RANSOMWARE

5 DICAS FUNDAMENTAIS PARA EVITAR SEQUESTRO DE DADOS

ostec
Segurança digital de resultados

O material traz informações essenciais sobre ataques Ransomware, que vem causando danos expressivos a empresas e usuários no Brasil e no mundo.

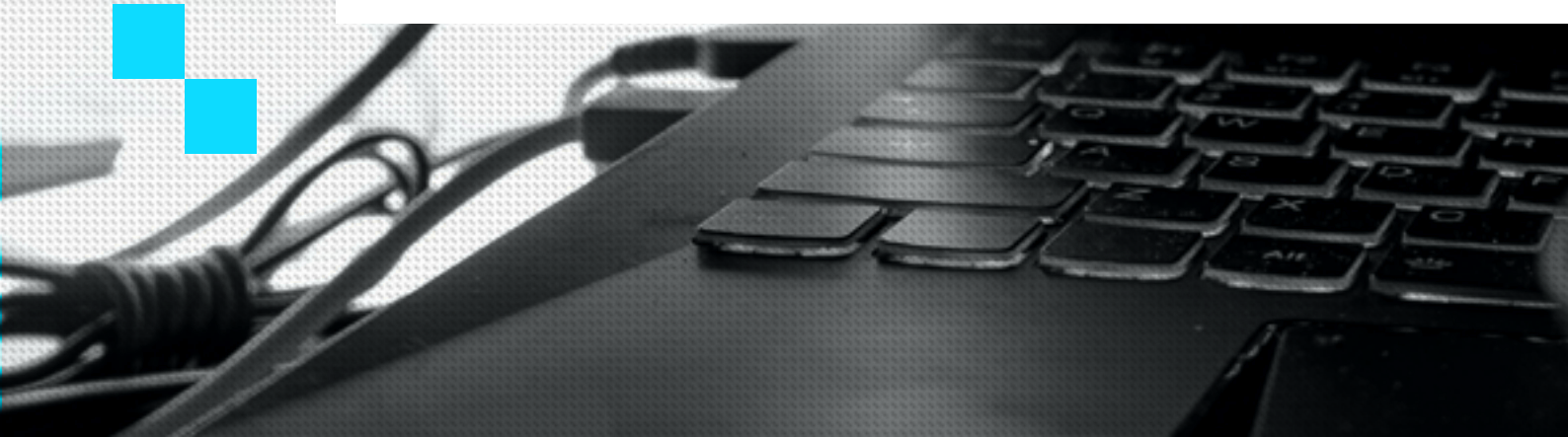
ÍNDICE

INTRODUÇÃO

Nos últimos anos, mais precisamente a partir de 2015, diversas empresas brasileiras passaram por problemas associados a sequestro de dados. A causa raiz destas ocorrências é um tipo de malware denominado ransomware (ransom em inglês significa resgate), que tem por finalidade obter dinheiro das vítimas em troca da devolução do acesso aos dados comprometidos.

O mais comum chama-se CryptoLocker, que criptografa determinados dados impedindo a utilização de sistemas ou aplicações. O atacante solicita então um pagamento para que se possa ter acesso novamente aos dados criptografados.

O pagamento na maioria das vezes é realizado através de bitcoin, que é uma moeda virtual onde o rastreamento é basicamente impossível de ser realizado e, portanto, localizar o atacante torna-se altamente complexo.



Esse tipo de malware era bastante utilizado na Rússia, e começou a comprometer empresas brasileiras mais fortemente a partir do ano de 2015. Atualmente, na Darkweb, é possível, inclusive, comprar como serviço uma estrutura de ransomware (RaaS), fazendo com que o problema tome proporções ainda maiores, atingindo empresas dos mais variados segmentos e portes.

O malware não possui peculiaridades, mas existem algumas dicas fundamentais para manter seu ambiente menos vulnerável a este tipo de ameaça.

DICA #1

MANTENHA O BACKUP EM DIA

Ter um backup é fundamental para qualquer estratégia de segurança, sendo a complexidade deste orientada pelo tamanho e importância do dado corporativo. Uma boa estrutura de backup é o principal ferramenta para minimizar os impactos de ataques ransomware.

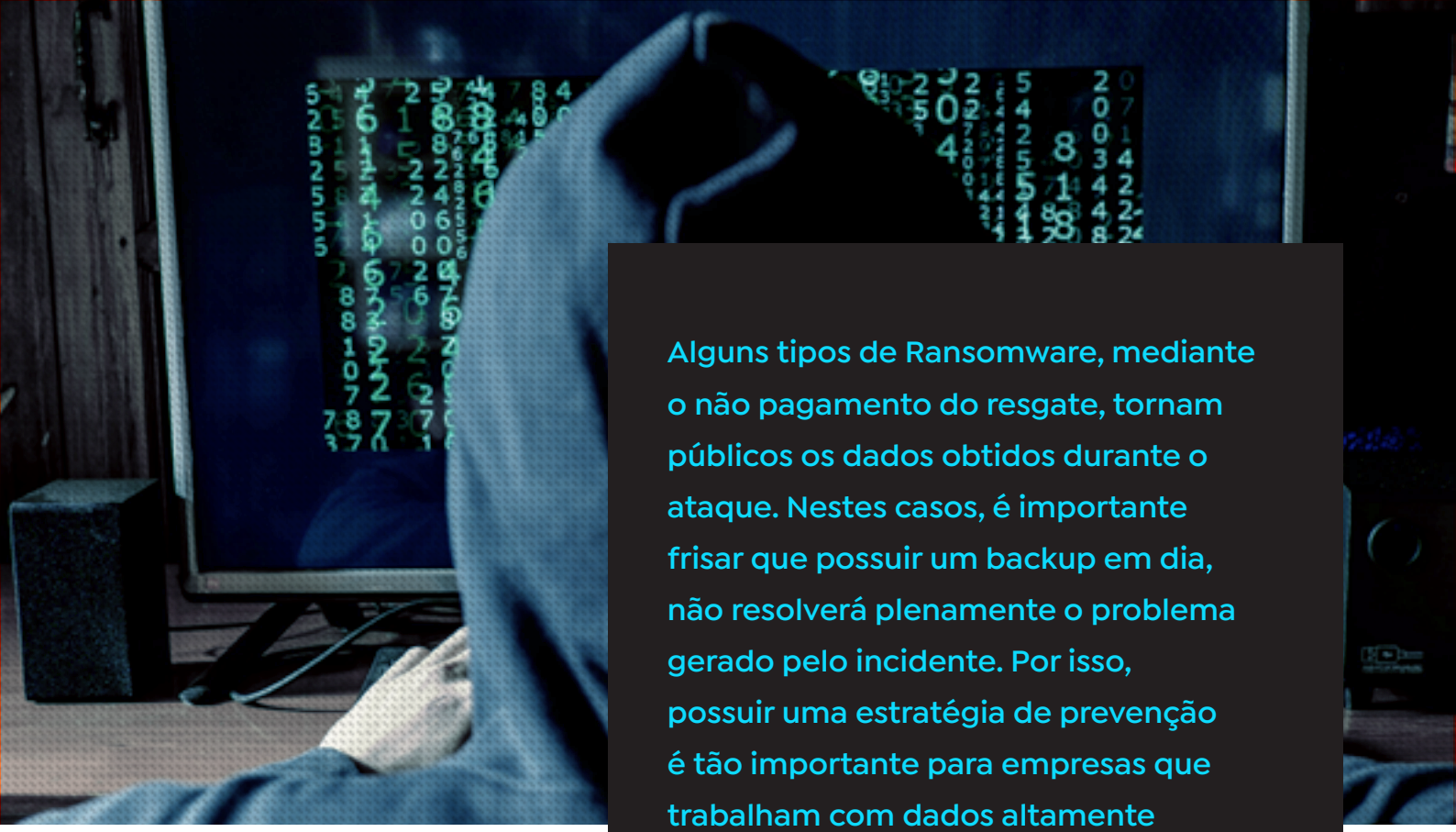
Isso por que se eventualmente a estrutura da empresa for comprometida, e a mesma possuir

os backups em dia, será possível zerar o servidor, máquina virtual ou dispositivo comprometido, e criar um novo ambiente a partir do último ponto de restauração.

Para outros negócios, no entanto, isso não é interessante, por que no intervalo entre um backup e outro são registradas muitas informações importantes, que não podem ser perdidas. Se esta for a realidade da sua empresa, independentemente do ransomware, é importante que a estrutura de backup seja repensada para que o ciclo de processamento atenda, de maneira plena, as necessidades do negócio.

O fato é que uma estrutura de backup pode ser um facilitador, tendo em vista que você não deve, em hipótese alguma, pagar pelo resgate dos seus dados. Tome cuidado com backups que são mantidos dentro do mesmo equipamento, ou em nuvem (acessível pelo equipamento comprometido), ou ainda em disco externo ou removível que continua conectado. Tudo isso pode ser comprometido, impossibilitando a restauração do backup!

Lembre-se, o backup não é uma solução de prevenção, mas pode claramente ser um grande aliado no momento em que um ambiente for comprometido, tanto em tempo de restauração, quanto ao não pagamento das quantias solicitadas.



Alguns tipos de Ransomware, mediante o não pagamento do resgate, tornam públicos os dados obtidos durante o ataque. Nestes casos, é importante frisar que possuir um backup em dia, não resolverá plenamente o problema gerado pelo incidente. Por isso, possuir uma estratégia de prevenção é tão importante para empresas que trabalham com dados altamente sensíveis.

DICA #2

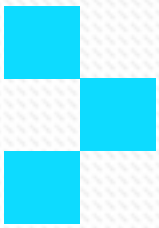
EVITE REDIRECIONAMENTOS PÚBLICOS DE PORTA

Um dos campos de pesquisa oportunista de ramsonware é procurar por portas abertas de serviços de terminal (como WTS/RDS/VNC e etc), que oferece, mediante usuário e senha, acesso à computadores ou servidores. Neste sentido, é de grande importância esclarecer que não se tratam de ataques direcionados, e sim oportunista, atingindo empresas, independente do seu porte ou segmento. Isso significa que os atacantes estarão

testando sequencialmente, ou aleatoriamente toda, ou boa parte, dos endereços disponíveis na internet sem focar especificamente uma empresa.

Mesmo em estruturas com firewalls e outros dispositivos de segurança, infelizmente, ainda é comum encontrar redirecionamentos de porta para serviços internos sem qualquer restrição de origem. Isso significa que, indivíduos na internet, terão acesso àquela(s) porta(s).

Sabe-se que a maioria dos serviços trabalha com um nível básico de segurança exigindo credenciais de acesso, mas infelizmente a quantidade de senhas fracas e usuários padrões, abrem precedentes para ataques de força bruta, possibilitando acesso ao equipamento e execução do malware.



Portanto, quando for criar um redirecionamento de porta para um serviço privado, especialmente se oferece acesso ao controle do servidor ou ativo, pense bem e preferencialmente desista, ou aplique uma camada mínima de segurança limitando o acesso a um conjunto conhecido de endereços IP.

Alterar porta padrão de serviços para tentar impedir os ataques é uma grande ilusão, pois a maioria das estruturas de escaneamento em massa, identificam além das portas conhecidas e padronizadas, também o comportamento do protocolo. Então, segurança por obscuridade, de fato não é um bom caminho.

É orientada a utilização de VPNs para oferecer

esse tipo de serviço através da internet. Se quiser saber um pouco mais sobre acesso remoto seguro, utilizando VPNs, leia o artigo “VPN: Saiba o que é, seus tipos e importância”.

DICA #3

TENHA UM ANTIVÍRUS ATUALIZADO

Embora possa parecer uma coisa um tanto quanto óbvia em uma estrutura de segurança, muitas empresas ainda insistem em não manter um antivírus devidamente atualizado. Ou, preferem, utilizar soluções gratuitas, que em alguns casos são eficientes, mas oferecem limitações de cobertura ou tempo de atualização.

Portanto, analise um antivírus de mercado que possua boa reputação e eficiência e coloque em toda a sua estrutura computacional. Lembre-se que, se um determinado computador de sua rede estiver desprotegido, ele poderá ser porta de entrada para outros problemas em sua estrutura.

Na atualidade muitas soluções conseguem detectar o ransomware, mas infelizmente como a estrutura já foi comprometida, a recuperação dos dados, em si,

é algo realmente complexo de ser realizado. Mesmo assim, estas soluções são fundamentais em uma estratégia de defesa em profundidade.

Se você não possui nenhuma referência de um bom antivírus, recomendamos fortemente consulta no site http:/www.av-comparatives.org, trata-se de uma organização independente que tem como objetivo avaliar os AVs sobre vários aspectos e gerar reports para o mercado.

DICA #4 MANTENHA OS SOFTWARES ATUALIZADOS

Outro aspecto super simples, e por muitas vezes negligenciado, é a manutenção de softwares devidamente atualizados, e não utilização de softwares piratas, para minimizar as chances de comprometimento da estrutura tecnológica da empresa.

Dentro de uma empresa tenha o controle e padronize quais são os softwares que podem ser instalados nos equipamentos, bem como o que é permitido para o uso por determinados usuários ou setores.

Tenha um controlador de domínio e mantenha os usuários dos computadores sem privilégio de administração, sempre que possível. Infelizmente algumas aplicações tem sérios problemas de arquitetura de desenvolvimento e precisam ser executadas com permissões de administrador, contudo a orientação é evitá-las ao máximo, para garantir a continuidade e integridade do ambiente.

Nesta mesma linha construa uma política de senhas forte, que não somente tenha critérios claros de construção, mas que também possuam ciclos mais curtos de troca, dificultando ataques de força bruta. E por fim, evite usar logins com nomes muito comuns ou totalmente previsíveis pelo mundo externo (admin, administrador, administrator, adm, etc).

Lembre-se, manter um ambiente totalmente legalizado, com controle de softwares nos computadores e servidores, com as devidas atualizações, é um passo importante para evitar os mais variados problemas, incluindo malwares e sequestro da base de dados.

DICA #5

DEFESA EM PROFUNDIDADE

A defesa em profundidade, ou também conhecida como defesa em camadas, basicamente afirma que um elemento sozinho, dentro de uma arquitetura computacional, jamais será capaz de proteger toda a sua estrutura. Complementa afirmando que são necessárias diversas camadas de segurança, com variados softwares e finalidades, para potencializar a integridade e confidencialidade das informações.

Em resumo, isso significa que jamais um dos itens aqui citados trará o resultado desejado. Pelo contrário, a soma dos itens abordados nesse material, juntamente com outras soluções de segurança, é o que vai, em conjunto, minimizar a exposição do ambiente, ou em último caso, quando infectado, diminuir os impactos ou estragos causados na estrutura corporativa.

Por conta disso, possuir um firewall devidamente configurado e alinhado as necessidades de segurança do seu negócio, com perfis de acesso e políticas muito bem definidas, ajudam a prevenir a ocorrência de sinistros

com malwares. É importante que estejam incorporados recursos como IDS/IPS, WAF e outros.

Além disso, atualmente os e-mails acabam sendo um grande problema para empresas, pois embora o modelo e propósito de infecção tenha sido alterado, mais focado em phishing, existe uma fatia representativa dos incidentes que são causados por cliques em anexos presentes nos e-mails.

Possuir um antispam corporativo é algo fundamental, pois através deste cria-se uma camada robusta de segurança, impedindo que determinadas ameaças transponham o perímetro da organização, chegando até a caixa de entrada das contas de e-mail corporativas. Além disso, um antispam evita problemas associados a produtividade, uma vez que atua na redução do recebimento de e-mails não solicitados.

Saindo do perímetro, reforçamos a importância de um antivírus com controle centralizado, permitindo gerenciar a atualização de todas as estações da empresa, assim como a utilização de dispositivos removíveis e outros pontos potenciais de infecção.

Por fim, a estrutura de segurança precisa ser pensada em camadas, mesmo que em algumas vezes um pouco redundantes, mas dependendo do nível de criticidade do negócio, é fundamental atuar de forma mais rígida.

OUTRAS CONSIDERAÇÕES

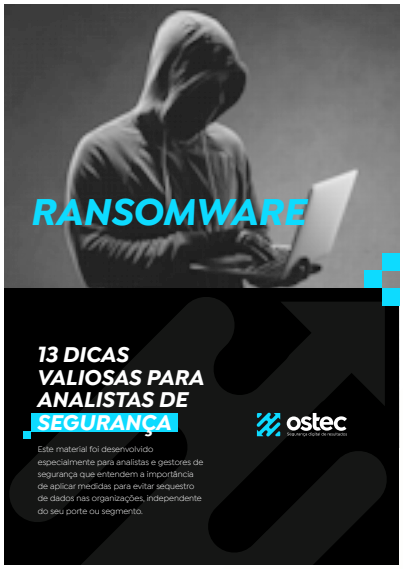
Se sua empresa foi infectada por um ransomware, contate imediatamente seu parceiro de segurança ou alguma empresa especializada para auxiliar na condução da situação e jamais pague pelo resgate!

Para aqueles que não tiveram problemas e eventualmente não estão em conformidade com as reflexões expostas nesse material, sugerimos profundamente que validem seus ambientes para evitar maiores inconvenientes.

A prevenção é sempre o melhor caminho, por conta disso, recomendamos que você faça um diagnóstico gratuito de segurança para seu negócio, e se preferir, agende também gratuitamente uma conversa com um de nossos especialistas.

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-security


contato@ostec.com.br


www.ostec.com.br


ostec.blog

ostec
Segurança digital de resultados