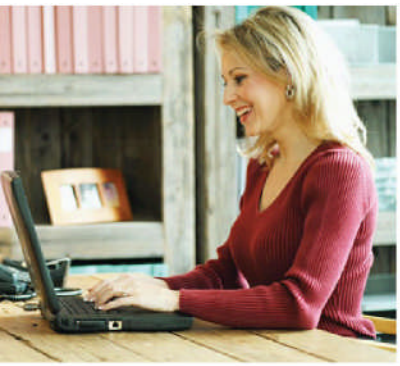
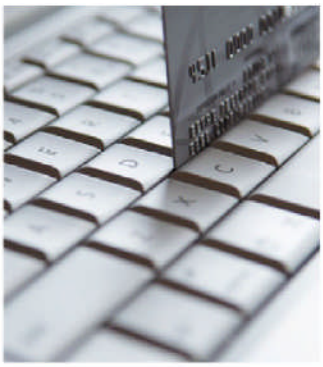
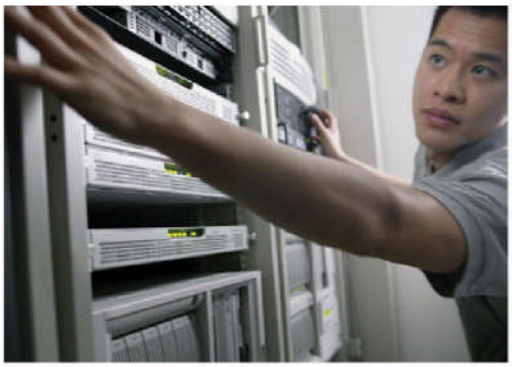
Güçlü Web uygulaması koruması ile BT güvenliği yatırımınızı iyileştirin

IBM Internet Security Systems – Proventia Web uygulaması güvenliği


Öne Çıkanlar

- *Bağımsız bir Web uygulaması güvenlik duvarına ek yatırım yapılmasını gerektirmeyen, daha zengin, daha az karmaşık bir Web güvenliği çözümü sağlamak üzere tasarlandı*
- *Potansiyel iş kesintilerini ve güvenlik açıklarını sınırlamak için proaktif Web uygulaması, Web 2.0 ve veritabanı koruması sunar*
- *Yasal uyumluluk gereksinimlerinin ve PCI DSS dahil olmak üzere endüstri standartlarının karşılanmasına yardımcı olur*

Web uygulamaları için koruma ile BT güvenliği çözümünüzün güçlendirilmesi

Web uygulamaları, müşterileriniz ile daha yakın etkileşimler kurmanıza ve çalışanlarınızla işbirliğini geliştirmenize yardımcı olabilir. Ancak, son birkaç yılda neredeyse her ölçekten kuruluşların karşılaştığı Web ile bağlantılı tehditlerin sayısı önemli ölçüde artmıştır. Bu saldırıların yarısından fazlasında Web uygulamaları hedeflenmiştir.

2008 yılı sonu itibariyle, tüm açıklanan Web güvenlik açıklarının yaklaşık dörtte üçü için yama mevcut olmaması daha da rahatsız edicidir. Önemli bir güvenlik açığı alanı olan Yapılandırılmış Sorgu Dili (SQL) injection saldırıları, son altı ay içinde 30 kat artmıştır.[1] Hassas verileri hedefleyen ve giderek yaygınlaşan bu saldırılar, kullanıcılar tarafından girilen verileri işlemek için arka uç kodunu değiştirerek Web sitelerini istismar etmektedir.

Saldırılardaki artışın nedenlerinden biri, geliştirilen Web uygulamalarının sayısındaki büyük artıştır. Sahip oldukları potansiyele karşın, bu yeni, işbirliği odaklı bilgi paylaşımı yöntemlerinin etkileşimli yapısı, bu yöntemleri saldırılara karşı çok hassas ve savunmasız hale getirmektedir. İşinizi ve itibarınızı korumak için şirketinizin güvenlik çözümlerini geliştirecek yollar bulmanız gerekmektedir.

IBM Internet Security Systems™ – Proventia® Web uygulaması güvenliği, web ile ilgili güvenlik açıklarının ortadan kaldırılmasına ve güvenlik yapınızın güçlendirilmesine yardımcı olabilir. IBM Proventia ağ ve sunucu güvenliği ürünlerinin en son modellerine bütünleştirilen bu özellik, ağ, ağ geçidi ve sunucu düzeylerindeki saldırıları denetlemenize yardımcı olabilir.

IBM Internet Security Systems (ISS) X-Force® araştırma ve geliştirme ekibinin güvenlik uzmanlığı ile desteklenen benzersiz iletişim kuralı analiz modülü (PAM), ISS çözümlerinin çekirdek teknolojisi olarak derin paket denetlemesi sağlanmasına yardımcı olur. Bu çözüm, ilke uygulama, çok parçacıklı kimlik doğrulama ve yetkilendirme, gelişmiş XML tehdidi koruması ve hızlandırılmış Güvenli Yuva Katmanı (SSL) işleme dahil olmak üzere IBM WebSphere® DataPower® aygıtlarının gelişmiş güvenlik

İletişim kuralı analiz modülü (PAM) teknolojisi

IBM iletişim kuralı analiz modülü (protocol analysis module - PAM), geleneksel izinsiz giriş önleme sisteminin ötesinde ağ ve sunucu koruması sunmak için güvenliğin birleştirilmesini sağlar. PAM, kapsamlı korumaya olanak sağlayan modüler yapısıyla artık Web koruma teknolojilerini de içermektedir.

yeteneklerinden yararlanarak, izinsiz girişlerin tanımlanmasına yardımcı olur ve Web uygulamaları ile arka uç veritabanlarına gönderilen kötü niyetli paketlerin engellenmesini destekler.

Bağımsız bir Web uygulaması güvenlik duvarı satın almak yerine, güvenilir ISS güvenlik çözümlerinde önceden etkinleştirilmiş Web korumasının avantajından yararlanabilirsiniz. Örneğin:

- *IBM Proventia Network Intrusion Prevention System,* geniş bir İnternet tehditleri yelpazesine karşı önleyici korumanın etkinleştirilmesine yardımcı olur*
- *IBM Proventia Server Intrusion Prevention System, verilerin ve uygulamaların güvenilir, kullanılabilir ve gizli tutulmasına yardımcı olur*
- *IBM RealSecure® Server Sensor, kritik önem taşıyan kurumsal sunucular üzerindeki olayları, ana bilgisayar günlüklerini, gelen ve giden ağ etkinliğini analiz ederek otomatikleştirilmiş, yaklaşık gerçek zamanlı izinsiz giriş belirleme ve önleme sağlar*
- *IBM Proventia Network Multi-Function Security,* yetkisiz giriş, ağ saldırıları, kötü niyetli kod, karışık tehditler, içerik tabanlı saldırılar, casus yazılım ve e-dolandırıcılık gibi çeşitli tehditlerle aynı anda mücadele edilmesine yardımcı olur*

Proventia ürün serisine güç veren PAM motoru, Web korumanın geliştirilmesine ek olarak, proaktif güvenlik yöntemlerinin benzersiz bir birleşimini de sağlar. Bunlar arasında:

- *IBM Virtual Patch® yönetimi aracılığıyla önleyici tehdit koruması, yamaların takip edilmesi gereksinimini ortadan kaldırır*
- *Hem bilinen, hem de bilinmeyen tehditlerin engellenmesine yardımcı olan tehdit belirleme ve önleme teknolojileri*
- *Veri kaybı önleme çabalarının geliştirilmesi için içerik analizi*
- *Uyumluluğun sağlanmasına yardımcı olmak için ağ ilkesi uygulama*

Ayrı bir Web güvenliği noktası ürünü satın alınması ve yönetilmesi gereksiniminin ortadan kaldırılması

IBM, en son izinsiz giriş önleme ürünleri modellerinin çekirdek motoruna geliştirilmiş güvenlik yetenekleri yerleştirerek, bağımsız Web uygulaması güvenlik duvarları kullanmanın ek maliyetinden ve karmaşıklığından kaçınmanıza yardımcı olabilir. Tipik güvenlik çözümlerine göre önemli bir avantaj olarak ağınız, sunucunuz ve Web uygulamalarınız için proaktif bir koruma düzeyi sağlamak amacıyla tüm çözümlerimiz benzersiz bir injection mantığı motoru (injection logic engine - ILE) içermektedir. IBM'in en son ağ ve sunucu izinsiz giriş belirleme ve önleme çözümlerini kullanıyorsanız, özellikle Web uygulamalarınız için güçlü koruma sağlama yeteneğine zaten sahipsiniz demektir. Bu nedenle ek teknoloji yatırımı yapmanıza gerek yoktur ve tüm çözümü tek IBM Proventia Management SiteProtector™ sistemi veya IBM ISS Yönetilen Güvenlik Hizmetleri aracılığıyla yönetebilirsiniz.

Web korumasına proaktif bir yaklaşım sağlanması

Proventia Web uygulaması güvenliği, destek olarak ILE'yi kullanarak Web uygulamalarınıza yönelik saldırıların engellenmesine yardımcı olur. ILE, geçerli Web taleplerinde genellikle görülmeyen özgün kalıplar çağırarak injection saldırılarının önceden engellenmesine yardımcı olur. ILE, belirli anahtar kelimeleri ve simgeleri toplayarak ve puanlayarak SQL injection saldırılarını belirleyebilir ve engelleyebilir. ILE, güvenlik ihlallerine tespit edilmelerinin ardından tepki vermek yerine injection saldırılarına karşı saldırı taktiği uygular. ILE, kapsamlı SQL sözdizimsel çağrı listesi aracılığıyla sisteminizi aşağıdaki şekilde korur:

- *Parametre değerlerinin değerlendirilmesi ve puanlanması*
- *Puanlama eşiğini aşan taleplerin engellenmesi*
- *Gerçekleşen SQL injection tipinin tanımlanması için belirli anahtar kelime kombinasyonlarının etiketlenmesi*

Web uygulaması güvenliğine yönelik bu proaktif yaklaşım, sadece saldırıları denetleyen ve tepki veren pek çok Web koruma çözümünden farklıdır.

Proventia Web uygulaması güvenliği, aşağıdakiler için birincil saldırı kaynaklarının ele alınmasına yardımcı olur:

- *Web uygulamaları - kabuk komutu injection saldırılarının, sunucu tarafı ekleme (SSI) injection saldırılarının, siteler arası komut dosyası oluşturmanın (XSS) ve dizinde gezinmenin engellenmesine yardımcı olur*
- *Veritabanları - SQL, Hafif Dizin Erişimi İletişim Kuralı (LDAP) ve XML Yol Dili (XPath) injection saldırılarının engellenmesine yardımcı olur*
- *Web 2.0 - Java™ Komut Dosyası Nesnesi Noktasyonu (JSON) ele geçirme, potansiyel siteler arası talep sahteciliği (CSRF) saldırılarının ve gelişmiş siteler arası komut dosyası oluşturma yöntemlerinin engellenmesine yardımcı olur*

Verilerinizin ve itibarınızın korunmasına yardımcı olurken aynı zamanda uyumluluk girişimlerini kolaylaştırır

Proventia Web uygulaması güvenliği, uyumluluk gereksinimlerini ve Ödeme Kartı Endüstrisi (PCI) Veri Güvenliği Standardı (DSS) 6.6 gibi endüstri düzenlemelerini daha kolay yönetmenize yardımcı olur. Bu standart, müşterilerinizin ödeme kartı işlemlerine yönelik yüksek güvenlikli bir ortam sağlanması için gerekli olan güvenlik yönetimi, ilkeler, prosedürler, ağ mimarisi, yazılım tasarımı ve diğer kritik önem taşıyan koruyucu önlemler için gereksinimler içerir. Aynı zamanda, verileriniz için daha fazla güvenlik sağlayabilir ve itibarınızı koruyabilirsiniz. IBM, Proventia Web uygulamasını geniş izinsiz giriş önleme sistemi çözümleri yelpazesine ekleyerek PCI DSS 6.6 ile uyumluluğun yönetilmesini kolaylaştırır.

Neden IBM?

Proventia Web uygulaması güvenliği, Web uygulamalarınızın güvenlik açıklarına karşı güçlendirilmesine yardımcı olmak için uygun maliyetli bir çözüm sağlamak üzere tasarlanmıştır. Bu çözüm, güvenlik açıklarını ve sorunlarını değerlendiren, IBM ISS ürünleri için değerlendirmeler ve karşı önlem teknolojisi geliştiren ve halkı gelişmekte olan İnternet tehditlerine karşı eğiten IBM'in X-Force güvenlik uzmanları ekibinden yararlanır.

Güvenlik açıklarının verilerinizin açığa çıkmasına, itibarınızın tehlikeye atılmasına ve hatta işinizin kesintiye uğramasına neden olması durumunda, Proventia Web uygulaması güvenliği, size bağımsız Web uygulaması güvenlik duvarı satın alınmasına veya kurulmasına gerek kalmaksızın kapsam sağlanması konusunda yardımcı olabilir. Ayrıca, güvenlik yeteneklerinizin değerlendirilmesine ve ardından BT ve iş gereksinimleriniz için en uygun çözümün tasarlanmasının ve devreye alınmasının planlanmasına yardımcı olmak için IBM ISS profesyonel hizmetlerinin beceri ve deneyimlerinden yararlanabilirsiniz.

Aynı zamanda, personeliniz üzerindeki iş yükünü azaltmak için ortamınızın izlenmesine ve yönetilmesine yönelik yönetilen koruma hizmetleri de sağlıyoruz. Ayrıca, IBM Rational® AppScan® ürünleri ve hizmetleri, Web uygulamalarınızın güvenlik riski analizini gerçekleştirebilir. ISS ürün portföyü ve hizmetleri, güvenlik açıklarınızın nerede bulunduğu ve nasıl korunacağı konusunda daha az endişelenerek yeni iş girişimlerine odaklanmanıza yardımcı olur.

Daha ayrıntılı bilgi için

Proventia Web uygulaması güvenliği hakkında daha ayrıntılı bilgi edinmek için lütfen Web sitemizi ziyaret edin: ibm.com/services/security.

© Copyright IBM Corporation 2009

IBM Global Services
Route 100
Somers, NY 10589

Amerika Birleşik Devletlerinde hazırlanmıştır.
Nisan 2009
Her Hakkı Saklıdır

IBM, IBM logosu, ibm.com, AppScan, DataPower, Internet Security Systems, Proventia, Rational, RealSecure, SiteProtector, Virtual Patch, WebSphere ve X-Force, International Business Machines Corporation şirketinin ABD'de ve/veya diğer ülkelerde geçerli markaları veya tescilli markalarıdır. Bu belgede bunlar veya diğer IBM markalı terimler tescilli marka işareti (® veya ™), ile işaretlenmişse, bu işaretler bu belgenin yayınlandığı tarih itibariyle IBM'in sahip olduğu ABD'de tescilli markaları veya markaları ifade etmektedir. Bu gibi ticari markalar diğer ülkelerde de tescilli veya özel hukuk kapsamındaki ticari markalar olabilir. IBM ticari markalarının bir listesi, **ibm.com**/legal/copytrade.shtml İnternet adresinde "Telif ve marka bilgileri" başlığı altında mevcuttur.

Java ve Java tabanlı diğer tüm ticari markalar ve logolar Sun Microsystems, Inc. firmasının ABD'de ve/veya diğer ülkelerdeki ticari markalarıdır.

Diğer şirket, ürün veya hizmet adları farklı şirketlerin ticari veya hizmet markaları olabilir.

1 2008 X-Force Eğilim ve Risk Raporu. IBM Internet Security Systems.

* Proventia Web uygulaması güvenliği, ağ izinsiz giriş önleme hizmetleri ürün serilerinin MX ve GX modellerinde yerleşik olarak mevcuttur.

Bu belgede IBM ürünlerine veya hizmetlerine yapılan atıflar, IBM'in söz konusu ürün veya hizmetleri faaliyet gösterdiği tüm ülkelerde sunacağı anlamını taşımaz.

Sorumluluğun Reddi: Yasal gereksinimlere uyum sağlanması müşterinin sorumluluğundadır. Müşterinin işini etkileyebilecek tüm ilgili yasalar ile yönetmelik gereksinimlerinin ve okuyucunun bu yasalara uyum sağlaması için uygulaması gereken etkinliklerin tanımlanması ve yorumlanması amacıyla yetkin bir hukuk danışmanına başvurulması sadece müşterinin sorumluluğundadır. IBM herhangi bir yasal danışmanlık sağlamadığı gibi, hizmetlerinin veya ürünlerinin müşterinin herhangi bir yasa veya yönetmeliğe uyum sağlamasına olanak tanıyacağını da beyan veya garanti etmemektedir.

Recyclable, please recycle

SES03002-USEN-00