Problemas de segurança

IoTSafety

Com o aumento considerável da utilização da tecnologia e das redes, os serviços e requisições provindos da WEB aumentam proporcionalmente, o que faz com que o aumento de vulnerabilidades e ataques aconteçam em grande escala. Assim como nas demais tecnologias, a Internet das coisas se preocupa seriamente com o fator de segurança. Alguns desses problemas de segurança são oriundos de outras tecnologias, mas outros são problemas decorrentes da própria IoT.

A segurança da informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que sua missão seja alcançada (FONTES 2010). A importância de seguir políticas de segurança, junto com os critérios de confidencialidade, integridade, disponibilidade e autenticidade são fundamentais para garantir a preservação de dados e informações de uma empresa. Essas políticas de segurança que definem qual a posição da empresa, mediante um eventual problema, onde seu objetivo é definir como as informações retratadas devem ser manejadas corretamente.

De acordo com uma pesquisa feita pela Irdeto Global Connected Industries feita com 700 empresas de diferentes países, oito em dez empresas já vivenciaram ataques cibernéticos em seus dispositivos de IoT, e apenas 7% afirmaram que suas respectivas empresas possuem os meios necessários para combater os ataques. A pesquisa constatou que mais de 26% das empresas não possuem tecnologia alguma para combater os ataques, tanto em aplicações móveis quanto sistemas mais complexos.

Um dos grandes problemas que afetam a segurança da IoT está relacionado com a conectividade de redes de sensores, redes sem fio e frequências de rádio. Alguns exemplos destes problemas são ataques de autenticação e/ou integridade em redes sem fio, ataques de negação de serviços (DoS) e DDoS, programas maliciosos que quebram criptografias, programas que infectam a máquina do usuário, ou em disponibilidades de frequências de rádio. A resolução deste problema é uma ideal implementação de criptografias para a proteção destes sensores bem como para se proteger de ataques maliciosos. Cabe a quem desenvolve os sensores ou os dispositivos que estão utilizando esses sensores e sistemas a preocupação com a segurança quanto a invasões.

O usuário também é um fator de grande perigo para os sistemas, sua inexperiência no assunto faz com que sejam mais facilmente afetados a ataques e por não terem consciência da ameaça ou capacidade de identificar os malwares, não impedem que estes malwares sejam espalhados e acabam proliferando cada vez mais uma vez que se conectam a outras redes e aparelhos. O usuário deve estar sempre atento sobre como interage com determinados equipamentos, sempre verificando a confiabilidade dos equipamentos e das empresas em que estão colocando suas informações.