CUSTOMERONE

Symantec

シマンテックが実践するソースコードのセキュリティ対策

企業のソースコードについての懸念は、たいていの場合「うまく動作するだろうか」という点に絞られています。しかし、同じように重大な「ソースコードがハッカーや窃盗犯から十分に守られているだろうか」という問題はしばしば見落とされています。

シマンテックでは、数年にわたってこの 2 つ目の問題に取り組んできました。従来のセキュリティ対策はかつては十分でしたが、現在ではもはや適切とは言えなくなっています。そのため、弊社はソースコードのセキュリティを確保するための堅牢な対策を作り上げました。

2012 年以降、ソースコードの保存に使用していた数百ものリポジトリを統合し、5 つの保護レイヤーに守られた virtual vault でソースコードを保護しました。さらに、シマンテックの監視ソリューションを最大限に活用してコードを管理しました。最後に、内部ポリシーを変更し、コードを危険にさらす可能性がある従業員の行動を禁止しました。

その成果は順調に現れています。現在では、開発者のコードへのアクセスを妨げることなく高度なセキュリティでソースコードを保護しています。

シマンテックの対策は、ソースコードやその他の機密データの保護を検討しているあらゆる企業にもご活用いただけるものです。このホワイトペーパーでは、シマンテックが達成したこととその方法、およびお客様が同様の成果をどのように得ることができるかをご紹介します。お読みになった後でこのモデルの活用方法についての詳しい説明にご興味がございましたら、エグゼクティブブリーフィングとデモをご案内させていただくことも可能です。

シマンテックは、世界をリードするサイバーセキュリティ企業として、自社のソースコードのセキュリティを保護するために高度な対策を開発してきました。『**シマンテックが実践するソースコードのセキュリティ対策**』では、シマンテックのベストプラクティスをお客様と共有します。

このホワイトペーパーは、CIO、CTO、CISO および知的財産の保護について深くご検討されている上級管理職の皆様に向けたものです。リポジトリの統合、複数のセキュリティ層を使用したコード保護など、シマンテックが自社のソースコードを保護した方法についてわかりやすくご説明します。期待通りの成果を上げた点、そして改善すべき点についてもご紹介しています。

シマンテックの目標は常に、考え得る最高のソリューションを提供して、お客様がセキュリティを構築できるよう支援していくことです。

背景

2014 年 6 月からシマンテックの最高セキュリティ責任者を務める Tim Fitzgerald にとって、サイバーセキュリティ対策の重要性を決定付けた 2 つの出来事がありました。1 つ目は、2009 年末に国家の支援を受けた攻撃に 30 社以上の企業が標的となったニュースです。もう 1 つは、2012 年に Symantec pcAnywhere のコードがその 6 年前に盗まれていたことを知り、シマンテックでセキュリティの継続的改善へのニーズが増大したことでした。

最初の事件は、2010 年に Google 社が中国のハッカーを告発したことで明らかになりました。この事件では、ハッカーが、特定の電子メールアカウントに不正アクセスして知的財産を盗むために、Google 社のシステムに侵入しました。この発表は、Tim がシマンテックで情報セキュリティマネージャとして働き始めて 3 日目のことでした。彼はこのニュースに愕然するとともに、チームがこのような致命的な危機に立ち向かえるかを深刻に考えたことを覚えています。

その後、2012 年にハッカー集団が機密性の高いシマンテックのソースコードの一部を 2006 年に盗んでいたことを公表しました。ソースコードは盗まれた当時ですでに古く使用されていないものでしたが、この事件はシマンテック全体、とりわけシマンテックの知的財産を保護する方法について厳しい目で見直すきっかけとなりました。

「CSO になって最優先でなすべきことが、ソースコードの窃盗を徹底的に防ぐことでした」と Tim は述べ、さらに次のように続けます。「壊滅的な情報漏えいを阻止することが私たちの目標です」

その後、数年を経て、統合、保護、監視、管理の 4 つのステップからなる意欲的な計画によりソースコードの保護を実現しました。以下では、シマンテックの取り組みについて、ソリューションの概要から実現方法の検討に至るまでを簡単にご説明します。

ソリューションの概要

2015 年夏にソースコードリポジトリをアリゾナとバージニアの二重化した環境に集約しました。現在、コードは複数の「鍵」に加えて 5 段階の保護によって守られた「Bank Vault（銀行大金庫）」と呼ぶ場所に保存されています。

このソリューションでは、さまざまなシマンテック製品を活用することにより、ソースコードが企業ポリシーに違反して（たとえば、電子メールで送信、USB メモリに保存などで）移された場合に警告を通知します。

- **Data Loss Prevention** は、機密性の高いデータの漏えいがないかどうかをスキャンし、ネットワークレイヤーとエンドポイントレイヤーを監視します。
- **Control Compliance Suite** は、IT インフラの「リスクのしきい値」を管理し、推奨される改善事項を提供します。
- **Validation and ID Protection Service** は、2 要素認証により不正なアクセスを制限します。
- **Symantec Endpoint Protection (SEP)** は、ファイアウォール、侵入防止、ウイルス対策などを使用して標的型攻撃を防御し、エンドポイントの安全を確保します。

さらに、ソーシャルエンジニアリングによる情報漏えい行動を防止するためのポリシーも策定しました。とりわけエンジニアがソースコードのアクセス要求を受けた際には格別の注意を払うよう教育しました。たとえば、同僚からの要求であってもエンジニアは依頼者の上司に確認することが必須です。

ここまで達成するのは容易なことではなく、対策の決定、導入、調整に数年を要しました。しかし、その労力に十分な価値があることは明白です。

Tim は次のように述べています。「当初の状況と比べ、現在ははるかに良くなっています。安定した保護方式の構築に向けて着実に進展していますので、侵入や壊滅的な事態を引き起こすことは、ますます難しくなっています」

実現までのプロセス

先に述べたように、ソースコードを保護するために、統合、保護、監視、管理という 4 つのステップを計画しました。

具体的には、次のとおりです。

1. リポジトリを統合し、2 つの集中管理システムに移行。
2. 最も強力なセキュリティ技術を利用して、ソースコード環境を保護。
3. ソースコードの疑わしい移動をセキュリティポリシーで追跡。このポリシーは、必要な警告が生成されるように調整しながらも、誤検知を大量に発生させないように対象が限定されている。
4. システム全体を専門スタッフが管理することで、プロセス全体をきめ細かく管理。

ステップ 1: リポジトリの統合

最初のフェーズは、ソースコードのリポジトリを統合することでした。具体的には、世界中に分散していた 750 のリポジトリすべてを、2 つの保護された承認済みプラットフォームに移行しました。

これほど多くのリポジトリが存在していた理由の 1 つは、企業を買収するたびに、その企業で使われていたリポジトリをそのまま使用していたためです。シマンテックの開発者は、コードに簡単にアクセスできるという理由から、この方法を好んでいました。しかし、グローバルセキュリティ部門にとっては、扱いやすさとはほど遠い状態でした。セキュリティ部門は、コードの 1 行 1 行を念入りに調べ、不正なアクセスから適切に保護されていることを確認する必要があったからです。

プロセスを簡素化し、既知の脆弱性が存在するレガシーシステムをなくすために、何年もかけてリポジトリを統合しました。また、開発作業を中断しなくても済むように統合ペースを遅らせたりもしましたが、ハッカー集団の技術が高度化するにつれて、自分たちが行動を起こさなければならないことを強く自覚しました。

結果的には、この統合プロセスは比較的スムーズに進みました。ところが、リポジトリソリューションを提供するサードパーティベンターの評価を始める段階になって、社内から抵抗が起こりました。シマンテックの開発者の大半は Perforce 社のソリューションを以前から利用していましたが、一部の開発者が Git と呼ばれるオープンソース製品の利用を許可するよう強く求めたのです。

当時、オープンソースの Git は当社の目的にかなう堅牢性を備えていなかったため Git の使用を禁止しました。2 年かかって Perforce への移行が完了しましたが、その頃には、Git ベースのソリューションの 1 つであった Atlassian 社の Stash（今の BitBucket）が成熟していたため、2 番目のオプションとして従業員に利用を許可しました。このことが、反対意見を鎮めるのに役立ったのです。

ステップ 2: ソースコードの保護

統合プロジェクトを進めている間、シマンテックの他のチームは、ソースコードを 5 つのレイヤーで保護するという対策を開発していました。そのレイヤーとは、アプリケーションセキュリティ制御、ホストベースセキュリティ、ネットワークセキュリティ、物理的セキュリティ、そして最も外側に位置する厳格なポリシーと基準のセットです。

（一部の内容は社外秘ですが、エグゼクティブブリーフィングでは詳細を説明させていただきます。）

当社の開発者は、セキュリティレイヤーの追加が効率性の低下を招くのではないかとの懸念を示していました。そのため、すべての新しい手段が少なくとも以前と同程度の効率で利用できるようにしました。

「これは非常に重要でした」と、ソースコード保護プログラムの責任者を務めた Suresh Sinha は述べています。「われわれは、市場でのシマンテックの信用を守ると同時に、開発者に対して、彼らがベストを尽くして製品開発に取り組めるようなプラットフォームを提供したいと考えていたのです」。

ステップ 3: ソースコードの移動の監視

ソースコードを安全に保管した後は、シマンテックのポリシーに従った形でのみコードにアクセスされるようにする必要がありました。そのための最適な製品がSymantec Data Loss Prevention でした。Symantec DLP は、機密性の高いデータの漏えいがないかどうかをスキャンし、ネットワークレイヤーとエンドポイントレイヤーを監視します。

当社のセキュリティ担当者は、コードの利用状況を追跡するために埋め込んだ秘密のウォーターマークがスキャンされるように、Symantec DLP をプログラミングしました。

また、他の機密データが当社のネットワーク間でどのように移動しているかを追跡できるように Symantec DLP を設定しました。結果的に、これは優れた学習体験となりました。この製品では、設定によって、社会保障番号やクレジットカード番号の桁数が一致しているかどうかなどを調べたり、一部の顧客情報を追跡したりすることが可能です。ルールの設定は簡単ですが、問題は十分な量の（しかし多すぎない）情報を得られるように調整することにあります。

試しに Columbus という買収コード名を探すルールを設定しました。その結果、（問題のない記述や誤検知などのために）担当チームが調査できないほど大量の警告が生成されました。この状況がルールの数だけ発生したため、ヒット件数は膨大な数に達し、1 日あたり 10,000 件もの警告を、わずか 6 人のスタッフで詳しく調査しなければなりませんでした。当然ながら、大量の警告が調査されないままとなりました。

「DLP を使った当初の取り組みは、十分に練られたものではありませんでした」と Tim は認めています。「このソリューションの利用がうまくいったりいかなかったりを何度か繰り返した後、すべてを実現するソリューションとして利用するより、戦略的に利用したときの方が効果的であることがわかったのです」。

ここから得られる教訓は次のとおりです。DLP を使った追跡対策をあらかじめ十分検討してから、実装を開始しましょう。追跡が必要なデータは何か、どの程度詳細なデータが必要かを把握するようにしてください。次に、そのためのルールを作成するにあたり、ある程度の試行錯誤が必要になります。作成したルールによって大量の警告が発生しても、そのルールの利用をやめることなく、実用的な結果が得られるまで調整と改善を続けることが大切です（CustomerONE の『Symantec Data Loss Prevention: 導入から成熟した運用まで』で、この取り組みについて詳しく取り上げています）。

ステップ 4: プロセスのインテリジェントな管理

以前、当社では、IT エンジニアリングチームとインフラチームがリポジトリをさまざまな形で利用していました。そのため、冗長で重複する取り組みが行われ、警告への対応が一貫していないことがありました。

この問題を解決するため、すべての管理作業をセキュリティオペレーションセンター（SOC）に移管しました。SOC のスタッフは、どれが重大な警告で、どれが優先度の低い警告であるかを理解しています。また、さまざまな問題に自分たちで対処する方法や、他の部署にその問題を上げるタイミングをわかっています。

シマンテックはお客様にも、これと同じような取り組みを勧めています。単一の窓口を設けることで、ユーザーは警告が専門の訓練を受けたスタッフによって一括で管理されていることを把握できます。

また、ソースコードを安全に保管するため、IT スタッフに協力を求めました。他の人たちと同様に、当社のエンジニアも安全な環境では油断しがちになります。彼らは、同僚だと名乗る人物がコードへのアクセス許可を求めてきた場合に、その人を信頼してしまうかもしれません。あるいは、コードをある場所から別の場所に移動するときに、リスクの高い抜け道を利用する可能性があります。

そこで、カリフォルニア州南部にある当社のグローバルシマンテックラボでは、そのような行為を防止するための特別なポリシーを策定しています。たとえば、当社ではエンジニアに対し、コードへのアクセス要求に警戒と疑いの目を持つことを求めています。また、電話やメールの相手の素性が明らかになるまでは、機密情報をその人物に送らないよう求めています。相手の要求内容を記録し、その人の上司とグローバルセキュリティチームの両方に確認を取るまでは、許可を与えないようにする必要があるのです。

当社の懸念は、エンジニアが、自分たちの主要な業務の遂行を妨げる審査ポリシーに従おうとしないのではないかということでした。しかし、それは杞憂に終わりました。

「彼らはセキュリティ企業で働いていることを自覚しています」と、グローバルシマンテックラボでシニアマネージャを務める Thomas Teller は述べています。「彼らはわれわれに対し、すべての場所で高い基準を設けることを求めています。ソースコードの機密性の維持に関して、彼らは付け込まれる隙を与えたくないと考えています」。

課題

自社のソースコード保護対策の策定にあたっては、2 つの課題が生まれる可能性に備える必要があります。それは、レガシーインフラを刷新するための技術的な課題を克服することと、プログラムを実施するための適切なスタッフを見つけることです。

当社の場合、レガシーインフラの再構築は、異なるシステムどうしのやり取りをどのように実現するのかという複雑な変更を伴うものでした。また、エンジニアに多くの苦労を強いることなくセキュリティ制御を強化する方法を見つけ出す必要がありました。

これらは大変困難な課題でしたが、当社の従業員は課題に対処できるだけの技術力を持っていました。しかし、自社のスタッフが同じような技術的ノウハウを持ち合わせていない場合は、どうすればよいでしょうか。

シマンテックのマネージャで、ソースコード保護プロジェクトの実施を支援した Danny Graves は、次のようにアドバイスしています。まず重要になるのは、自社で最も技術に精通した人たちの協力のもとでスマートな対策の策定に取りかかることです。次に、前述のような障害が発生する前に、障害を予測してその対応を計画しなければなりません。

「この複雑な業務は、プロジェクト管理に行き着きます」と彼は言います。「自社の開発部門、セキュリティ部門、IT 部門の主要なメンバーを関与させ、幹部だけでなく、この環境を毎日利用する『実務担当者』を巻き込んでください。そして、全員が一堂に会した場で、可能な限りベストな取り組みを実行できる戦略への合意を取り付けるのです」。

ベストプラクティスには、パッチ管理、暗号化、強力な認証、エンドポイント保護、一元管理が含まれています。

技術的な問題に対処しながら、2 番目の課題であるスタッフの配置に取り組む必要があります。

この仕事には、さまざまなスキルを持つ人が必要になります。たとえば、エンジニアリング責任者、プロジェクト管理者、Data Loss Prevention のエンジニアなどです。どの人員も不足しがちですが、適切な人が見つかれば、長期的には時間の節約につながります。

「（DLP の）利用がうまくいったりいかなかったりを何度か繰り返した後、（DLP が）効果的であることがわかったのです。」

— シマンテック最高セキュリティ責任者、Tim Fitzgerald

エグゼクティブブリーフィングで理解を深める

このホワイトペーパーは、シマンテックがソースコードをどのように保護しているかを概観していただくためのものです。お客様固有の状況に即して機密情報を保護するうえで、どのようなご活用が可能かについて、ご説明する用意がございます。

さらに詳しい情報については、米国カリフォルニア州マウンテンビューの本社と英国のレディングに設置されている Executive Briefing Center までお問い合わせください。

エグゼクティブブリーフィングは、シマンテックのソリューションでお客様のビジネス環境やネットワーク環境を保護する方法について理解を深めていただくために用意される特別な機会です。お客様固有の目標に合わせてブリーフィングの内容をカスタマイズするとともに、新しい技術や課題が公表間近になったときにいち早くご紹介します。

本ホワイトペーパーに登場するシマンテックのソリューションと製品

Data Loss Prevention: DLP は、クラウド、モバイル、オンプレミスの各環境にわたって重要なデータが保存されている場所を検出します。

また、企業ネットワークへの接続/非接続時にデータがどのように使われているか監視するとともに、データを漏えいや盗難から保護します。

Control Compliance Suite: CCS は、セキュリティ対策と脆弱性に対して自動化された継続的な評価と統一されたビューを提供することにより、リスク優先度に基づくデータセンターセキュリティの運用とコンプライアンスを実現します。

Validation and ID Protection: VIP は、標準ベースの二要素認証とリスクベースのトークンレス認証を使用して、ネットワーク、アプリケーション、データを保護する使いやすい認証を提供します。

Symantec Endpoint Protection: SEP は、多層型の保護とインテリジェントなセキュリティによって、標的型攻撃や APT（Advanced Persistent Threat）からすべてのエンドポイントを保護します。

customer_one@symantec.com

CustomerONE チーム
350 Ellis Street
Mountain View, CA 94043
800-745-6054

シマンテックの CustomerONE チームは、お客様が弊社の IT セキュリティ担当者と話し合いを進められるよう手配することが可能です。セキュリティに関する問題や懸念に適切に対処できるようにご支援します。ご興味がございましたら、直接ご連絡いただくか、営業担当にお問い合わせください。