SEGURANÇA CIBERNÉTICA

PROF. ENG. DANIEL JOSÉ PIMENTA

PLANO DE CIBERSEGURANÇA

SEG. DA INFORMAÇÃO X SEG. CIBERNÉTICA

A segurança da informação tem um conotação mais ampla, ela envolve a proteção de dados e informações em todos as sua formações possíveis, que podem estar contidas em meios eletrônicos, em papéis, em áreas e layouts, em produtos, equipamentos ou processos empresariais.

A segurança da informação tem como propósito proteger as informações, sem importar se onde estejam situadas: impressas em papel, armazenadas em computadores/servidores ou até mesmo na memória das pessoas que as conhecem.

PLANO DE CIBERSEGURANÇA

SEG. DA INFORMAÇÃO X SEG. CIBERNÉTICA

A norma ISO/IEC 27032- Guidelines for cybersecurity, define segurança cibernética como preservação da confidencialidade, da integridade e da disponibilidade da informação no espaço cibernético.

A diferença entre segurança da informação e segurança cibernética pode ser identificada através do objetivo e espaço de atuação de cada uma delas.

Enquanto que a segurança da informação tem o objetivo de preservar a informação em todas as sua formas e localizações, a segurança cibernética tem o objetivo de preservar os dados no formato digital e no espaço cibernético.

Podemos dizer que a segurança cibernética está incutida dentro da segurança da informação.

A Figura abaixo, extraída da norma ISO/IEC 27032, exemplifica uma forma de inserção da segurança cibernética no campo da segurança da informação.

Fonte: adaptado de ISO/IEC 27032 (2012)

Percebe-se que a segurança cibernética, além de achar-se inserida no escopo da segurança da informação e da proteção das infraestruturas críticas de informação, permeia a segurança das redes, da Internet e das aplicações (sistemas).

PLANO DE CIBERSEGURANÇA

SEG. DA INFORMAÇÃO X SEG. CIBERNÉTICA

Segurança cibernética envolve um conjunto de ações para proteção de pessoas, sistemas e dispositivos contra ataques maliciosos no espaço cibernético. É uma ramificação da segurança da informação.

Segurança da informação: envolve a prevenção e proteção contra todo tipo de risco, seja físico ou digital, controlando acessos de pessoas a locais, permissões para acessos de arquivos, entre outros.

INVESTIMENTO NECESSÁRIO PARA GARANTIR A PROTEÇÃO DOS DADOS

- Desenvolvimento e implementação de uma Politica de Segurança da Informação adequada as necessidades da organização;
- Investimento em pessoal especializado e recursos relacionados a segurança cibernética;
- Elaboração de um Plane de Gestão da Segurança Cibernética adequado as necessidades da empresa;
- Investimento em um programa de educação e conscientização dos colaboradores sobre boas práticas de segurança cibernética;
- Estabelecimento de boas práticas na gestão dos ativos de informações da empresa.
- Previsão orçamentária adequada as necessidades de segurança da organização, que deve ser dimensionadas mediantes análise de risos adequadas.

FIREWALL

Um firewall é um sistema ou grupo de sistemas que aplica uma política de controle de acesso entre redes

Os firewalls são resistentes a ataques de rede.

Firewalls são o único ponto de trânsito entre redes corporativas internas e redes externas porque todo o tráfego flui através do firewall. Os firewalls aplicam a política de controle de acesso.

FIREWALL

Tipos:

1) Firewall de filtragem de pacotes (sem estado).

Firewalls de informações de filtragem de pacotes geralmente fazem parte de um tráfego de roteadores, que **permitem** ou **negam** a pesquisa com o estado da Camada 4 com base em definição.

Por exemplo, os servidores SMTP atendem a uma porta 25 por padrão. Uma pessoa pode configurar o firewall de filtros de pacotes para bloquear a porta 25 de uma estação de trabalho específica para impedir que ele transmita um vírus de e-mail.

FIREWALL

Tipos:

2) Firewall de monitoramento de estado.

Realiza uma espécie de comparação entre o que se espera que ocorra num tráfego de informações e o que realmente está ocorrendo. Ele avalia todo o tráfego de dados procurando por padrões permitidos ou aceitáveis com base em suas regras.

Somente os pacotes que combinam a conexão ativa conhecida podem passar pelo firewall. A inspeção dos estados dos pacotes (SPI), também referida como filtragem de pacotes dinâmicos.

https://minutodaseguranca.blog.br

FIREWALL

Tipos:

3) Firewall de Gateway de Aplicativo

Esse tipo de dispositivo – tecnicamente um proxy e às vezes chamado de firewall proxy – funciona como o único ponto de entrada e saída da rede. Os gateways no nível do aplicativo filtram os pacotes não apenas de acordo com o serviço ao qual se destinam – conforme especificado pela porta de destino – mas também por outras características, como a string de solicitação HTTP.

Embora os gateways que filtram na camada do aplicativo forneçam segurança de dados considerável, eles podem afetar drasticamente o desempenho da rede e podem ser difíceis de gerenciar.