PHISHX

Como utilizar de forma segura Internet das Coisas (IoT)

O que é Internet das Coisas

.A IoT (Internet das Coisas) é uma rede de dispositivos conectados à internet, como eletrodomésticos, veículos, dispositivos médicos, sensores e outros objetos que possuem a capacidade de coletar e transmitir dados online.

Esses dispositivos são capazes de se comunicar uns com os outros e, também, com outras redes, incluindo a nuvem. Eles podem coletar, armazenar e analisar dados, permitindo que as organizações e pessoas tomem decisões informadas.

Como a Internet das Coisas está presente no nosso cotidiano

Com o aumento da conectividade e o desenvolvimento de tecnologias de rede e computação em nuvem, a IoT está se tornando cada vez mais comum em nossas vidas e nos negócios. A popularização desses dispositivos também permitiu que a IoT seja usada em uma grande variedade de setores e aplicações.

Dentro da área da saúde, existem dispositivos médicos, como medidores de glicose e pressão arterial, que permitem que pacientes e profissionais de saúde monitorem e gerenciem condições de saúde em tempo real.

Quando falamos do setor industrial, sensores em máquinas e equipamentos podem coletar dados em tempo real, permitindo que problemas possam ser identificados e resolvidos mais rapidamente.

Quais são os riscos dessa tecnologia

Apesar de possibilitar uma conectividade maior, essa tecnologia também trouxe riscos de segurança associados aos dispositivos. Dessa forma, senhas fracas, ataques cibernéticos e vulnerabilidades de softwares podem permitir a invasão desses dispositivos, comprometendo dados e informações importantes.

Muitos dispositivos IoT têm configurações padrão que não são alteradas pelos usuários após a configuração inicial, o que os torna vulneráveis a ataques cibernéticos. Além disso, esses dispositivos podem ficar muito tempo sem que sejam atualizados, permitindo que invasores explorem vulnerabilidades para acessar redes, dispositivos e informações confidenciais.

Como proteger suas informações e dispositivos

Para mitigar esses riscos, é importante adotar medidas de segurança, como manter os dispositivos sempre atualizados e adotar a autenticação em dois fatores sempre que possível.

Além disso, lembre-se de desabilitar funções desnecessárias do dispositivo, como a capacidade de fazer login remotamente ou aceitar atualizações não solicitadas. Você também pode limitar o compartilhamento de informações, para que apenas informações necessárias sejam compartilhadas com as partes confiáveis.

Outro ponto importante é desativar dispositivos IoT quando eles não estiverem em uso e monitorar regularmente o tráfego de rede para detectar atividades suspeitas. Por último, utilizar uma solução que permite limitar o tráfego de entrega e saída de dados desses dispositivos pode evitar que esses dispositivos sejam atacados.

O que fazer em caso de violações de segurança

A resposta para uma violação de segurança de dispositivos IoT depende da natureza do incidente, mas aqui existem algumas etapas gerais que podem ajudar a lidar com a situação.

O primeiro passo é desconectar o dispositivo comprometido, para evitar que a violação se espalhe para outros dispositivos. Em seguida, altere as senhas e reforce as configurações de segurança do dispositivo comprometido e de qualquer outra conta, rede ou sistema que também pode ter sido atacado. Para isso, não se esqueça de utilizar diferentes formas de autenticação.

Nesse tipo de caso, é importante agir rapidamente para limitar o dano e prevenir futuras violações. Isso pode incluir notificar a equipe de segurança de TI, monitorar contas e dispositivos afetados, reportar a violação às autoridades relevantes e aprender com o incidente para melhorar a segurança futura.