O cubo da segurança cibernética Part. 2 Segunda dimensão : Estados dos dados

Data do Post	@August 16, 2021 9:00 AM (GMT)
Status	Done
Palavras-chave	Cubo da Segurança Cibernética
Fonte	
Pronto	Preparado
IG post	☑
Publicado	☑

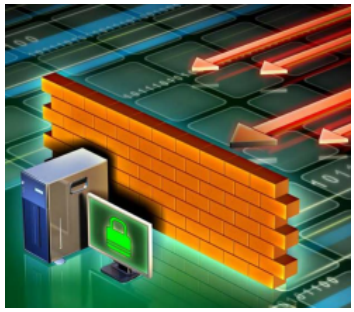
Contramedidas de proteção consiste em uma serie de medidas de proteção para salvaguardar os dados. Nesse decurso, existem quatro formas de proteção :

- baseada em software;
- baseada em hardware;
- baseada em rede;
- baseada em nuvem.

Nesse artigo vamos debruçar-nos sobre isso.

Proteção de tecnologia baseada em software

As proteções de tecnologia incluem programas e serviços que protegem sistemas operacionais, bancos de dados e outros serviços sendo executados em estações de trabalho, dispositivos portáteis e servidores. Os administradores instalam contramedidas ou proteções baseadas em software em hosts ou servidores individuais. Existem várias tecnologias baseadas em software usadas para proteger os ativos de uma empresa:



- Os firewalls de software controlam o acesso remoto a um software. Os sistemas operacionais normalmente incluem um firewall ou um usuário pode comprar ou fazer download de software de terceiros.
- Scanners de rede e de porta detectam e monitoram portas abertas em um host ou servidor.
- Analisadores de protocolo, ou analisadores de assinatura, são dispositivos que coletam e examinam o tráfego de rede. Eles identificam problemas de desempenho, detectam problemas de configuração, identificam aplicativos com comportamento inadequado, estabelecem o parâmetro e os padrões de tráfego normal e depuram problemas de comunicação.
- Scanners de vulnerabilidades são programas de computador projetados para avaliar os pontos fracos em computadores ou redes.
- Sistemas de detecção de invasão baseados em host (IDS) examinam as atividades apenas em sistemas de host. Um IDS gera arquivos de log e mensagens de alarme quando detecta atividade incomum. Um sistema que armazena dados confidenciais ou que presta serviços essenciais é um candidato para IDS baseado em host.

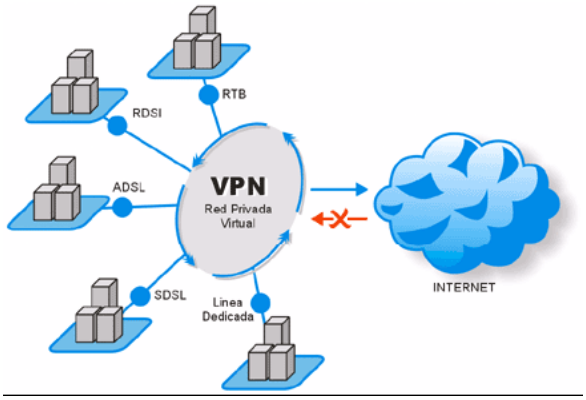
Proteção de tecnologia baseada em hardware

Existem várias tecnologias baseadas em hardware usadas para proteger os ativos de uma empresa:

- Dispositivos de firewall bloqueiam o tráfego indesejado. Os firewalls contêm regras que definem o tráfego permitido dentro e fora de uma rede.
- Sistemas de detecção de invasão (IDS) detectam sinais de ataques ou tráfego incomum em uma rede e enviam um alerta.
- Sistemas de prevenção de intrusões (IPS) detectam sinais de ataques ou tráfego incomum em uma rede, geram um alerta e tomam medidas corretivas.
- Os serviços de filtros de conteúdo controlam o acesso e a transmissão de conteúdo ofensivo ou censurável.

Proteção de tecnologia baseada em rede

Existem várias tecnologias baseadas em rede usadas para proteger os ativos da empresa:



- **Rede privada virtual (VPN)** é uma rede virtual segura que usa a rede pública (ou seja, a Internet). A segurança de uma VPN está na criptografia do conteúdo do pacote entre os endpoints que definem a VPN.
- **Network Access Control (NAC)** requer um conjunto de verificações antes de permitir que um dispositivo se conecte a uma rede. Algumas verificações comuns incluem software antivírus atualizados ou atualizações do sistema operacional instaladas.
- **Segurança de access point sem fio** inclui a implementação de autenticação e criptografia.

Proteção de tecnologia baseada em nuvem

As tecnologias baseadas na nuvem mudam o componente de tecnologia da organização para o provedor de nuvem. Os três principais serviços de computação em nuvem são:

- **Software as a Service (SaaS)** permite aos usuários ter acesso a bancos de dados e software de aplicativo. Os provedores de nuvem gerenciam a infraestrutura. Os usuários armazenam dados nos servidores do provedor de nuvem.
- **Infrastructure as a Service (IaaS)** fornece recursos de computação virtualizados pela Internet. O provedor hospeda o hardware, o software, os servidores e os componentes de armazenamento.
- **Platform as a Service (PaaS)** proporciona acesso a ferramentas e serviços de desenvolvimento usados para entregar os aplicativos.

Os provedores de serviços de nuvem ampliaram essas opções para incluir IT as a Service (ITaaS), que proporciona suporte para os modelos de serviço IaaS, PaaS e SaaS. No modelo ITaaS, a empresa contrata serviços individuais ou em pacote com o provedor de serviços em nuvem.

Provedores de serviços de nuvem usam dispositivos de segurança virtual que são executados dentro de um ambiente virtual com um sistema operacional pré-preparado em pacotes, codificado, sendo executado em hardware virtualizado.

Implementação da educação em segurança cibernética e Treinamento

Um programa de conscientização sobre segurança é extremamente importante para uma organização. Um funcionário pode não ser intencionalmente malicioso, mas pode simplesmente não conhecer os procedimentos adequados.

Há várias formas de implementar um programa de treinamento formal:

- Torne o treinamento de conscientização de segurança uma parte do processo de integração do funcionário

- Vincule a conscientização de segurança aos requisitos do trabalho ou às avaliações de desempenho
- Realize sessões de treinamento presenciais

A conscientização de segurança deve ser um processo contínuo, já que novas ameaças e técnicas estão sempre surgindo.

Procedimentos e Políticas da segurança cibernética

Uma política de segurança é um conjunto de objetivos de segurança de uma empresa que inclui regras de comportamento para os usuários e administradores e especifica os requisitos de sistema. Esses objetivos, regras e requisitos garantem, juntos, a segurança da rede, dos dados e dos sistemas computacionais de uma organização. Os padrões ajudam uma equipe de TI a manter a consistência na operação da rede. Os padrões fornecem as tecnologias que programas ou usuários específicos precisam, além de qualquer requisito de programa ou critérios que uma empresa deva seguir.

As diretrizes são uma lista de sugestões sobre como fazer as coisas de forma mais eficiente e com segurança. Eles são semelhantes aos padrões, mas mais flexíveis e, geralmente, não são obrigatórios. As diretrizes definem como os padrões são desenvolvidos e garantem adesão às políticas de segurança gerais.

Documentos de procedimento são mais longos e mais detalhados do que os padrões e as diretrizes. Documentos de procedimentos incluem detalhes de implementação que normalmente contêm instruções e gráficos passo a passo.

Conclusões

Esse artigo é o último de uma serie de três artigos que, essencialmente, falou sobre o cubo da segurança cibernética. Aqui vimos algumas formas que os administradores podem proteger as redes empresarias de ataques, dos quais vimos proteção baseada em nuvem, em rede, em softwares e hardware. E não menos importante, vimos que é da responsabilidade das empresas criarem estratégias para conscientizarem os seus funcionários sobre a adoção a boas práticas de proteção.

Além disso, vimos a importância da implementação da educação em segurança cibernética. Pois um programa de conscientização sobre segurança é extremamente importante para uma organização. Um funcionário pode não ser intencionalmente malicioso, mas pode simplesmente não conhecer os procedimentos adequados.