REDES WI-FI E IoT

SOBRE REDES WI-FI E IoT

As redes Wi-Fi e IoT devem utilizar sistemas de tunelamento para que haja autenticação do usuário, antes da liberação da conexão, acesso e enlace. Havendo acesso à internet, o mesmo será monitorado e com controle de filtro de conteúdo, nos termos da Lei 14.098/2005.

> Art. 1º. As escolas públicas, os Centros Educacionais Unificados (CEUs), bibliotecas, postos de atendimento - Telecentro e quaisquer outros locais onde funcionem computadores da Prefeitura ligados à Internet, todos da rede pública municipal, ficam obrigados a instalar a tecnologia de filtragem de conteúdo.
>
> Parágrafo único. Sites que tenham conteúdos de sexo, drogas, pornografia, pedofilia, violência e armamento, dentre outros, a critério do Executivo, devem ser proibidos.

A rede Wi-Fi corporativa interna deverá ser segregada, física ou logicamente, da rede Wi-Fi disponibilizada ao cidadão comum (conhecida como rede guest), visando reduzir o risco de acesso indevido ao ambiente corporativo. Sugere-se estudar a viabilidade de isolamento físico e lógico da rede guest para fins de segurança da informação, através da adoção de VLANs (Rede local virtual) distintas.

A rede Wi-Fi guest poderá exigir cadastro prévio de usuário para o seu usufruto, a critério do Órgão administrador. A rede Wi-Fi corporativa interna deverá exigir autenticação do usuário, conforme acima, utilizando-se no mínimo o algoritmo WPA2.

Interconexões que contemplem serviços de IoT devem estar segregados, física e/ou logicamente, com a implementa-ção de regras que permitam apenas os serviços e usuá-rios atinentes à consecução do negócio.Os dispositivos ou sensores IoT são utilizados para detectar características do ambiente, gerando sinais de controle para atuadores e eventualmente podem trazer redução de custos, porém a utilização destes dependem de avaliação para atender necessidades específicas.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Substituir todas as senhas padrão de fábrica dos dispositivos geridos pelo Órgão do SMTIC por senhas adequadamente fortes, seguindo, sempre que aplicável, a política de senhas do Órgão.
- Desabilitar o recurso de WPS (Wi-Fi Protected Setup), para mitigar o risco de quebra das chaves de criptografia do WPA2.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Implementar processos de atualização periódica de firmware e de software para mitigar possíveis vulnerabilidades de segurança.
- Introduzir cadastro prévio de usuário para que este possa usufruir da rede Wi-Fi guest, para evitar que terceiros passem a utilizar a rede de forma corriqueira como se fosse a sua própria rede, exceto para os pontos de Wi-Fi livre.
- Estudar a conveniência de ter o mesmo usuário para autenticação, independentemente de ser rede Wi-Fi ou cabeada.
- Avaliar a precisão, custo, segurança, longevidade e conectividade no caso de implantação de uma solução envolva dispositivos ou sensores IoT.