Verilerinizi daha geniş kapsamlı, daha derinlemesine sunucu koruması ile koruyun

IBM ISS Tehdit Azaltma Hizmetleri - uç nokta sistemi koruma - sunucu koruma

Öne Çıkanlar

- ***Şifreli Web işlemleri üzerinden tünel oluşturanlar da dahil olmak üzere çok sayıda saldırı türüne karşı koruma sağlamak amacıyla tasarlanmıştır***
- ***En derin ağ düzeylerinde üstün koruma sunmak için çok sayıda inceleme teknolojisini birleştirir***
- ***Veri gizliliğinin sağlanmasına yardımcı olur ve kapsamlı izleme aracılığıyla yasal uyumluluğu kolaylaştırır***
- ***Merkezileştirilmiş güvenlik yönetimi ve çok sayıda işletim sistemi için kapsamlı destek aracılığıyla maliyetin ve karmaşıklığın azaltılmasını destekler***
- ***Sanallaştırmanın avantajlarından yararlanmanıza yardımcı olur***

Savunma stratejinizin derinleştirilmesi

Her yıl, her iki kuruluştan biri güvenlik duvarına ve virüs önleme korumasına sahip olmasına karşın ciddi bir güvenlik ihlali yaşar ve bu durum ihlal başına ortalama 6.6 milyon ABD dolarına mal olmaktadır1. İşletim sistemi ve uygulama yamaları, sürekli devam eden saldırıları önlemeye çalışsa da, Web saldırılarındaki büyük artıştan da anlaşılacağı gibi, bilgisayar korsanları, Web uygulamaları aracılığıyla giderek daha yüksek miktarda hassas veri çalmaktadır. Kasıtsız veya kasıtlı dahili ihlaller de potansiyel güvenlik tehlikeleri olmayı sürdürmektedir.

IBM Internet Security SystemsTM (ISS) X-Force® araştırma ve geliştirme ekibi tarafından desteklenen IBM Internet Security Systems – sunucu koruması, sunucularınızı giderek artan saldırı yöntemlerine karşı korumaya ve kapsamlı izleme, kayıt ve denetleme yetenekleri ile uyumluluğu daha ayrıntılı olarak yönetmeye yardımcı olmak için çok katmanlı izinsiz giriş önleme ve belirleme sağlamaktadır.

IBM ISS - sunucu koruması, iki kanıtlanmış ürün tarafından sağlanır: IBM Proventia® Server Intrusion Prevention System (IPS) ve IBM RealSecure® Server Sensor. Bu ürünlerin her biri, geniş bir işletim sistemleri yelpazesini destekler ve hizmet engelleme, uzaktan izinsiz yetki kazanma, SQL injection ve siteler arası komut dosyası oluşturma gibi çeşitli saldırılara karşı güçlü güvenlik sağlar.

En yüksek düzeyde iş hacmi ve çalışma süresi sürdürülürken sunucuların korunması

Güvenlik, tüm bileşenlerinin toplamıdır. IBM ISS - sunucu koruması, diğer sunucu koruma çözümlerinin aksine, altı güvenlik katmanından biri olarak derin paket inceleme sağlar. Proventia Server IPS ve RealSecure Server Sensor ürünleri, engelleme yetenekleri arasında aşağıdakileri sağlar:

- *Hem başarılı, dış bilgisayar korsanlarının, hem de güvenlik açıklarınızı daha iyi hedefleyebilecek dahili kaynakların tehditlerini azaltmanızı sağlayarak denetimi elinizde tutmanıza yardımcı olan bir **güvenlik duvarı**.*
- *Sistem, ağ, uygulama düzeyi tehditlerine ve dahili tehditlere karşı doğru, önleyici koruma sağlanmasına yardımcı olmak için çok sayıda savunma katmanından yararlanan **izinsiz giriş önleme sistemi**.*

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.

- *Bir güvenlik açığı yaması yayınlanmış olup olmamasına bakılmaksızın, bilinen ve bilinmeyen saldırıların önlenmesine yardımcı olan **IBM Virtual Patch® teknolojisi**.*
- *Bilinen ve bilinmeyen önbellek taşması güvenlik açıklarının istismar edilmesinin önlenmesine yardımcı olması için **arabellek taşması istismarı koruması (buffer overflow exploit prevention - BOEP)**.*
- *Çalışan yetkisiz uygulama sayısını azaltarak sunucuların kötü niyetli etkinliklere maruz kalma olasılığını azaltmak için uygulama ilkelerini uygulamanıza yardımcı olan **uygulama siyah ve beyaz listeleri**.*
- *Web uygulamasına iletilmeden önce **güvenli Web işlemlerini inceleme becerisi**.*

IBM ISS - sunucu koruması, tüm IBM ISS güvenlik teknolojisinin temelini oluşturan iletişim kuralı analiz modülü (PAM) adı verilen derin paket inceleme motoruna sahiptir.

PAM, çok sayıda inceleme teknolojisini birleştirerek diğer sunucu koruma çözümlerinin sunduklarının çok daha ötesinde, kapsamlı ve proaktif savunma sağlar. Ayrıca, IBM ISS - sunucu koruması, mevcut BT altyapınızla sorunsuz bir şekilde bütünleşerek kurallara uygun trafik akışlarının kesintisiz olarak sürdürülmesini sağlar, böylece verilerinizi kötü niyetli yazılımlara karşı korurken işinizi sorunsuz bir şekilde yürütmeye devam edebilirsiniz.

Veri gizliliği ve yasal uyumluluk önlemlerinin kolaylaştırılması

IBM ISS - sunucu koruması, Ödeme Kartı Endüstrisi (PCI) Veri Güvenliği Standardı (DSS) ve Sağlık Sigortası

Taşınabilirlik ve Sorumluluk Yasası (HIPAA) gibi standartların ve düzenlemelerin yanı sıra dahili güvenlik standartlarına da uyumluluğunuzu yönetmenize yardımcı olmak için dört tip izlemeyi birleştirir:

- ***Sistem bütünlüğü izleme**, kullanıcıların işletim sistemiyle ve uygulamalarla olan etkileşimlerini size bildirir ve kimin oturum açtığına, hangi işlemleri yaptığına ve ne zaman oturumu kapattığına ilişkin bilgiler sağlar.*
- ***Dosya bütünlüğü izleme**, kullanıcıların hassas dosyalar ve klasörler ile olan etkileşimini izleyerek Sarbanes-Oxley gibi yoğun veri bütünlüğü standartlarını karşılamanıza yardımcı olur. Bu teknolojinin temel kullanım alanı, sisteme yapılan müdahalelerin belirlenmesi ve hassas verilere erişimin izlenmesidir.*
- ***Kayıt dosyası bütünlüğü izleme**, aynı zamanda kayıt dosyası anahtarları üzerindeki başarılı ve başarısız işlemlerin izlenmesi ve kaydedilmesi ve potansiyel güvenlik açığı noktalarını tanıyabilecek yönetici ve kullanıcı davranışlarının adli inceleme yolunun oluşturulması (bazı standartlarda raporlama için gereklidir) yoluyla veri bütünlüğü standartlarını karşılamanıza yardımcı olur.*
- ***Üçüncü kişi günlük dosyası izleme**, potansiyel güvenlik tehditleri oluşturan üçüncü kişi uygulamalarının tetiklediği olayları takip etmenize yardımcı olur.*

IBM ISS - sunucu koruması aynı zamanda, sunucuların en son virüs önleme güncellemelerini aldığının doğrulanması için virüs önleme uygulama özelliğine sahiptir ve uyumsuz sunucuları bildirir. Proventia Server for Microsoft® Windows®, ana bilgisayar izinsiz giriş önleme sistemleri (HIPS) ve PCI uyumluluğu açısından LSS laboratuvarları tarafından tasdik edilmiştir.

Geniş bir işletim sistemleri yelpazesi çapında güvenliğin basitleştirilmesi

IBM ISS - sunucu koruması, Microsoft Windows, Linux®, IBM AIX®, UNIX®, Solaris ve HP-UX dahil olmak üzere geniş bir kurumsal işletim sistemleri yelpazesi çapında izinsiz giriş önleme ve belirleme sağlamak üzere tasarlanmıştır. Aynı zamanda, güvenlik aygıtları, ilkeleri, olay analizi, uyarılar ve iş akışları için IBM Proventia Management SiteProtector® sistemi aracılığıyla tüm çözüm üzerinde, basit, rehberli denetime sahip olmanızı sağlar. Tek arabirim aracılığıyla, çok sayıda yönetim aracını devreye almak ve öğrenmek için zaman ve para harcamaksızın izleyebilir, analiz edebilir, ayarlamalar yapabilir ve raporlar oluşturabilirsiniz.

Sanallaştırma aracılığıyla BT operasyonlarının optimize edilmesi

IBM ISS - sunucu koruması, sunucu ve işletim sistemi düzeylerinde güvenliği sağlamanıza yardımcı olurken, aynı zamanda sunucu sanallaştırmanın sunduğu yatırım getirisini elde etmenize yardımcı olmaya hazır sanal bir ortamdır. Sanal makine merkezli koruma, HIPS aracının kurulu olduğu sanal makinelere/makinelerden ağ trafiğini analiz ederek sanal ağ için iletişimlerin güvenliğini sağlar. Bir diğer önemli avantajı, sanal makine bir fiziksel ana bilgisayardan diğerine taşınırken korumanın sürdürülmesi aracılığıyla taşınabilirliğin desteklenmesidir. IBM ISS - sunucu koruması, sürekli güvenlik sağlamak için tasarlanmıştır ve aşağıdaki ortamlar için destek sunar:

- *VMware ESX*
- *Windows Server 2008 Hyper-V*
- *IBM Power Systems™ mantıksal bölümler ve iş yükü bölümleri*
- *Hewlett-Packard vPars ve nPars*
- *Solaris Container*

Neden IBM?

IBM ISS - sunucu koruması, dünyanın en kapsamlı güvenlik açığı veritabanına sahip olan ve araştırmaları ve tehdit analizi ile bilgisayar korsanlarının bir adım ilerisinde olmayı sürdüren güvenlik çözümlerinin geliştirilmesine katkı sağlayan dünyaca ünlü X-Force ekibi tarafından desteklenmektedir. IBM'in danışmanlık hizmetleri ve becerikli hizmet profesyonelleri, çözümünüzün değerlendirilmesinde, tasarlanmasında ve devreye alınmasında veya daha kapsamlı yönetimde size yardımcı olabilir. IBM Yönetilen Koruma Hizmetleri (Managed Protection Services - MPS), pek çok farklı platform ve işletim sistemi çapındaki kritik önem taşıyan sunucu aygıtları çapında gerçek zamanlı, 24 saat koruma ve canlı, uzman yönetimi, izleme ve üst seviyelere yükseltme sağlar.

Daha ayrıntılı bilgi için

IBM ISS - sunucu koruması hakkında daha ayrıntılı bilgi için lütfen IBM temsilcinizle veya IBM Çözüm Ortağınızla iletişim kurun veya aşağıdaki Web sitesini ziyaret edin:

ibm.com/services/security

IBM, önceden bildirmeksizin belirtimlerde veya diğer ürün bilgilerinde değişiklik yapma hakkını saklı tutar. Bu yayın, teknik hatalar veya dizgi hataları içerebilir.
IBM BU YAYINI "OLDUĞU GİBİ", TİCARİLİK VEYA BELİRLİ BİR AMACA UYGUNLUĞA İLİŞKİN ZIMNİ GARANTİLER VE KOŞULLAR DA DAHİL, ANCAK BUNLARLA SINIRLI OLMAMAK ÜZERE, AÇIK VEYA ZIMNİ HİÇBİR GARANTİ VEYA KOŞUL BELİRTMEKSİZİN SUNMAKTADIR. Bazı ülkelerin yasaları, belirli işlemlerde açık veya zımni garantilerin reddine izin vermemektedir; buna bağlı olarak bu ifade sizin için geçerli olmayabilir. Buradaki bilgilerin kullanımından doğacak risk kullanıcının sorumluluğundadır. Burada bulunan bilgiler önceden bildirilmeksizin değiştirilebilir veya güncellenebilir. IBM, burada açıklanan ürün ve/veya programlarda önceden bildirmeksizin iyileştirmeler ve/veya değişiklikler yapabilir.

Bu belgede bahsi geçen IBM ve IBM dışı ürünlere ve hizmetlere ilişkin performans verileri, belirli işletim ve ortam koşullarında elde edilmiştir. Herhangi bir kişi tarafından söz konusu ürünlerin veya hizmetlerin uygulanması sırasında elde edilecek gerçek sonuçlar, söz konusu kişinin işletim ortamına özgü çok sayıda etkene bağlı olacaktır ve önemli ölçüde farklılık gösterebilir. IBM, bu sonuçların söz konusu ürün ve hizmetlerin herhangi bir uygulamasından beklenebileceğine veya elde edilebileceğine ilişkin herhangi bir beyanda bulunmaz.

Bu belgede bulunan üçüncü kişilere ilişkin tüm malzemeler, söz konusu kişilerden elde edilen bilgilere dayanmaktadır. Bilgilerin doğruluğunun bağımsız olarak doğrulanması için herhangi bir girişimde bulunulmamıştır. Bu belge, IBM tarafından herhangi bir üçüncü kişi ürününün veya hizmetinin açık veya zımni olarak önerildiği veya desteklendiği şeklinde yorumlanamaz.

1 CSI/FBI Computer Crime & Research Survey and Ponemon / PGP: U.S. Cost of a Data Breach Study.

IBM Global Services
Route 100
Somers, NY 10589 U.S.A.

Amerika Birleşik Devletlerinde hazırlanmıştır. Haziran 2009

SED03065-USEN-00