Pílulas de LGPD

Você sabe o que é RANSOMWARE?

O Ransomware é um tipo de malware que sequestra o seu computador e criptografa os seus arquivos, só os liberando após o pagamento de um resgate para o criminoso.

Todos os dias, pesquisadores de segurança tem encontrado novas variantes de ransomwares, descobrindo diferentes formas e métodos usados pelos criminosos para roubar dinheiro diretamente de consumidores e negócios.

Basicamente, existem dois tipos de ransomware: os bloqueadores e os codificadores. Os codificadores são os trojans que criptografam qualquer tipo de arquivos que poderiam ser valiosos para os usuários. Isso pode incluir fotos pessoais, arquivos, documentos, bancos de dados, etc. Os bloqueadores também são trojans (alguns dos bloqueadores mais proeminentes estão baseados em outros trojans, como é o caso do Reveton, que está baseado no trojan bancário ZeuS). Este tipo de ransomware apenas bloqueia os sistemas infectados e exige o pagamento.

Como acontece?

Na maioria das vezes a invasão ocorre no período da noite ou madrugada, momento em que um criminoso virtual invade o dispositivo da vítima e instala um software capaz de criptografar (codificar) as informações de seu computador. Ao acessar o computador após tal procedimento, a vítima receberá uma mensagem de que seus dados foram criptografados e se ela não realizar um pagamento exigido pelo criminoso, normalmente em bitcoins, perderá todos os dados do computador invadido.

Como isso afeta o negócio?

De acordo com o FBI, o Ransomware já movimentou mais de US$ 70 milhões no mundo todo, e são realizados, em média, 300 ataques todos os dias (fonte). A própria Kaspersky divulgou que o Brasil concentra 92% dos ataques de Ransomwares na América Latina.
Um ataque por ransomware pode afetar os negócios da seguinte maneira:

- **Paralisação da empresa:** As empresas deixam de funcionar pois seus computadores ficam inacessíveis. Esta parada pode ocorrer por tempo indeterminado.

- **Perda de informações importantes:** Como os arquivos são criptografados, a empresa precisa pagar ao criminoso para fazer a decriptografia dos arquivos. Mesmo pagando o resgate de seus computadores, ainda sim não é garantia que terá os dados de volta.

- **Perda de credibilidade:** Seus clientes podem não confiar mais em você, já que sua empresa poderá estar paralisada.

- **Prejuízos financeiros:** Imagine não conseguir emitir nota fiscal? Ou sem perder os dados clínicos dos pacientes?

Como evitar?

- Mantenha backup atualizado do computador, de preferência em HD externo ou pen drive e nunca os deixe espetados na máquina, pois também poderão ser invadidos ou infectados;

- Mantenha antivírus e firewalls sempre ativados e atualizados;

- Evite acesso a sites suspeitos;

- Fique alerta e não clique em links duvidosos de e-mails suspeitos.

Se acontecer, o que fazer:

1. Não apague os e-mails e/ou mensagens recebidas do criminoso;

2. Se houver conversa com o criminoso via rede social, salve o nome do perfil e o link completo do perfil (endereço completo que aparece ao se clicar na barra de endereço);

3. Em caso de contato por telefone, faça uma relação todos os números de telefone utilizados pelo criminoso, contendo data e horário das conversas;

4. Anote os dados de eventuais contas bancárias, inclusive carteiras eletrônicas de bitcoins informados pelo criminoso;

5. Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico.

Cuidar de você e da segurança dos seus dados. **Esse é plano.**

Unimed

LGPD