CINCO DICAS PARA **FORTALECER SUA SEGURANÇA** CONTRA OS ATAQUES DE **RANSOMWARE**

01 MANTENHA SEUS PROGRAMAS ANTIVÍRUS ATUALIZADOS

Para que o antivírus detecte rapidamente as ameaças à rede, é fundamental que sua biblioteca esteja **sempre atualizada**.

02 INVISTA EM FIREWALL

Não é possível garantir que todos os dispositivos em contato com sua rede corporativa contem com as **defesas necessárias** para conter ameaças, como celulares de visitantes ou as máquinas de colaboradores que atuam sob o modelo BYOD. Assim, a implantação de **sistemas de firewall é altamente recomendada**, visto seu potencial para impedir que *malwares* provenientes dessas fontes ameacem a integridade da rede protegida.

03 ESTABELEÇA UMA ROTINA DE BACKUPS

Como os ataques de *ransomware* inviabilizam o acesso dos usuários aos arquivos criptografados, ter em mãos uma cópia desses dados reduz significativamente o impacto do ataque.

04 MAPEIE OS DADOS CRÍTICOS PARA A OPERAÇÃO DA EMPRESA

Entre as consequências mais graves de um ataque de ransomware, está o impacto sobre **dados fundamentais** para o funcionamento da empresa. Para diminuir possíveis danos que obriguem a companhia a congelar suas atividades, é preciso levantar quais as informações críticas para a operação e trabalhar com o menor intervalo possível de **backups** desses dados.

05 TENHA UM PLANO DE CONTINGÊNCIA

Um forte aliado nesse quesito é o programa de **Recuperação de Desastres**, que espelha os dados operacionais em tempo real, armazenando-os num ambiente seguro. Em caso de ataque, esse local de backup assume como rede principal e garante a continuidade dos processos operacionais – em menos de 4 segundos.

"Fonte: Guia sobre Ransonware - Nov/2016"

Quer saber mais sobre esse assunto? Faça o download gratuito do e-book **Guia sobre Ransomware**, elaborado pela EsyWorld!

esy World