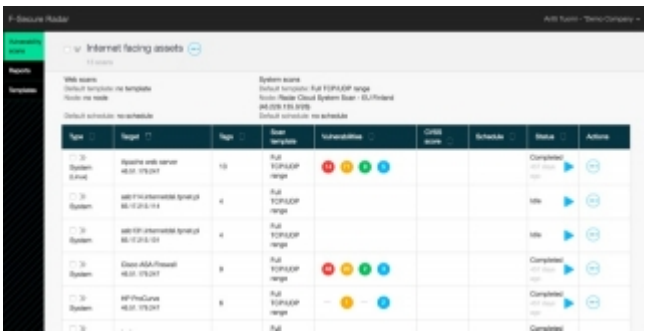
エフセキュア、ITシステムの脆弱性を自動スキャン・管理する「F-Secure Radar」をSecurity as a Serviceとして提供開始



パッチ適用状況、構成エラー、Webアプリの脆弱性を継続的に監視して可視化。
脆弱性へのシンプルな対応だけでも標的型サイバー攻撃を最大85%抑止可能

サイバーセキュリティのリーディングプロバイダー、エフセキュア株式会社（本社：東京都港区、カントリーマネージャキース・マーティン）は、ITシステムの脆弱性をスキャン・管理するソリューション「F-Secure Radar（エフセキュア・レーダー）」を国内販売開始することを発表します。「F-Secure Radar」はPCI ASV認定ソリューションであり、ITシステムの全概要を可視化し、攻撃者がシステム侵害に使用する可能性がある脆弱性を浮き彫りにします。

企業ネットワークへの侵害の多くは、古いソフトウェアやシステムの設定ミス（構成エラー）、Webアプリケーションの脆弱性など、単純なシステムの脆弱性を悪用して行われることがわかっていますが、ネットワーク上で稼動中のすべてのソフトウェアバージョンの把握、設定ミス、Webアプリケーション内の安全でないパスワードなど、脆弱性を継続的に調べるのはかなりの作業負荷で、複数のシステム、サーバー、プラットフォームがあればなおさらです。

「F-Secure Radar」は、ITシステム分析のためのさまざまな自動スキャン機能を備えており、サーバー、デスクトップ、ルータ、プリンター、そしてネットワークに接続されているその他の資産も含め、ネットワーク全体とすべての資産を可視化し、脆弱性を特定するとともに、深刻度に基づいて脆弱性を評価します。

尚、エフセキュアは、明日10月20日 から新宿で開催される情報セキュリティに関する日本最大級の国際カンファレンス「CODE BLUE(コードブルー)」に参加し、「F-Secure Radar」を展示・デモンストレーションし、2016年12月1日 より国内サービスプロバイダー向けに販売開始します。

エフセキュアのRadarサービス担当ディレクターであるRune Kristensenは次のように述べています。
「可視化は重要な防御措置です。当社は、企業が今後も可視性をさらに高められるように、Radar

の機能をさらに拡大していく考えです。たとえば、多くの企業が、セキュリティに十分な注意を払わず、時にはIT担当者に連絡することなく、あるサービスを第三者に外部委託することがあるので、エフセキュアは、企業ネットワークに統合されている第三者のサービスもスキャンできる方法を開発中です。これにより、企業は、そのデータサプライチェーンの脆弱性がどのように攻撃にさらされるかについて、きわめて重要な可視性を得ることが可能になるのです。」

◆「F-Secure Radar」の機能と特長

（1）Security Center
レポート、脆弱性管理、インシデント対応などを可視化するダッシュボード。
APIによりサードパーティ製品との統合が可能

（2）Discovery Scan
ネットワークホスト、非同期ポートの高速スキャン

（3）System Scan
構成エラー、不適切なパッチ管理などに関連するシステムの脆弱性を特定

（4）Web Scan
さまざまなWebアプリケーションにおけるセキュリティ脆弱性をスキャンして検知
「OWASP Top 10」を含む膨大な脆弱性をテスト

※「F-Secure Radar」に関して以下のセキュリティブログもご参照ください。
https://jp.business.f-secure.com/software-vulnerabilities-the-key-to-your-systems/

◆ 標的型サイバー攻撃を最大85%抑止するとされる脆弱性の改善

エフセキュアが「F-Secure Radar」を使って2016年初頭に行った調査によると、最も頻繁に発見される脆弱性トップ100は、企業ネットワークでは約85,000件特定され、そのうち約7%は、National Vulnerability Database（全国脆弱性データベース）の基準によると、非常に深刻度の高いものです*。
さらに、これらの深刻な脆弱性のほぼ半分は、セキュリティ侵害に悪用される可能性があり、攻撃者がリモートでコードを実行して、侵害したコンピュータを掌握することも考えられます。しかし、悪用される可能性のある脆弱性のうちほぼすべてが、適切なソフトウェアパッチの適用や管理上のシンプルな変更によって、容易に修正できるのです。
米コンピュータ緊急事態対策チーム（United States Computer Emergency Readiness Team）は、脆弱なソフトウェアへのパッチ適用など、簡単なステップをいくつか行うことで、標的型サイバー攻撃を最大85%抑止できるとしています**。

……
*出典：https://nvd.nist.gov/cvss.cfm
**出典：https://www.us-cert.gov/ncas/alerts/TA15-119A?hootPostID=b6821137ae5173095390bd502ae04892
……

◆ 脆弱性は「侵入歓迎」の合図

今回の調査結果では、数多く特定された深刻度の高い脆弱性の中でも、システムの構成エラーによる脆弱性が最も多いことが指摘されました。最も頻繁に発見される脆弱性トップ10は、深刻度は低または中ですが、調査で見つかった全脆弱性の61%を占めています。これらの問題は、高リスクの脆弱性ほど深刻ではありませんが、もっと調べて他の脆弱性を探そうとハッカーに思わせるに十分なものです。

エフセキュアのテクノロジーアウトリーチ担当シニアマネージャAndy Patelは、次のように述べています。「このような問題は、本来は特に切実なものではありませんが、些細な問題もサイバーセキュリティの問題ととらえるハッカーにとっては、『侵入歓迎』の合図にも等しいのです。何気なくウェブを閲覧しているときでも、このような脆弱性に偶然出くわすことがよくあります。悪事には無関心のハッカーでさえ、そこで何か悪事を行ったらどうなるのか知りたいという誘惑に駆られるかもしれません。幸運な企業なら、問題を警告してくれる親切なEメールを受け取れるかもしれませんが、不運な企業は、標的型攻撃の準備のために偵察をしているプロの犯罪者を呼び込んでしまうでしょう。」

■エフセキュアについて

https://www.f-secure.com/ja_JP/
エフセキュアは、オンラインセキュリティおよびプライバシー保護を提供するフィンランドの企業です。エフセキュアの製品は数多くの受賞実績があり、クライムウェアから企業へのサイバー攻撃にいたる全ての脅威から人々と企業を守ってきました。現在、世界40か国以上、6,000以上のパートナーが販売しており、また、200以上のクラウドサービスでも提供されています。「Switch on freedom」をスローガンに掲げ、全世界の人々が安全に“つながる”ことができるよう支援することを使命としています。エフセキュアは、1988年に創業し、NASDAQ OMX Helsinki Ltdに上場しています。エフセキュア株式会社は、エフセキュア社100%出資の現地法人として1999年に設立され、以降、増収を続けながら順調に企業規模を拡大しています。

Generated by ぷれりりプレスリリース
https://www.prerele.com