Parabéns se você chegou até que significa que fez tudo certinho e nas próximas paginas poderá iniciar a leitura.

GUARDE ESSE E-BOOK COMPARTILHE ELE COM SEUS AMIGOS E COLOQUE TODAS AS DICAS EM PRÁTICA POR MAIS SIMPLES QUE PAREÇA.

Para mais informações acesse:

www.3ainformatica.net

Email:

contato@3ainformatica.net

SAIBA COMO PROTEGER OS DADOS DA SUA EMPRESA

O QUE É UM RANSOMWARE?

WannaCry

Global Cyber Attacks

Olá seja bem-vindo a esse e-book que preparamos de forma bem resumida e simplificada para lhe auxiliar na prevenção da praga digital que mais causou prejuízo a empresas e também a usuários domésticos, o RANSOMWARE.

O que é o vírus RANSOMWARE ?

Programa que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate para restabelecer o acesso ao usuário.

- **É um tipo de código malicioso**
  - assim como vírus, trojan, backdoor, worm, bot e spyware.
- **Pode Infectar:**
  - computadores (desktop, notebook, servidores etc.)
  - equipamentos de rede (modems, switches, roteadores e etc.)
- **Ações mais comuns**
  - impede o acesso ao equipamento (locker ransomware)
  - impede o acesso aos dados armazenados, geralmente usando criptografia (ransomware)
- **Extorsão é o principal objetivo**
  - pagamento feito via bit-coins
  - não ha garantia que o acesso sera restabelecido mesmo que o resgate seja pago
- **Costuma buscar outros dispositivos conectados, locais ou em rede, e criptografá-lo também**

- **A infecção pode ocorrer pela execução do arquivo infectado recebido via:**
  - links em e-mails, redes sociais e mensagens instantâneas como o whatsapp, messenger e etc.
  - anexado a e-mails
  Acessado via:
  - arquivos compartilhados
  - paginas web maliciosas, usando navegadores vulneráveis
  - downloads de arquivos como foto, musicas, vídeo e aplicativos.
- **Não se propaga sozinho**

E PORQUE VOCÊ DEVE SE PREOCUPAR ?
TALVEZ VOCÊ AINDA NÃO SAIBA REALMENTE O VALOR DOS SEUS ARQUIVOS, JÁ OUVIU FALAR QUE SÓ DAMOS DEVIDO VALOR A ALGO QUANDO PERDEMOS?
E SE O PIOR ACONTECER PODE SER TARDE DEMAIS.

É uma realidade que nos dias de hoje evitamos o máximo de papel e optemos por guardar tudo de forma digital, e por isso é necessário tomarmos devidos cuidados básicos.

Imagine se você perdesse todo o banco de dados de clientes, produtos e finanças cadastrados ou as fotos do seu filho quando era recém nascido.

Um computador por exemplo: custa dois mil reais e se por acaso quebrar tem como concertar ou trocar, mas com arquivos não é assim.

Além de um valor inestimável para uma empresa nos dispositivos pessoais possui um valor sentimental.

Para evitar a perca dos seus dados é preciso que mantenha seus equipamentos seguros e adote uma postura preventiva, o que inclui, entre outras coisas, fazer cópias de segurança dos seus arquivos, ou seja, realizar **backups**.

COMO SE PREVENIR

VOCÊ FEZ O BACKUP HOJE ?

"A melhor prevenção é impedir a infecção inicial, nem sempre é possível reverter as ações danosas já feitas ou recuperar totalmente os dados".

Backup é a solução mais efetiva contra Ransomware!.

- Mantenha os backups atualizados de acordo com a frequência de alteração de dados.
- Configure para que seus backups sejam realizados automaticamente
- Certifique-se de que eles estejam sendo feitos (validação) e testes se é possível recupera-lo.
- Nunca recupere um backup se desconfiar que ele contém dados não confiáveis
- Mantenha os backups desconectados do sistema para que eles não sejam infectados também.
- Faça cópias redundantes

OUTROS CUIDADOS A SEREM TOMADOS:

- Tenha sempre as versões mais recentes e originais dos programas.
- Remova os programas que você não utiliza mais, pois versões antigas de programas são mais vulneráveis. (isso vale p/ Smartphone)
- Configure a atualização automática dos programas.
- Instale um antivírus e mantenha-o atualizado e com configurado para fazer varredura automaticamente.

- Verifique sempre os arquivos recebidos antes de abri-los ou executá-los.
- Assegure-se de ter um firewall pessoal instalado e ativo.
- Desabilite a auto-execução de mídias removíveis e arquivos anexados.
- Verifique se as permissões de instalação e execução são coerentes Selecione os aplicativos, escolhendo aqueles: bem avaliados com grande quantidade de usuários.
- Mensagens de conhecidos nem sempre são confiáveis, o campo do remetente pode ter sido enviado de conta falsa ou invadida.
- A informação passou a ser considerada um dos ativos de mais importância crítica para as organizações.

Estamos na era da tecnologia de informação, a sociedade busca inclusão digital como modo de sobrevivência, crescimento profissional, as empresas buscam tecnologia, inovação, recursos para investir em TI, melhorar seus processos e até vendas por meio da TI.

Enfim, espero que esse e-book tenha lhe ajudado ou ao menos lhe alertado não somente sobre a infecção do vírus RANSOMWARE como diz o titulo da capa, mas sobre o valor que os dados da sua empresa tem.

Alessandro Gama - Técnico/Analista de Suporte

3A SOLUÇÕES EM TI

MSP KASPERSKY Microsoft ECI Expert Corporate IT SOLUÇÃO DE BACKUP EM NUVEM