SEGURANÇA

SOBRE SEGURANÇA

A Segurança da Informação é uma questão de alta relevância para a interconectividade de redes.

Desta forma, além das diretrizes, recomendações e sugestões elencadas nos demais itens desta Orientação Técnica, requisitos adicionais de Segurança da Informação para a interconectividade, incluindo blacklists e whitelists de portas, protocolos, serviços e aplicações podem ser definidos:

- Pelos Órgãos do SMTIC para os seus respectivos sites internos.
- Pelo Integrador Estratégico, para interconectividade com a RPCD.

Além disso, esta OT traz as recomendações e sugestões abaixo, específicas sobre segurança, desde que haja mão de obra capacitada, disponibilidade orçamentária e disponibilidade da funcionalidade nos ativos pertinentes.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Controle de acesso físico aos equipamentos de rede e servidores.
- Todos os dispositivos críticos devem possuir backup da configuração (atualizado) apartado do equipamento de origem.
- Substituição das senhas padrão por senhas adequadamente fortes.
- Implementar, sempre que possível, a utilização do procotolo 802.1X para acesso aos sites internos e à RPCD.
- Usar soluções de firewall para criar perímetros que possibilitem melhor controle de acesso.
- Usar solução de antivírus em todas as estações e servidores windows conectados na rede, com atualização automática e periódica.
- Implementar processo periódico de instalação de patches de segurança de firmwares de dispositivos e equipamentos, bem como de softwares básicos, sistemas operacionais e aplicativos conectados na rede.
- Tomar como base a norma de segurança da informação em normas ISO 27099:2022 / ISO-IEC-27001-2013 /ISO/IEC 27010:2015.
- Atualizar periodicamente os firmware para mitigar vulnerabilidades de segurança.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Efetuar o controle do endereço físico do dispositivo (MAC address) vinculado à porta de acesso.
- Manter as portas sem uso nos equipamentos de rede em estado bloqueado.
- Implementar mecanismo de gestão centralizado das estações de trabalho, tais como policies do Active Directory ou similares. Este artifício tem como objetivo possibilitar gestão do ambiente computacional.
- Padronizar nomenclatura das estações de trabalho para as unidades.
- Usar sistema de prevenção de intrusão (IPS - Intrusion prevention system) para monitoração e bloqueio de tráfego suspeito (interconectividade externo-interno).
- Usar solução de firewall na camada de aplicações (WAF – web application firewall) para mitigar as vulnerabilidades de aplicações WEB publicadas na Internet.
- Usar solução contra ataques avançados baseados em comportamento.
- Usar solução de prevenção contra perda de dados.
- Bloquear todas as portas de sistema (0 a 1023) e as portas registradas (1024 a 49151), com exceção das portas necessárias para o provimento dos serviços utilizados por meio da interconectividade, bem como para a manutenção da própria interconectividade.
- Utilizar da Política Nacional de Segurança da Informação - PNSI para descritivo de um plano ou sugestão de segurança da informação, em atendimento ao Decreto Nº 9.637, de 26 de Dezembro de 2018.