PHISHX

Como o ransomware pode prejudicar sua empresa?

O que é Ransomware?

Ransomware é uma forma de software malicioso projetado para criptografar arquivos em um dispositivo, tornando inutilizáveis quaisquer dados ou sistemas que dependem deles. Os criminosos passam a exigir pagamentos para restaurar o acesso.

Em alguns casos, os atacantes também podem roubar esses dados, pedindo um pagamento adicional para que essas informações não sejam divulgadas para autoridades, concorrentes, ou até mesmo sejam disponibilizadas publicamente.

Esses ataques têm paralisado organizações no mundo todo, arrecadando quantias consideráveis de dinheiro com resgates. Por isso, é preciso estar ciente das possíveis consequências.

Porta de entrada

Os criminosos utilizam formas já conhecidas de ataques, como phishing, para se infiltrar nos sistemas. O usuário pode ser enganado por um e-mail falso, um SMS malicioso ou até mesmo por meio de mensagens em aplicativos de comunicação, além de postagens nas redes sociais.

Também podem se infiltrar através de um link malicioso, ou explorando vulnerabilidades de um navegador ou software. Dessa forma, é importante estabelecer medidas de segurança e tratar sobre o tema da segurança digital com as pessoas.

O que acontece em um ataque?

Quando se infiltram nos sistemas das organizações, os atacantes preparam e coletam dados essenciais, pedindo resgates para reverter o estrago feito. Quanto mais tempo passa, maior são os números de dados e arquivos comprometidos. Por isso, é essencial uma resposta rápida.

Uma vez que ele se instala é difícil lidar com o problema, gerando grandes custos e interrupção do trabalho para que seja resolvido. Os operadores desses ataques passam a extorquir as vítimas, pedindo resgates para que não disponibilizem os dados roubados.

Tipos de extorsão

Existem diferentes tipos de ransomware, assim como diferentes formas de extorsão. Os criminosos podem exigir um resgate para devolver o acesso aos dados, mas também podem extrair as informações consideradas sensíveis e ameaçar publicá-las em sites dedicados a esses vazamentos.

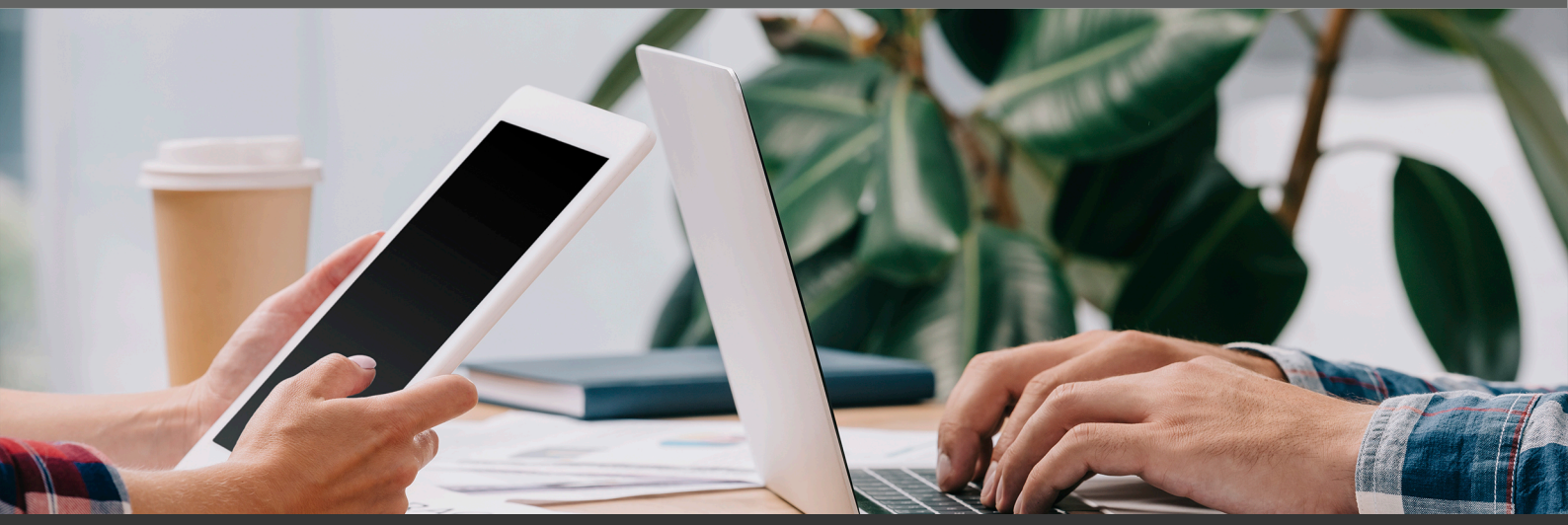
Além disso, podem utilizar ataques simultâneos para sobrecarregar os sistemas, comprometendo as operações. Para pressionar ainda mais as vítimas, os invasores também ameaçam informar clientes e investidores sobre o sequestro de dados. Essas extorsões causam ainda mais prejuízo.

O que fazer durante um ataque de Ransomware?

As organizações podem utilizar estruturas pré-definidas para lidar com esse tipo de ataque, reduzindo os níveis de risco. Ainda assim, é importante identificar qual é a ameaça, para saber quais medidas serão tomadas.

O pagamento do resgate não é necessariamente uma certeza de que o invasor devolverá os dados, ou deixará o seu sistema limpo. Por isso, é importante utilizar ferramentas de segurança para eliminar os arquivos maliciosos, reinstalar o sistema e tentar recuperar as informações.

Medidas de proteção

Existem algumas boas práticas para se prevenir desse tipo de ataque. É importante auditar o inventário de dispositivos, realizando atualizações constantes para mitigar vulnerabilidades. Também é preciso implementar medidas para garantir a segurança da infraestrutura, assim como utilizar ferramentas de segurança para se proteger das ameaças.

Mesmo criando normas para lidar e prevenir esse tipo de ataque, é essencial que todos os envolvidos com dados importantes sejam conscientizados. Tornar a segurança digital um tema constante nos treinamentos faz com que as pessoas saibam identificar possíveis ameaças.