

PRINCIPAIS BENEFÍCIOS

Abordagem personalizada

O princípio básico do MVPS é a flexibilidade. A VeriSign trabalha com cada cliente para tratar de pontos de entrada de informações (como, por exemplo, conexões de Internet, DMZ (demilitarized zone - zona desmilitarizada), redes internas, aplicativos sem fio e da Web etc.) e, então, desenvolve um programa ideal para lidar de maneira eficaz com a profundidade e a frequência dos testes de vulnerabilidade deste cliente específico.

Inteligência inigualável em segurança

O MVPS maximiza a VeriSign® Intelligence para garantir inteligência em segurança dentro da empresa, entre empresas e na Internet. A VeriSign possui uma visibilidade única em relação a ameaças de segurança na Internet, por gerenciar serviços de infra-estrutura de Internet como o DNS (Serviço de Nomes de Domínio). Os clientes ganham uma visão em tempo real do estado e da integridade de suas arquiteturas de segurança como resultado do acesso a informações e da habilidade da VeriSign em correlacionar essas informações de uma ampla base de dados de ameaça.

Serviços abrangentes

O MVPS oferece uma variedade de serviços que, juntos, fornecem um programa de gerenciamento de vulnerabilidade abrangente, levando em consideração a frequência, além da amplitude e da profundidade das avaliações de vulnerabilidade.

VeriSign® Managed Vulnerability Protection Service (MVPS)

Aumentar a velocidade dos negócios é uma proposta atraente para qualquer empresa que esteja tentando acompanhar o clima acelerado do mercado atual. Para que uma empresa se mantenha competitiva, a disponibilidade contínua de aplicativos e redes de TI internas e externas é de extrema importância. Como consequência, os ambientes corporativos atualmente incluem tecnologias complexas conectadas a outras organizações, como parceiros, fornecedores e clientes. Embora a tecnologia e a interconectividade melhorem a eficiência dos negócios, os aplicativos de base e as configurações de rede subjacentes criam vulnerabilidades de TI. Se as medidas de segurança apropriadas não forem estabelecidas, essas vulnerabilidades irão expor uma organização a riscos que incluem crime cibernético, vírus e worms.

Muitas organizações substituíram as auditorias de segurança anuais por verificações de integridade de vulnerabilidade para reduzir os riscos associados à crescente interconectividade e dependência da tecnologia. Apesar de todas as precauções, um número recorde de incidentes ainda ocorre. Além disso, as empresas estão descobrindo as limitações de uma abordagem voltada para a rede e agora estão explorando outros pontos de acesso para os aplicativos empresariais cruciais que não estão sendo adequadamente avaliados. Para obter a máxima proteção, uma organização precisa de um programa de gerenciamento de vulnerabilidades abrangente que considere a frequência, bem como a amplitude e a profundidade das avaliações de vulnerabilidade.

+ Abordagem

Tomar as medidas apropriadas para salvaguardar aplicativos e redes de maneira eficaz tornará os processos empresariais mais eficientes e limitará a exposição. A VeriSign pode ajudar empresas preocupadas com segurança a atingir o equilíbrio correto entre abordagens proativas, reativas e de detecção na segurança das informações. O VeriSign® Managed Vulnerability Protection Service (MVPS - Serviço de proteção a vulnerabilidades gerenciado) complementa e maximiza os investimentos em tecnologia existentes, como firewalls e IDSs (Intrusion Detection Systems – Sistema de detecção de intrusões), com testes contínuos de vulnerabilidade de redes e aplicativos, além do envio de alertas proativos de vulnerabilidade. Com o MVPS, as vulnerabilidades são claramente identificadas e as organizações, mais bem preparadas para combater futuras explorações.



Resposta imediata garantida

A VeriSign inicia um procedimento de dimensionamento específico para o cliente quando o problema é detectado e então age rapidamente para identificar a origem. A resposta rápida da VeriSign a incidentes de segurança garante que seus clientes sejam totalmente informados e estejam preparados para qualquer ameaça iminente.

Canal de gerenciamento/ comunicação confiável

O VeriSign® SDA patentado é um canal de gerenciamento e comunicação tolerante a falhas e seguro. O SDA, executado por trás dos dispositivos de segurança do cliente, oferece recursos seguros de armazenamento e encaminhamento de eventos por meio de uma conexão criptografada com o centro de operações de segurança (SOC). Ele aumenta a eficiência da implementação de segurança, garante mais proteção e confiabilidade e reduz custos operacionais e de capital, já que a VeriSign assume todas as despesas de gerenciamento e hardware do SDA. A implantação do SDA não é obrigatória, mas extremamente recomendada.

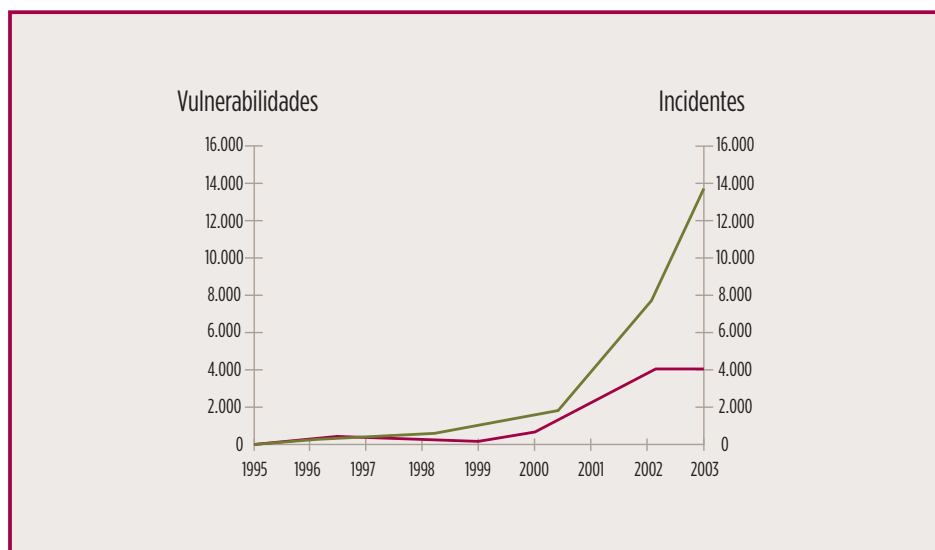
Testes com boa relação custo-benefício

A taxa de inscrição mensal do MVPS oferece à organização a combinação exata de testes manuais e automatizados, análises e relatórios. Os testes abrangentes da VeriSign são realizados com um custo geral mais baixo do que o custo de um teste único, que perde valor a cada vulnerabilidade detectada.

Baseado no risco comercial

O programa de segurança mais eficiente é aquele que atinge o maior equilíbrio entre custo e risco comercial. A VeriSign também desenvolve um programa personalizado para garantir que os sistemas estejam permanentemente protegidos contra hackers e códigos maliciosos, dentro e fora do perímetro de rede do cliente.

Vulnerabilidades x incidentes de segurança



+ Descrição

O MVPS fornece uma solução abrangente para organizações que estejam buscando uma proteção personalizada, contínua e com boa relação custo-benefício contra as vulnerabilidades exploráveis. Sua estrutura inclui verificações de vulnerabilidade remotas, testes de vulnerabilidade e de penetração, assim como alerta de vulnerabilidades em tempo real. Essas funções são aplicadas a diversos recursos da empresa, incluindo:

- Redes internas ou de zona desmilitarizada (DMZ)
- Redes externas voltadas para a Internet
- Aplicativos de comércio eletrônico para Web
- LANs sem fio
- Sistemas de acesso remoto e modems

É de total responsabilidade da VeriSign programar e realizar os testes, além de fornecer relatórios detalhados. A VeriSign notifica seus clientes sobre as vulnerabilidades graves e recomenda soluções. Além disso, os centros de operações de segurança (SOCs) da VeriSign garantem aos clientes acesso 24 horas aos analistas e engenheiros da empresa.

+ Recursos do serviço

- **Otimização de frequência e profundidade** – com o MVPS, os clientes podem personalizar o tipo e a frequência das avaliações de vulnerabilidade. A VeriSign trabalha junto com seus clientes para criar um serviço que atenda suas necessidades e políticas exclusivas. Por exemplo, a VeriSign pode realizar testes de penetração detalhados nos sistemas de Internet do cliente semestralmente e realizar verificações automatizadas mais baratas trimestrais, mensais ou semanais. Enquanto as verificações garantem uma excelente avaliação ampla, os serviços de testes da VeriSign® maximizam os testes manuais para uma avaliação profunda e personalizada. Conseqüentemente, os clientes da VeriSign são informados sobre as últimas vulnerabilidades com a frequência e a profundidade necessárias por um programa com bom custo-benefício, que atende as necessidades de segurança específicas da organização.

Testes distribuídos

O VeriSign SDA permite a execução de testes remotos nas redes DMZ ou internas de seus clientes.

Diferentemente dos outros provedores de serviços, a VeriSign pode detectar e classificar vulnerabilidades "ocultas" para ter uma visão geral de toda a rede, dentro e fora dos firewalls.

Instalações de teste seguras

A VeriSign conduz todos os testes baseados na Internet em seu Centro de avaliação de vulnerabilidades, que reside nos SOCs de host disponíveis 24 horas por dia, 7 dias por semana. Os dados importantes do cliente são coletados, analisados e mantidos em um ambiente seguro e controlado.

Especialização em configuração de testes e verificações

Os clientes beneficiam-se da profunda experiência demonstrada pelos engenheiros de MVPS da VeriSign. Com um grande conhecimento sobre adequação e otimização de testes e verificações, esses engenheiros asseguram os melhores resultados para os ambientes do cliente.

Suporte para avaliação de resultados

Os analistas de segurança experientes da VeriSign fornecem aos clientes de avaliação de vulnerabilidade o suporte para compreensão e priorização das vulnerabilidades descobertas em suas redes e sistemas, além de planejar atividades de reparo. Os analistas de segurança permanecem disponíveis durante o serviço para tirar dúvidas e oferecer orientações sobre a segurança das redes dos clientes.

- **Distribuição de relatórios para analistas especializados** – por meio de uma transmissão digital segura, a VeriSign emite relatórios de avaliação que especificam as vulnerabilidades identificadas. Esses relatórios são enviados aos contatos designados pela organização e fornecem descrições detalhadas sobre as vulnerabilidades juntamente com as recomendações de reparo específicas à empresa. São incluídas informações sobre os bens afetados, o impacto, o nível de esforço para reparo e links para sites de fornecedores e segurança.
- **Suporte de segurança contínuo** – em todas as avaliações de segurança, a VeriSign atribui um analista de segurança profissional para trabalhar com o cliente e analisar os resultados de seus relatórios e as ações recomendadas. Isso faz com que o cliente entenda melhor as possíveis vulnerabilidades e auxilia na realização de ações preventivas.
- **Emissão de relatórios inteligentes** – os dados de vulnerabilidade de toda a empresa são canalizados para um portal central pela arquitetura de verificação distribuída da VeriSign®. Com as opções de relatório flexíveis, os clientes podem visualizar os resultados por host, gravidade e vulnerabilidade, além de realizar consultas ad hoc que filtram os dados por região, IP, porta e outros critérios. Para oferecer uma visão clara das tendências gerais de vulnerabilidade, o quadro do portal exibe um panorama das vulnerabilidades mais frequentes detectadas nas verificações de todos os clientes da VeriSign. A capacidade de determinar tendências de vulnerabilidades e outras estatísticas que considerem os dados no decorrer do tempo oferece aos clientes um método de demonstrar uma postura de segurança aprimorada e retorno do investimento para a gerência executiva.
- **Alertas de vulnerabilidades correlacionadas** – o VeriSign® Managed Vulnerability Alerting correlaciona com precisão as ameaças que surgem e os bens de uma organização. Usando o TeraGuard™, a arquitetura de correlação avançada da VeriSign, os dados de host do cliente são coletados e comparados com os bens afetados pelas vulnerabilidades recém-descobertas. A partir dessa correlação, a VeriSign limita notificações de falsos positivos e somente alerta os clientes sobre os hosts específicos que podem ser afetados, fornecendo informações detalhadas sobre a vulnerabilidade, além de instruções de reparo.

+ Centros de operações de segurança

Os SOCs da VeriSign são ambientes seguros e altamente disponíveis que fornecem monitoramento e gerenciamento 24 horas de infra-estruturas de segurança para grandes empresas. Construção em estilo bunker, acesso biométrico em camadas a áreas sensíveis e vigilância por vídeo são recursos especiais do controle de segurança física, enquanto um gerador reserva, uma fonte de alimentação condicionada (UPS) e sistemas de ponta para controle de incêndios garantem disponibilidade 24 horas por dia, 7 dias por semana. Todos os sistemas cruciais são totalmente redundantes, da eletricidade aos links de telecomunicações e processamento de dados, eliminando, dessa forma, qualquer ponto único de falha.

+ TeraGuard™

A arquitetura de gerenciamento de informações da VeriSign, o TeraGuard™, coleta uma grande variedade de dados de fontes diferentes por meio do SDA. O SDA fica localizado nas instalações do cliente e converte os dados dos dispositivos de rede e segurança em um único fluxo normalizado de eventos relacionados à segurança. O TeraGuard então analisa e prioriza esses eventos usando um processo de correlação em camadas, permitindo que a VeriSign rapidamente rejeite falsos positivos, identifique ameaças reais e tome as medidas apropriadas. A análise desse enorme volume de dados de ameaça de todos os clientes fornece aos analistas de segurança treinados da VeriSign uma ampla inteligência de segurança de Internet em tempo real que seria praticamente impossível uma organização reproduzir internamente.

Portal permanente de recursos do cliente

O Portal de recursos do cliente oferece uma visão detalhada dos dispositivos de segurança que são gerenciados pela VeriSign. Isso inclui vários relatórios por tipo de dispositivo e acesso a um mecanismo de consulta ad hoc para análises sofisticadas de eventos de segurança em diversos locais e plataformas. O acesso ao sistema é protegido por autenticação com token e criptografia SSL. O Portal de recursos do cliente funciona como um ponto de contato primário para atendimento ao cliente e registro de problemas, concedendo aos clientes da VeriSign acesso em tempo real a relatórios de eventos, inteligência em tempo hábil e uma plataforma personalizada de gerenciamento de vulnerabilidades.

Gerenciamento, monitoramento e suporte 24 horas

A equipe especializada de analistas de segurança da VeriSign fica disponível 24 horas por dia, 7 dias por semana, para fornecer gerenciamento, monitoramento e suporte, liberando, assim, as empresas da responsabilidade permanente e penosa de salvaguardar as informações corporativas mais relevantes.

Custo total de propriedade mais baixo

O MVPS economiza tempo e dinheiro das empresas ao reduzir ou eliminar gastos com equipes, treinamento, manutenção e investimento inicial.



Selo VeriSign Secured Seal™

Lembre-se de inserir o selo VeriSign Secured Seal™ em sua página inicial ou em outras páginas nas quais haja troca de informações confidenciais. O selo VeriSign Secured Seal informa aos visitantes de seu site que você escolheu a VeriSign como uma parte importante de sua solução de segurança total da Web.

+ O diferencial da VeriSign®

Escala global e Intelligence and Control™ – a VeriSign oferece a seus clientes a vantagem de um sistema de aviso antecipado que maximiza uma base abrangente de dados sobre ameaças disponíveis somente para a VeriSign e seus clientes com os serviços Intelligence and Control™. Com uma base de clientes mundial e mais de 2.600 dispositivos de segurança de rede sob seu gerenciamento, a VeriSign possui uma visão mais ampla e profunda sobre as atividades na Internet e, por isso, pode identificar e alertar proativamente seus clientes sobre novas tendências de ataque e ameaças cibernéticas.

Compromisso com a excelência – a VeriSign dedica-se ao crescimento e ao aprimoramento constantes dos MSS (Managed Security Services) e investe continuamente nos centros de operações de segurança e em infra-estruturas de suporte. Os serviços da empresa são altamente redundantes para assegurar que os clientes tenham suporte e disponibilidade permanentes, 24 horas.

O melhor suporte do mercado para dispositivos de terceiros – a VeriSign não recomenda um fornecedor especificamente e garante compatibilidade com uma grande variedade dos melhores produtos de segurança do mercado. A empresa desenvolve e implementa soluções de segurança baseadas nas necessidades e nos requisitos específicos de seus clientes e regularmente avalia e aprimora os produtos oferecidos para garantir compatibilidade com produtos de segurança de outras empresas. Os clientes têm a garantia de que suas infra-estruturas cruciais serão totalmente protegidas pela combinação certa de uma equipe de segurança treinada disponível 24 horas gerenciando e monitorando as principais tecnologias do setor.

Parceiro de confiança – a VeriSign tem uma sólida tradição no gerenciamento de serviços de segurança confiáveis e milhares de organizações beneficiam-se dessa tradição todos os dias. Juntamente com autenticação forte, segurança de aplicativo e de comércio eletrônico, os serviços VeriSign® MSS representam um compromisso incomparável com o fornecimento de serviços que permitem às empresas dedicarem-se a comércio eletrônico, comunicações e computação colaborativa de maneira confiável.

+ Comece hoje

Para obter mais informações sobre os serviços de consultoria e MSS da VeriSign, ligue para (0) XX 11 5853-2900 ou envie um e-mail para faleconosco@verisign.com.

Visite www.verisign.com.br para obter mais informações.

Nota: Em fevereiro de 2004, a VeriSign adquiriu a Guardent, a líder reconhecida em MSS (Managed Security Services). Os serviços gerenciados e a consultoria de segurança da Guardent foram integrados ao portfólio de soluções da VeriSign.

© 2006 VeriSign Brasil. Todos os direitos reservados. VeriSign, o logotipo VeriSign, TeraGuard, Intelligence and Control, VeriSign Secured, o VeriSign Secured Seal, "Where it all comes together" e outras marcas comerciais, marcas de serviço e designs são marcas registradas ou não-registradas da VeriSign e de suas subsidiárias nos Estados Unidos e em outros países.