

Microsoft ネットワークを 業界で最もインテリジェントに防御

Application Intelligenceの優位性

マイクロソフトのプロトコルをアプリケーション・レベルで認識し、正当なアクセスを阻止することなく、マイクロソフトのアプリケーションをインテリジェントに保護する唯一のセキュリティ・ゲートウェイとして機能

複合型ワームおよびその亜種の攻撃を未然に阻止

マイクロソフトの新たな脆弱性に対して定期的なアップデートにより保護

課題

あらゆる規模の企業がマイクロソフトのアプリケーションおよびオペレーティング・システムに依存してビジネスを行っています。そのため、ハッカーやサイバーテロの犯罪者により、マイクロソフトのソフトウェアに存在する多くのセキュリティ上の脆弱性が狙われ、多くの不正なアクセスや悪意のある攻撃の対象となっています。Code Red、Slammer、Blasterなどのワームは、企業の生産性や収益に対して巨額の損失を与えており、最新のBlaster攻撃への対策コストは3億ドル以上¹を要するという概算もあります。ネットワーク管理者が攻撃から企業システムを守るためには、次の2つの選択肢があります。

- **定期的なセキュリティ・パッチの管理。**マイクロソフトでは、既知の脆弱性を修正するパッチ類などソフトウェアのアップデートに関するセキュリティ情報を毎月公表しています。しかしながら、企業にとって、社内システムを迅速にアップデートすることは並大抵の作業ではありません。つまり、セキュリティ修正プログラムと自社内で使用している基幹アプリケーションすべての互換性テストを行い、テスト終了後、Windowsとアプリケーションを実行しているデスクトップやサーバすべてに修正プログラムをインストールする必要があります。多くの企業において、次々と発見される脆弱性とその修正プログラムへの対応が遅れるため、不正なアクセスや悪意のある攻撃が増加する結果となっています。
- **感染したトラフィックのブロック。**Gartnerのような定評あるアナリストは、マイクロソフトの多くの脆弱性への対処について、感染したトラフィックを境界線でブロックすること、つまり全システムに修正プログラムをインストールするまでは、ネットワークに対しいかなるトラフィックも許可しないことだと述べています。しかし、ネットワーク・トラフィックをブロックすることは、企業にとって、正当なコミュニケーションを遮断し、Microsoft Exchangeなどのアプリケーションが使用できなくなることを意味します。

社員や支店・支社およびビジネスパートナーを相互接続し、マイクロソフトのアプリケーションを使用している場合、極めて短時間のうちに悪意ある攻撃を受ける可能性を持った脆弱性があり、どちらのオプションも有効ではありません。

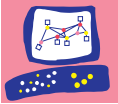
チェック・ポイントのソリューション

VPN-1[®]/FireWall-1[®]に搭載されているチェック・ポイントのApplication Intelligence[™]は、第3のオプションを企業に提供します。本製品はネットワーク全体でアプリケーションを適切に機能させながら、マイクロソフトのアプリケーションを狙った攻撃を防御するだけでなく、インテリジェントで適応性の高いセキュリティを実現します。マイクロソフトのアプリケーションを狙う攻撃を防御する、最も包括的な技術を企業に提供するApplication Intelligenceは、ネットワーク・トラフィックがプロトコル標準およびその正当な使用法を遵守しているかを確認することにより、マイクロソフト環境を攻撃する一般的な方法として知られるバッファ・オーバー・フローと言った不正な攻撃を検知します。

他のソリューションでは、接続性とセキュリティのトレードオフを強要される場合でも、Application Intelligenceであればマイクロソフトのアプリケーションを安全に使用することができます。例えば、Microsoft Exchangeの電子メールを使用するためには、境界線にある多くのセキュリティ・デバイスで、一定範囲のポートを開けるように設定を行う必要がありますが、必要以上にポートを開けることは企業のリスクを増大させることとなります。チェック・ポイントの境界ソリューションは、Exchangeが必要とするアプリケーション・レベルのオペレーションを完全に認識しているため、アプリケーションの必要に応じてダイナミックにポートを開き、トラフィックを検査した上でExchangeの接続を許可します。すなわち、チェック・ポイントのApplication Intelligenceは、単なる接続性のみの提供ではなく、常に安心できる接続性を実現します。



¹Network World

Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

チェック・ポイントのApplication Intelligenceは、以下を代表とするアプリケーションに対応します。

Microsoft Exchange

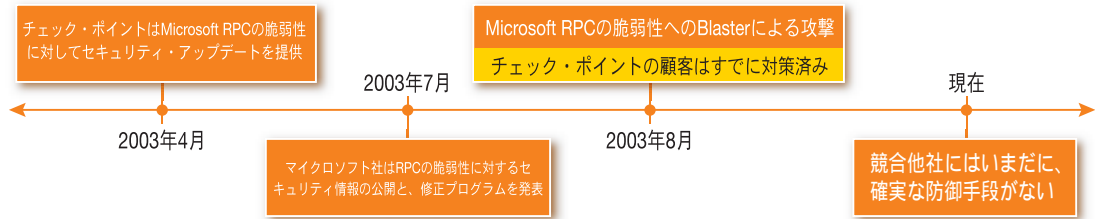
Common Internet File System (CIFS)

Microsoft Remote Procedure Call (DCE-RPC)

MS-SQL

その他

チェック・ポイントのApplication Intelligenceテクノロジーを搭載するVPN-1/FireWall-1は、Windowsに対する多くの攻撃の根本的原因を理解する唯一のセキュリティ・ゲートウェイです。他社のアプリケーションに対する防御ソリューションでは、プロトコルの準拠とシグネチャ・データベースを使用した防御のみを行うのですが、Application Intelligenceはネットワーク内におけるアプリケーションの正しい使用方法を正しく認識しています。こういった意識的なテクノロジーにより、VPN-1/FireWall-1は、ネットワークに対し行われる攻撃手法に亜種や変種がいくつ存在しようが、出現する可能性がある不正な攻撃からマイクロソフトの脆弱性を保護できます。



チェック・ポイントの顧客は、Blaster ワームの出現以前にすでに保護されていました。

ケーススタディ: Application IntelligenceによるMS Blastでの攻撃阻止

2003年7月16日、マイクロソフトは、Windowsの脆弱性を持つリモート・プロシージャ・コール(RPC)の実装についてのセキュリティ情報を重大なアップデートとして公表しました。マイクロソフトは、修正プログラムを提供すると共に、修正プログラムのインストール中に起こりうる攻撃を阻止するための技術文書も提供しました。チェック・ポイント製品以外のセキュリティ・ゲートウェイを使用するユーザは、ゲートウェイの135番ポートを閉じてネットワークへの侵入を防ぐというマイクロソフトが提示した回避策が唯一利用できる手段でしたが、この回避策では、Exchangeなどのマイクロソフトの多くのアプリケーションの機能をブロックしてしまうというものでした。

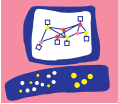
2003年8月11日、BlasterやMS Blastとして良く知られるワームが世界中に拡散しました。直ちに何十万ものコンピュータがワームに感染し、Blasterに感染したコンピュータが自ずから攻撃者となり、脆弱性への対策がなされていない他のコンピュータをスキャンし始めたのです。そのため、ネットワーク全体でのスキャントラフィックが激増し、多くの企業ネットワークが停止し、何百万ドルもの生産性と利益が失われる結果となりました。

Application Intelligenceに対応したチェック・ポイントのソリューションを正しく導入している企業は、正当かつビジネス上重要なアクセスを含むすべてのトラフィックをApplication Intelligenceにより、状況に応じブロックしたり、あるいは通過を許可できるため、自社ネットワークへの正当なデータのアクセスを許可しつつ、Blasterに感染した危険なトラフィックのみを検知し遮断することができたのです。

実際、チェック・ポイントの顧客は、マイクロソフトが7月にセキュリティ情報を発表する3か月前から保護されていました。2003年4月8日、チェック・ポイントは顧客に対し、SmartDefenseアドバイザリを送付し、この勧告と共に配信したアップデートにより、企業はマイクロソフトRPCの脆弱性からマイクロソフトのアプリケーションを保護することができました。マイクロソフトのプロトコルやアプリケーションがネットワーク上でどのように実行されるべきかを理解しているApplication Intelligenceにより、チェック・ポイントでは不正なアクセスや悪意のある攻撃などの脅威に対して効果的な対策ができ、ワームの被害が世界的規模でネットワークで拡大する前から顧客を保護することが可能でした。チェック・ポイントのセキュリティの専門知識やその信頼性を高く評価していた企業は、4ヶ月もの間表面化しなかった攻撃から自社を保護することに世界中で成功したのです。

チェック・ポイントのApplication Intelligenceがブロックする攻撃リストについては、http://www.checkpoint.co.jp/appint/appint_application_layer.htmlをご覧ください。



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

チェックポイント・ソフトウェア・テクノロジーズについて

チェック・ポイント・ソフトウェア・テクノロジーズは、インターネット・セキュリティ分野において世界をリードする企業で、VPN およびファイアウォールの世界市場においてマーケット・リーダーとして評価されています。チェック・ポイントは、境界セキュリティ、企業内セキュリティ、およびWebセキュリティ向けのIntelligent Securityソリューションを提供しています。チェック・ポイントのソリューションは、最もアダプティブでインテリジェントな検査テクノロジーであるINSPECTと、最も低い総保有コストでセキュリティ・インフラストラクチャを管理するSMART管理アーキテクチャをベースとしており、世界中で最も信頼性が高く、広範囲に導入されています。同社のソリューションは、86カ国で認定された1,900社のパートナーによって販売、統合、保守が行われています。詳細については、チェック・ポイントのWebサイト (<http://www.checkpoint.co.jp>または<http://www.opsec.com>) をご覧ください。

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
〒160-0022 東京都新宿区新宿5-5-3 建成新宿ビル6F
<http://www.checkpoint.co.jp> E-mail : info@checkpoint.co.jp Tel : 03(5367)2500

© 2004 Check Point Software Technologies Ltd. All rights reserved. Check Point, Check Pointロゴ, ClusterXL, ConnectControl, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FireWall-1 XL, FloodGate-1, INSPECT, INSPECT XL, InterSpect, IQ Engine, Open Security Extension, OPSEC, Provider-1, Safe@Office, SecureKnowledge, SecurePlatform, SecureXL, SiteManager-1, SmartCenter, SmartCenterPro, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, およびVPN-1 VSXは、Check Point Software Technologies Ltd.およびその関連会社の商標または登録商標です。その他の製品名は、各企業が所有する商標または登録商標です。本文に記載された製品は、米国の特許No. 5,606,668および5,835,726によって保護されています。また、その他の米国における特許や他の国における特許で保護されているか、特許出願中の可能性があります。



Intelligent Security



Check PointTM
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
〒160-0022 東京都新宿区新宿5-5-3 建成新宿ビル6F
<http://www.checkpoint.co.jp/> E-mail : info@checkpoint.co.jp Tel : 03(5367)2500

©2004 Check Point Software Technologies Ltd. All right reserved.
掲載内容を許可なく転載することを禁じます。