comme à son habitude, Jean attache le fichier à cet email. Il écrit son email et l'envoie. Outlook est un client de messagerie et n'est génériquement pas fiable. Comme ce n'est pas un processus fiable, il rompt une des trois conditions (processus fiable). Outlook attache le document Word en pièce jointe sous son format chiffré.
3. **L'email est alors envoyé à Justine**, qui le reçoit et l'ouvre. Le fichier en pièce jointe est chiffré dans la boite d'envoi de Jean. Le fichier en pièce jointe est chiffré dans la boite de réception de Justine. Le fichier en pièce jointe reste chiffré lors de son transfert entre Jean et Justine.
4. **Justine double-clique sur le document Word** dans l'email et il s'ouvre sans aucun problème dans Word, où Justine peut alors le relire et ajouter ses commentaires. Outlook n'est pas fiable, donc il enregistre le document dans un emplacement temporaire sous sa forme chiffrée. Outlook lance ensuite Word pour ouvrir le fichier temporaire qu'il vient de créer. Word est fiable et a accès à la clé. Dans la mesure où Justine est fiable, son appareil est fiable et MS Word est fiable, le fichier est déchiffré et tout son contenu s'affiche sur l'appareil de Justine.

   De plus, si Justine lit cet email depuis son mobile protégé par Sophos Mobile Control, elle peut enregistrer la pièce jointe chiffrée dans Secure WorkSpace (conteneur chiffré) et puisque ce conteneur partage la même clé, elle pourra voir le contenu du document tout en le gardant sécurisé.

Ni Jean ni Justine n'ont eu besoin de changer leur comportement, et toutes leurs interactions étaient chiffrées. Ils ont bénéficié d'une expérience transparente et peuvent collaborer sans aucune difficulté.

Collaboration externe

Du moment où toutes les données sont chiffrées, la collaboration externe ne se fait plus de la même manière. Les utilisateurs peuvent alors collaborer avec des personnes extérieures de deux façons :

1. Protection par un mot de passe (enveloppé dans un fichier HTML 5)
2. Déchiffrement

Collaboration externe avec un fichier déchiffré

Il existe de bonnes raisons de vouloir déchiffrer des données. Par exemple pour rendre public des documents, comme des brochures. L'information publique doit être accessible à tout le monde, et il est donc parfaitement normal de vouloir la déchiffrer. Le déchiffrement des données est le seul moment où le chiffrement Next-Gen sera apparent aux yeux de l'utilisateur. En effet, ce dernier devra confirmer vouloir poursuivre le déchiffrement d'un fichier.

Le déchiffrement d'un fichier requiert une décision délibérée de la part de l'utilisateur. Comme mentionné ci-dessus, le fichier peut alors passer à travers le DLP pour en examiner le contenu, et s'il obtient le feu vert, le fichier est alors déchiffré. En outre, le chiffrement, ou dans ce cas le déchiffrement, est permanent. Toutes ces actions sont enregistrées et vérifiées pour permettre aux administrateurs de surveiller les comportements malveillants des employés. Une fois le fichier déchiffré, l'utilisateur peut reprendre son travail.

Collaboration externe à l'aide d'un fichier protégé par mot de passe

Que se passe-t-il si vous avez un contrat que vous souhaitez partager en toute sécurité avec une personne extérieure, et que vous devez lui permettre de déchiffrer le fichier sans savoir à l'avance si elle dispose d'un logiciel de chiffrement sur son système ?

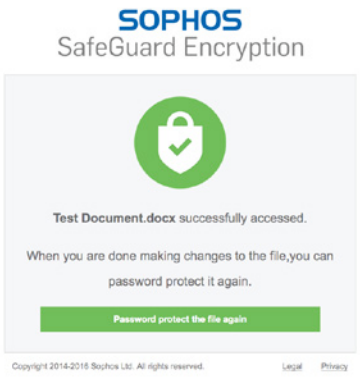
L'utilisateur peut simplement créer un fichier protégé par mot de passe et définir un mot de passe. Dans l'ensemble, le logiciel chiffre de nouveau le fichier du contrat (que nous appellerons contrat.doc) avec le mot de passe créé par l'utilisateur et l'enveloppe dans un format HTML 5 : un fichier contrat.html est alors créé. L'utilisateur devra partager le mot de passe avec le destinataire. Il en résulte un fichier HTML unique qui peut être interprété par n'importe quel navigateur HTML5 ou n'importe quel système d'exploitation. Ce fichier HTML unique est composé de trois parties distinctes :

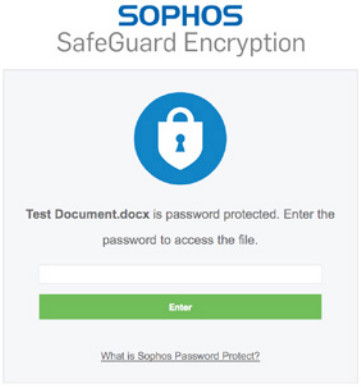
1. Le niveau de présentation (ce que le destinataire voit sur son navigateur Web lorsqu'il ouvre le fichier),
2. Le code pour déchiffrer la charge active jointe,
3. Le fichier chiffré (contrat.doc dans notre exemple).

L'utilisateur envoie alors par email au destinataire le fichier contrat.html au lieu de contrat.doc. Lorsque le destinataire double-clique sur le fichier HTML dans son client de messagerie, il ouvrira automatiquement le navigateur qui lui demandera d'entrer le mot de passe. Après avoir fourni le bon mot de passe, le navigateur exécutera le code pour déchiffrer le fichier et enregistrera ce dernier localement sur la machine du destinataire sous un format non chiffré.

Cela permet d'envoyer un fichier confidentiel dans un format chiffré, qui sera déchiffré sans aucune difficulté par le destinataire.

Si le destinataire souhaite renvoyer le fichier actualisé, l'enveloppe HTML peut également servir de conteneur. Le destinataire peut simplement mettre à jour le fichier et faire glisser le fichier actualisé sur l'écran HTML. De cette façon, une collaboration bilatérale sécurisée avec un utilisateur externe qui ne dispose pas de Sophos SafeGuard Encryption est créée.





Simplifiez la vie de vos utilisateurs

Pour simplifier la vie de vos utilisateurs, Sophos fournit un plug-in Outlook qui peut détecter l'envoi d'un email accompagné d'une pièce jointe hors de l'entreprise. Il informe alors l'utilisateur qu'il/elle est sur le point d'envoyer un fichier non chiffré et lui demande de choisir l'option de collaboration externe qu'il souhaite, avant de prendre les mesures nécessaires. Alternativement, un administrateur peut spécifier une action à prendre par défaut, grâce à une politique qui sera prise en compte automatiquement.

Accès aux données multiplateforme

Pour que la productivité des utilisateurs soit maintenue, le chiffrement Next-Gen doit fonctionner sur tous les appareils que ces derniers utilisent. Cette fonctionnalité fonctionne sous Windows, OS X, iOS et Android.

Comme nous l'avons mentionné plus haut, les utilisateurs possèdent aujourd'hui trois appareils en moyenne. Si un de leurs ordinateurs est infecté par un malware, verrouillé et non fiable, les utilisateurs peuvent toujours travailler sur leur second ordinateur ou leur tablette, indépendamment du fait qu'ils soient au bureau ou en déplacement. Si un appareil est compromis, c'est embêtant, mais l'utilisateur peut simplement utiliser un autre appareil en remplacement.

Menaces et protection des données Next-Gen

Avec Sophos, les clients peuvent atteindre un meilleur niveau de sécurité lorsqu'ils associent le chiffrement Next-Gen avec nos offres de sécurité synchronisée. Un client doté de Sophos Endpoint, Sophos UTM/Firewall et Sophos SafeGuard a la garantie que ces trois produits fonctionneront ensemble, pour offrir non seulement une excellente solution qui détectera et supprimera plus efficacement les menaces, mais s'assurera également que les menaces ne puissent pas accéder aux données chiffrées. C'est la protection Next-Gen pour votre entreprise.

Conclusion

Le chiffrement Next-Gen révolutionne la protection des données. Le chiffrement actif en permanence, contrairement au chiffrement traditionnel par fichier/dossier, enlève des épaules des utilisateurs le poids de choisir quels éléments sont importants et quels éléments doivent être chiffrés. Par conséquence, il est beaucoup plus simple pour les utilisateurs de chiffrer/déchiffrer des fichiers automatiquement et en toute transparence, sans altérer leur flux de travail. Synchronized Encryption protège les données contre les menaces en révoquant les clés des systèmes infectés et en refusant l'accès aux applications non fiables ou malveillantes. Tout cela garantit le maintien de la productivité des utilisateurs, tandis que leurs données, et votre entreprise, restent protégées.

Plus de 100 millions d'utilisateurs dans 150 pays font confiance à Sophos pour leur fournir la meilleure protection du marché contre les menaces complexes et les fuites de données. Régulièrement primées, ses solutions intégrées de sécurisation et de protection des informations sont simples à déployer, à administrer et à utiliser, et offrent le coût global de possession le plus avantageux du marché. Sophos offre des solutions de chiffrement des données, de protection des systèmes d'extrémité, de sécurité du Web, de la messagerie, des mobiles, des serveurs et des réseaux, avec le support permanent des SophosLabs, notre réseau mondial de centres d'analyse des menaces. Pour en savoir plus, consultez notre page : www.sophos.fr/products.

Équipe commerciale France
Tél. : 01 34 34 80 00
E-mail : info@sophos.fr

01/08/2016 WP-FR (NP)