SOPHOS

メールが盗聴されている？！

安全なメールゲートウェイとは

Chris McCormack、Senior Product Marketing Manager

アメリカ政府がインターネットでやり取りされる膨大な個人情報を収集していることが発覚してから、オンラインでのプライバシーに関する関心が大きく高まっています。また、企業の機密データの喪失は、政府による傍受や産業スパイなどとは比較にならないダメージとなります。メールは、意図しないデータ開示、プライバシーの侵害、個人情報保護の規制へのコンプライアンス違反などの非常に高い危険性をはらんでいます。このホワイトペーパーでは、今日の脅威の中をうまく切り抜け、メールのセキュリティを確保するお手伝いをさせていただきます。コンプライアンスの障害となるものを説明するとともに、単なる暗号化だけでなく安全なメールゲートウェイが必要な理由を説明します。

ソフォス ホワイトペーパー 2014年 11月

メールは秘密を守れません

すべてのメールトラフィックは、暗号化されていない公衆のインターネット内をテキスト形式で送信されます。これは葉書を郵便で送るのと同じです。悪意があるか、偶然であるかにかかわらず、他人宛のメールに出くわした人はだれでもすべての内容を本人がわからないところで読めてしまいます。

だれが自分のメールを読むことに興味を持っているか知りたいと思いませんか？ ISP やオンラインメールのサービスプロバイダーはどうでしょうか？Google は絶対に興味を持っています。最近の裁判所への申し立てでは、 Google 社は、Gmail のユーザーがプライバシーや機密性に対する「通常の期待」は抱けないことを認めています。[1] 2013 年 5 月の Google 社に対する複雑訴訟形態の棄却の申し立ての中で、同社は次のように証言してます。

> 「すべてのユーザーは、自分のメールが自動処理の対象であることを理解している必要があります。ビジネス上の人に手紙を送った場合に、受取人のアシスタントがその手紙を開けても驚かないのと同様に、今日の Web ベースのメールも、配信途上で受信者の [メールサービスのプロバイダー] によって処理されても驚きに値しないはずです。実際、第三者に自発的に渡した情報にプライバシー保護の期待を抱くことはできません。」[2]

権利擁護団体 Consumer Watchdog によると、これは「驚くべき告白」です。Consumer Watchdog では、メールのプライバシーを心配するユーザーは Gmail を使用しないように勧めています。[3]不幸なことに、これは解決策ではありません。これは、メールをまったく使用しないように推奨するのと同じぐらい実践的ではない推奨です。自分が Gmail を使用していなくても、Gmail を使用している顧客、パートナー、またはその他の利害関係者とメール通信しなければなりません。

また、米国国家安全保障局 (NSA) がここ数年間秘密裏に実行している大衆向け通信監視プログラム「PRISM」の存在を耳にしたことがあるかと思います。NSA は、Google、ISP、Hotmail や Yahoo などのその他のオンラインメールサービスから非公開の量のメッセージングのトラフィックを収集および保存しています。

しかし、メールに潜む危険性は、Google や NSA などの意図的な詮索だけに限られたものではありません。1 人だけに送ろうと思ったメールで間違って「全員に返信」を押してしまったことは何度ぐらいありますか？また、メールクライアントのオートコンプリート機能のおかげで、間違った相手にメールを送ってしまったことはありませんか？このような誤りは日常的に起きています。機密情報を意図しない相手に送ってしまった結果は、漏えいを公に認めなければならなかったり、罰金、信頼喪失、評判への傷からそれ以上の損害を被ったりするなど計り知れません。

1 http://www.theguardian.com/technology/2013/aug/14/google-gmail-users-privacy-email-lawsuit

2 http://www.dailytech.com/Google+Yes+we+Read+Your+Gmail/article33184.htm

3 http://www.consumerwatchdog.org/newsrelease/google-tells-court-you-cannot-expect-privacy-when-sending-messages-gmail-people-who-care

スプーフィング、スピア型フィッシング、およびスノーシュースパム

最新のメール攻撃として考慮しなければならないものとして、進化し続けるフィッシングがあります。フィッシングとは、信頼できる送信元からのメールを装ってユーザー名、パスワード、クレジットカードの情報などの取得を試みる行為です。

フィッシングは、メールアドレススプーフィングというテクニックのおかげで成功することがしばしばあります。メールアドレススプーフィングでは、攻撃者は「差出人」のアドレスとして銀行などの正当なアカウントを模したり、場合によっては勤め先の会社のドメイン名を使用して自分の会社の IT 部門からのメールであるように見せかけたりします。

最近では、組織内の特定の個人またはグループを狙ったさらに個人的で悪質なスピア型フィッシングと呼ばれる攻撃が流行しています。スピア型フィッシングは、標的とする組織のネットワークへの入り口を確保し、機密情報を取得することを目的とした高度で頻繁な攻撃キャンペーンの一般的な手法です。

また、従来型のメールスパムもまだまだ見受けられます。既存のスパム対策フィルターのおかげで、ほとんどスパムメールを見ることがなくなるとともに、フィルターをくぐり抜けたナイジェリアの王子からの奇妙なメールなどもすぐにスパムとわかります。

しかし、特定の種類の騙しの手口にかかりやすく、悪意のあるメール添付資料を開いてしまう可能性があるユーザーも存在します。研究結果として、Facebook などのソーシャルメディアサイトからの通知を装ったスパムの効果がより高いことがわかっています。[4]

スパムの送信者も、スノーシュースパムなどのスパム対策フィルターをくぐり抜けるテクニックを使用し、さらに革新的になっています。スノーシュースパムでは、その名前が示す通り、膨大な数の IP アドレスを使用して送信を行います。これによってスパム対策フィルタがすべてを捕捉しにくくなるため、ユーザーのインボックスにメールが到達する可能性が高くなります。

政府規制へのコンプライアンス

顧客、パートナーおよび従業員の機密情報を保護することは、ベストプラクティスであるのみでなく、法律で定められている場合が多くあります。規制へのコンプライアンスは、医療機関、金融機関、および政府関連機関では優先事項となります。また、これ以外の組織でも、顧客に影響する可能性があるデータ保護法を検討する必要があります。

規制法規は、データ漏えいの場合に守る必要があるコンプライアンスと開示要件を定めたさまざまな法規が地域ごとにあります。米国では、金融機関 を統制する GLBA、支払カードのセキュリティを対象とした PCI DSS、医療分野を対象とした HIPAA と HITECH、およびその他のさまざまな州の規制が存在します。別の法域にいる場合でも、同様の規制があります。欧州の EU Data Protection Regulation には、2015年に欧州議会で制定される予定の新しい法規制が複数概説されています。

それらのすべてに共通するのは、電子的に保存または転送 (メールなどの方法で) される個人情報の暗号化が要件となっていることです。これらの法律には、通常、流出や漏えいが発生した場合のコンプライアンス違反に対する罰則または罰金と開示要件が定められています。

4 “Evolving spammers using bogus social media email to fool users,” BizReport (英語)、2013 年 8 月 28 日: http://www.bizreport.com/2013/08/evolving-spammers-using-bogus-social-media-email-to-fool-use.html

コンプライアンスへの 3つの簡単なステップ

1. まずはポリシーの定義とユーザー教育から

データ喪失防止戦略の主要な要素を説明するポリシーを書類化し、従業員および利害関係者に渡します。ポリシーでは、保護する必要があるデータのタイプ、データを保護する目的、保護しなかった場合の結果、保護を確実に行うための手順に焦点を絞ります。

2. メールデータ保護テクノロジーの導入

ユーザーとポリシーは、効果的で透明度の高いテクノロジーでサポートされている必要があります。偶発的なデータ喪失防止のためのソリューションおよび機密データが組織外に出ないように保護するソリューションが必要です。ポリシーベースの暗号化を使用した安全なメールゲートウェイは、データ保護コンプライアンスのための効果的なソリューションに欠かせない要素です。

3. 不可欠な要素から時間をかけて拡張

データ保護は簡単に圧倒されるほどの作業量になるため、データ保護でのさまざまなニーズに優先順位を付けることが非常に重要です。まず、流出可能性の最も高い原因となるメールから始めます。最も機密性の高い顧客、従業員、取引先のデータ、つまり、クレジットカード番号、社会保障番号、その他の PII データまたは HIPAA データなどを保護するために必要なポリシーが制定されていることを確認します。それらのポリシーがスムーズに実行されたら、実装を拡張することを検討する必要があります。

阻害要因

メールの保護と暗号化ソリューションを導入するためにはこれだけの動機があります。では何が実行を阻害しているのでしょうか？

複雑さ: ほとんどのメール暗号化ソリューションは、調達、導入、管理が困難です。会社全体におよぶ大きな影響を持つインフラストラクチャーの評価および導入には大きな投資が必要です。既に使用しているセキュリティベンダーから投入できるソリューションで、大規模な導入プロジェクトや管理のための専門家が必要ないソリューションであれば話はとても簡単です。

コスト: ほどんどのメール暗号化ソリューションは、導入経費が高く、その後もソリューションの維持管理費がかかります。既に割り当てられているスパム対策費の予算内に収まる、暗号化と DLP の機能を搭載したメールセキュリティソリューションがあれば理想的だと思いませんか？

ユーザー体験: ほとんどのメール暗号化ソリューションはエンドユーザーのワークフローの邪魔になります。機密メールの暗号化には、ユーザーによる明示的な操作が必要なため誤りが発生する可能性があります。また、暗号化されたメールは、ユーザーが通常のメールワークフローとは異なるワークフローで処理する必要があるため、生産性を低下するとともに、ソリューション利用への抵抗感が増加します。優れたソリューションは、バックグラウンドで透過的に実行され、DLP ポリシーに基づいてメールを自動的に暗号化します。また、ユーザーに影響することも新しいクライアントソフトウェアも必要とすることもありません。

安全なメールゲートウェイとは

以下に示すのは、データ保護のための効果的で安全なメールゲートウェイソリューションを検討する場合の機能のチェックリストです。

シンプルで簡単な管理

- スパム対策、DLP、および簡単なポリシーベスのメール暗号化が単一ベンダーの 1 つの製品として統合され、かつ単一のコンソールから管理できるメールゲートウェイソリューションを探すこと
- 機密データのタイプが事前定義され、インストール後に簡単に DLP ポリシーを構築できるソリューションを選ぶこと
- メール暗号化ポリシーが、トレーニングや説明書なしでだれでも簡単に新しいポリシーを作成したり、既存のポリシーを微調整したりできるぐらい簡単であること
- 骨の折れる複雑なキー管理の必要がないソリューションを選択すること

優れたユーザー体験

- メールと添付資料の両方を自動的にスキャンして機密データのタイプの特定を行い、暗号化のためのメールへのフラグ付けをユーザーに強要することなく、自動的かつ透過的に組織外に出る前に必要な暗号化を行う効果的なメール暗号化ソリューションを選択すること
- 送信者・受信者のいずれの手も煩わさないメール暗号化ソリューションを選択することデスクトップ、ノートパソコン、モバイルデバイス、オンラインで好みのメールクライアントを使用してこれまでどおりメールを送信できるソリューションであること
- 暗号化されたメールを受信者が表示するために特別なソフトウェアが不要で Web ポータルの起動も必要としないメール暗号化ソリューションであること

価格の妥当性

- 理想的なソリューションは、DLP とメール暗号化を既に割り当て済みの予算内で導入できるもの
- 現行のスパム対策ソリューション以外の特殊なハードウェア、ソフトウェア、またはトレーニングの必要がない、評価と導入が簡単なソリューションを選択すること

メールが盗聴されている？！

ソフォスの SPX 暗号化および データ流出防止機能

ソフォスは、特許出願中の革新的な SPX 暗号化機能および事前にパッケージ化された機密データのタイプを搭載の DLP ポリシー機能で、お客様のデータ保護のニーズに応えます。

パム対策、メール暗号化、および DLP を 1 つのアプライアンスに統合した、特殊なクライアントソフトウェアのインストールを必要としない導入が簡単な製品です。

暗号化キーや証明書を使用しない単一の直感的なコンソールとわずか数分間で設定できるスマートな DLP ウィザードを使用することですべてを簡単に管理できます。

ソフォスの DLP エンジンには、事前にパッケージ済みの数百個の機密データタイプが用意されています。このため、製品を箱から取り出したらすぐに、効果的な DLP ポリシーを作成できます。カスタムタイプの作成も簡単です。

ユーザーに対して完全に透過的であるため、ユーザーの好みのメールクライアント (モバイルデバイスを含め) が使用できます。そして、これらすべての機能を搭載した Sophos Email Appliance と Sophos UTM Email Protection は、スパム対策のみに支払っている料金とほぼ同額という、お求めやすい価格でお届けいたします。

SPX 暗号化テクノロジー搭載 Sophos Email Protection の製品評価

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

11.14.wpjp.simple

SOPHOS