RANSOMWARE

13 DICAS VALIOSAS PARA ANALISTAS DE SEGURANÇA

ostec
Segurança digital de resultados

Este material foi desenvolvido especialmente para analistas e gestores de segurança que entendem a importância de aplicar medidas para evitar sequestro de dados nas organizações, independente do seu porte ou segmento.

ÍNDICE

INTRODUÇÃO	3
DICA #1	4
DICA #2	4
DICA #3	5
DICA #4	5
DICA #5	6
DICA #6	6
DICA #7	7
DICA #8	7
DICA #9	8
DICA #10	8
DICA #11	8
DICA #12	9
DICA #13	9
CONSIDERAÇÕES FINAIS	10

INTRODUÇÃO

Este material foi desenvolvido especialmente para analistas e gestores de segurança que entendem a importância de aplicar medidas para evitar sequestro de dados nas organizações, independente do seu porte ou segmento.

Diante de tantas ocorrências associadas a sequestro de dados, torna-se inevitável promover alterações na estrutura corporativa para prevenir ou minimizar os impactos causados por sinistros gerados por Ransomware.

O e-book foi estruturado por especialistas em segurança digital, com vasta experiência prática na implantação de projetos envolvendo níveis variados de complexidade. Por isso, a leitura deste material é considerada item obrigatório para profissionais de tecnologia que visam minimizar as chances de passar por transtornos associados a cryptomalwares focados em sequestro de dados corporativos.

DICA #1

O lado humano por muito tempo foi considerado o elo mais fraco em uma arquitetura de segurança digital. Contudo, a realidade pode ser outra quando as pessoas recebem as devidas orientações e passam a fazer parte da estratégia de defesa da empresa. Por mais recursos que a organização possua, é imprescindível que os colaboradores recebam orientações sobre boas práticas de segurança da informação e uso dos recursos corporativos. Treinamentos com abordagem preventiva e reciclagens constantes são essenciais. Distribuição de materiais informativos e educativos é uma alternativa simples para lhe ajudar nesta tarefa.

DICA #2

Mantenha o "perímetro" da sua empresa seguro. Utilize uma **solução de firewall** e não exponha externamente redirecionamentos de locais internos da sua rede sem origens definidas e/ou recursos de autenticação e/ou criptografia com o uso de credenciais controladas.

DICA #3

Utilize senhas complexas e altere-as periodicamente - defina uma política de senhas. Senhas fracas são facilmente quebradas com ataques de brute force (força bruta), podendo expor portas para a injeção de ransomware na sua empresa.

DICA #4

Proteja o endpoint. Assegure que o que chega de fora até o usuário final esteja o protegido contra ameaças. Um software antivírus atualizado e uma boa solução de **segurança de e-mails (antispam)** são ferramentas básicas de proteção.

DICA #5

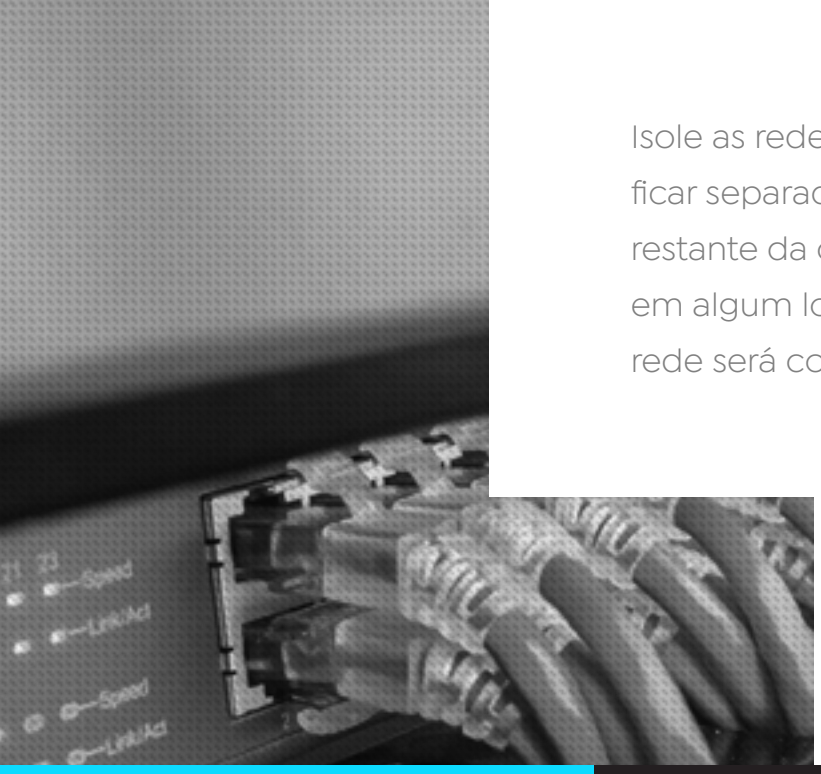
Atualize o parque. Não só de hardware atualizado depende o bom funcionamento da empresa. Softwares desatualizados são comumente utilizados para a exploração de vulnerabilidades de segurança, e por isso representam um risco para a empresa.

DICA #6

Controle o uso de dispositivos externos. Pendrives, HDs externos, celulares, câmeras e outros dispositivos com unidades de armazenamento podem iniciar uma infecção em uma estação de trabalho, o que por sua vez pode potencialmente disseminar a ameaça para toda a rede.

DICA #7

Isole as redes. Operações e setores críticos devem ficar separados em faixas de redes distintas do restante da organização. Assim, caso ocorra infeção em algum local, um menor número de ativos de rede será comprometido.



DICA #8

As redes visitantes devem estar sempre isoladas das redes corporativas. Como não temos nenhum controle sobre os dispositivos dos visitantes (mesmo que bem-intencionados), esta é uma premissa básica de segurança.

DICA #9

Controle os acessos e os compartilhamentos. É importante que todos os acessos aos conteúdos externos (sites, FTPs) e internos (compartilhamentos) possuam algum tipo de monitoramento e/ou controle, se possível com uso de credenciais de acesso controladas.

DICA #10

Crie estratégias de alta disponibilidade e disaster recovery (redundância de dados, política de backup) e execute testes constantes para garantir que em caso de qualquer sinistro você possui a estrutura necessária para uma recuperação rápida e consistente.

DICA #11

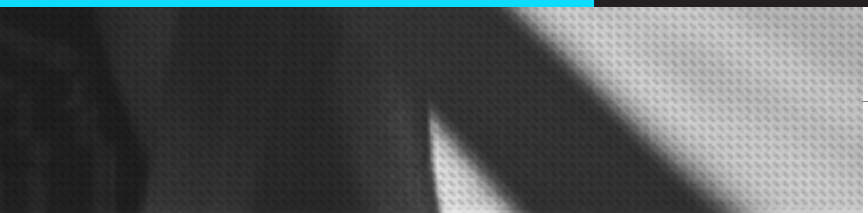
Considere a contratação de um seguro cibernético. Este tipo de produto está cada vez mais em alta, cabe a você e sua empresa avaliarem a relação entre custo e benefício para o negócio.

DICA #12

Forme um comitê para assuntos de segurança digital, defina agendas recorrentes com foco no tema e delegue responsabilidades. Este comitê não precisa ser formado apenas por profissionais da área de TI (e nem é indicado que seja, para gerar consciência, engajamento e senso de prioridade em todas as áreas).

DICA #13

Defina uma política de segurança da informação. Caso isso não seja aderente com a realidade do negócio, inicie com o desenvolvimento de política para o uso da internet. Reuna todos os itens acima e escreva orientações básicas para que todos os colaboradores tomem ciência, assinem e se comprometam. Você pode incrementar esta política com itens que abordam desde diretrizes para uso de equipamentos até cláusulas sobre confidencialidade das informações corporativas, por exemplo.



CONSIDERAÇÕES FINAIS

Em muitos casos, dependendo do tamanho, orçamento e principalmente maturidade da empresa em relação à tecnologia e segurança da informação, não é possível atacar todos os pontos a curto ou até mesmo a médio prazo.

Comece aos poucos, com os itens mais simples e, o mais importante, procure conscientizar os decisores em relação aos riscos do sequestro de dados ao negligenciar princípios básicos de segurança da informação. Caso necessário, uso como referência o conteúdo Quanto sua empresa pode perder em um ataque de sequestro de dados.

Busque um levantamento de quanto custa cada dia, hora ou minuto de operação da empresa parada, quanto valem os dados operacionais, dados de funcionários, parceiros, fornecedores e clientes.

A informação certamente é um dos itens mais valiosos de uma organização, e muitas pessoas mal-intencionadas já tomaram ciência disto.

CONTINUE LENDO

SE VOCÊ GOSTOU DO ASSUNTO E GOSTARIA DE NOVAS LEITURAS, FIQUE A VONTADE PARA CONSULTAR ATRAVÉS DOS LINKS ABAIXO TEMAS RELACIONADOS EM NOSSO PORTAL.

VOCÊ SE INTERESSOU PELO CONTEÚDO?

ESCLAREÇA SUAS DÚVIDAS COM ESPECIALISTAS NO ASSUNTO

CONVERSE COM ESPECIALISTA

facebook.com/ostec

linkedin.com/company/ostec-business-security

contato@ostec.com.br

www.ostec.com.br

ostec.blog

ostec

Segurança digital de resultados