Trend Micro Deep Security™

「企業を取り巻くセキュリティの10大脅威」その対策と解決方法は?

独立行政法人 情報処理推進機構(IPA)の公開した「2010年版 10大脅威 あぶり出される組織の弱点!」。そのなかでもウェブサイトの改ざんなど広範囲への影響につながるサーバの問題を、トレンドマイクロの「Trend Micro Deep Security」が解決します。

企業をとりまく“10大脅威”

第1位	変化を続けるウェブサイト改ざんの手口
第2位	アップデートしていないクライアントソフト
第3位	悪質なウイルスやボットの多目的化
第4位	対策をしていないサーバ製品の脆弱性
第5位	あわせて事後対応を! 情報漏えい事件
第6位	被害に気づけない標的型攻撃
第7位	深刻なDDoS攻撃
第8位	正規のアカウントを悪用される脅威
第9位	クラウド・コンピューティングのセキュリティ問題
第10位	インターネットインフラを支えるプロトコルの脆弱性

出典:IPA 『2010年版 10大脅威 あぶり出される組織の弱点!』(2010年3月31日公表、http://www.ipa.go.jp/)

● 第1位 変化を続けるウェブサイト改ざんの手口
● 第8位 正規アカウントを悪用される脅威
➡ 不正アクセスを検知・防御するための「監視」が重要に

ウェブサイトの不正改ざんには、速やかな検知と、管理者に警告する仕組みが有効です。これに対して、Trend Micro Deep Securityでは、不正な変更を捕捉する「不正改ざん検出機能(Integrity Monitoring)」を提供しています。仮にアカウント情報が何らかの方法で攻撃者に窃取された場合も、ウェブサイト上のHTMLファイルなどの不正な書き換えを検知して、不正な改ざんを防止できます。

さらに「ファイアウォール機能」では、ウェブサイトの更新に用いられるFTPセッションにおいて、どのアカウントがいつアクセスしたかを常に監視することで、複数のツールの情報を統合する手間なく、変更されたファイルとの相関関係を踏まえた分析が可能です。また、正規アカウントの悪用に対しては、「セキュリティログ監視機能」を提供。これは、OSやミドルウェアから出力されるログを常に監視し、例えばあるアカウントについてパスワードの認証エラーが複数回発生しているといった不審なアクセスが発生した際に管理者に通知を行うものです。

Windows、Solaris、Linuxといった各種OSに導入した複数のエージェントやDeep Security Virtual Applianceについての、セキュリティポリシーやタスクスケジュール設定などをWebベースで集中管理が可能です。

● 第4位 対策をしていないサーバ製品の脆弱性
➡ 仮想パッチ適用により「脆弱性への対応」を実現

サーバにおける脆弱性対策が進まない理由は、大きく2点あります。1つ目は、セキュリティパッチの適用が稼働中のサービスに影響を与える可能性があること。2つ目は、サポート切れのサーバOSには、最新のセキュリティパッチが提供されないという点です。

これに対し、Trend Micro Deep Securityでは「IDS/IPS機能」による「仮想パッチ」で問題を解決しています。具体的には、外部との通信を監視し、脆弱性攻撃に用いられる特定のパケットをシグニチャとのマッチングにより検出・ブロック。これによって、システムは“仮想的にパッチを当てた状態”となり、OSやサービスに変更を加えずに、脆弱性をねらった攻撃からシステムを守ることができます。最近では、いわゆる“ゼロデイアタック”がサーバの世界にも広がってきていますが、そうした脅威にもこの仮想パッチは有効です。

さらに注目すべきポイントは、サーバの抱える脆弱性を調べ、必要な仮想パッチを自動的に適用する点です。これにより管理者の負担も大幅に軽減可能です。また、仮想パッチの解除も自動化されているため、正式版パッチ適用後の運用負荷も軽減できます。加えて、SQLインジェクションやクロスサイトスクリプティング(XXS)といったWebアプリケーション層を狙う攻撃を防御する「Webアプリケーション保護機能」も提供。サーバ環境が抱える脆弱性にトータルに対応しています。

Trend Micro Deep Security™

● 第7位 深刻なDDoS攻撃
● 第10位 インターネットインフラを支えるプロトコルの脆弱性
➡ アプリケーションからOS、ネットワークに至る「多層防御」が重要

DDoS攻撃のような脅威に対しては、アプリケーション層などの上位層での対策に加え、さらに広範なレイヤを意識した「多層防御」が必要です。

これに対してTrend Micro Deep Securityでは、IDS/IPS機能に加え、Webアプリケーション保護機能、ファイアウォール機能、セキュリティログ監視機能、不正改ざん検出機能という5つの機能を1製品に実装しているため、アプリケーションからOS、ネットワークに至る各レイヤでの多層的な防御が可能です(図1)。

特にネットワークレイヤでの防御を行うファイアウォール機能では、IPアドレスやMACアドレス、ポートといった単位で通信を制御可能なほか、同一のポートを利用するアプリケーションごとの通信を制御するといったきめ細かな対応が行えます。

図1　多層防御を実現する5つの機能

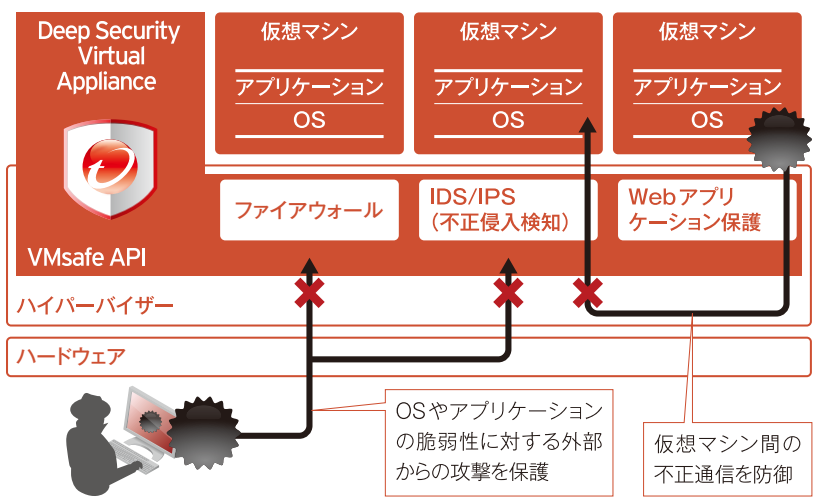
IDS/IPS、ファイアウォール、Webアプリケーション保護、セキュリティログ監視、不正改ざん検出という5つの機能を1つのエージェントに実装することで、未知の攻撃、脆弱性にも対応可能な多層防御を実現しています。

● 第9位 クラウドコンピューティングのセキュリティ問題
➡ 新時代のIT活用を支える「クラウド・仮想化への対応」

今日では「クラウドコンピューティング」や「仮想化技術」が大きな注目を集めています。しかし、クラウド環境は、物理環境をクラウド上、あるいはクラウド上の仮想環境に「移行」しただけであり、引き続き脆弱性を狙った攻撃やセキュリティ上の問題があることに変わりはありません。つまりそこに置くサーバなどにも、物理的な環境と同様にウイルス対策に加えて、脆弱性に対する対策が必要なのです。

しかし、クラウドはホスティング、ハウジングなど「場所」を提供するサービスであり、セキュリティ対策は事業者側のポリシーに依存し、ネットワーク構成を変更する必要のある従来のアプライアンス型のIDS/IPSなどを勝手に設置することはできません。

図2　仮想アプライアンス「Deep Security Virtual Appliance」



VMsafeテクノロジーに対応した仮想アプライアンス「Deep Security Virtual Appliance」により、各ゲストOSに対するエージェントレスによるセキュリティ対策を実現。仮想化環境特有の問題にも対応します。

これに対してソフトウェア型で提供されるTrend Micro Deep Securityであれば、設置したサーバまたは、仮想化されたゲストOS上にエージェントをインストールすればよいため、手軽にセキュリティ対策が行えます。

さらにTrend Micro Deep Securityでは、仮想化環境の特性を活かした先進機能を実装しています。具体的には、VMsafeテクノロジーに対応した「Deep Security Virtual Appliance」の提供。仮想化環境のハイパーバイザー上にこの仮想アプライアンスをインストールすることで、個々のゲストOSにエージェントをインストールすることなく、ファイアウォール、IDS/IPS、Webアプリケーション保護という3つの機能を各ゲストOSに適用することができます(図2)。

これにより、物理ネットワークを経由しない仮想マシン間の攻撃、仮想マシンの移動時の危険など、仮想化環境下での対応を実現。また各ゲストOSへのエージェント配布が不要なため、仮想OSを増やした際のスケーラビリティの面でのメリットも大きく、VMwareを使ってサービスを提供している事業者はもちろん、プライベートクラウドを構築するユーザにとっても、最適なソリューションとなっています。

※各見出しの順位、及び脅威の内容は出典：IPA「2010年版 10大脅威 あぶり出される組織の弱点！」より抜粋。

トレンドマイクロ株式会社が書面により事前に承諾している場合を除き、形態および手段を問わず本ドキュメントまたはその一部を複製することは禁じられています。TRENDMICROは、トレンドマイクロ株式会社の登録商標です。各社の社名、製品名、およびサービス名は、各社の商標または登録商標です。2010年5月31日現在の情報をもとに作成されたものです。今後、価格の変更、仕様の変更、バージョンアップ等により、内容の全部もしくは一部に変更が生じる可能性があります。
Copyright © 2010 Trend Micro Incorporated. All rights reserved.

安心を、ひとつ上のステージへ。

TREND MICRO™

お問い合わせ先
トレンドマイクロ株式会社
〒151-0053 東京都渋谷区代々木2-1-1 新宿マインズタワー
TEL. 03-5334-3601　URL. http://www.trendmicro.co.jp/deepsecurity