Resumo da solução: como se proteger contra ransomwares

Oito melhores práticas para evitar que seus dados sejam mantidos como reféns

Ransomware é um termo usado para descrever um malware que nega o acesso aos dados ou sistemas, a menos que seja paga uma taxa ao criminoso cibernético. Todas as organizações estão sujeitas a ataques de ransomware. Felizmente, há algumas etapas que você pode realizar para minimizar o risco da sua organização. Veja a seguir oito melhores práticas para proteger a sua organização contra ataques de ransomware.

1. Treinamento e conscientização

O treinamento e a conscientização do usuário são primordiais, além de ser a primeira etapa para se proteger contra o ransomware. As instruções ao usuário devem incluir:

- Tratar qualquer e-mail suspeito com cuidado
- Verificar o nome do domínio que enviou o e-mail
- Verificar se há erros ortográficos, analisar a assinatura e legitimidade da solicitação
- Passar o mouse pelos links para verificar seus destinos e, se houver alguma URL suspeita, digitar o endereço do site ou pesquisar nos mecanismos de busca, mas não clicar no link do e-mail

2. Segurança de e-mail

Implante uma solução de segurança de e-mail capaz de verificar todos os anexos, além de filtrar spyware e spam. Junto com avaliações de risco e treinamento periódico do usuário, realize testes de vulnerabilidade de phishing.

3. Antimalware

Seja em dispositivos pessoais ou corporativos, os endpoints estarão em risco se não forem gerenciados pela TI ou não tiverem a proteção antimalware correta. A maioria das soluções antivírus é baseada em assinatura e se mostra ineficaz quando não é atualizada regularmente. As mais recentes variantes de ransomware são criptografadas de forma exclusiva, o que as tornam indetectáveis com o uso das técnicas baseadas em assinatura.

Vários usuários desativam seus antivírus para que a velocidade do sistema não seja reduzida. Para abordar essas limitações, existem soluções de segurança de endpoint que utilizam inteligência artificial e aprendizado de máquina avançado para detectar malware. Elas também apresentam um pequeno espaço ocupado, o que causa uma sobrecarga mínima no desempenho.

4. Endpoints móveis

O gerenciamento de endpoints também é um desafio em constante crescimento conforme os dispositivos com vários formatos e sistemas operacionais são introduzidos na rede. Os dispositivos móveis são particularmente vulneráveis, conforme observado pelo Relatório anual de ameaças da Dell Security de 2016, com ameaças emergentes de ransomware na plataforma Android™. Escolher uma solução capaz de automatizar as atualizações de versão e patch em um dispositivo heterogêneo, ambiente do aplicativo e sistema operacional, ainda terá um longo caminho na abordagem de diversas ameaças cibernéticas, inclusive o ransomware.

Para os usuários remotos que estão fora do perímetro do firewall empresarial, o acesso baseado em VPN deve não somente estabelecer uma conexão segura, como também conduzir um nível de interrogação de dispositivo para verificar a política de conformidade no endpoint. Se um endpoint não tiver as atualizações de segurança necessárias, ele não será permitido na rede ou seu acesso será concedido de forma limitada a somente alguns recursos.

Especificamente para usuários de dispositivos móveis Android, veja a seguir as etapasrecomendadas:

- Não enraíze o dispositivo, pois isso expõe os arquivos do sistema a modificações
- Instale sempre aplicativos da Google Play Store, já que aplicativos sites ou lojas desconhecidas podem ser falsos e possivelmente mal-intencionados
- Desative a instalação de aplicativos de fontes desconhecidas
- Permita que o Google verifique o dispositivoa procura de ameaças
- Tome cuidado ao abrir links desconhecidos, recebidos por SMS ou e-mails
- Instale aplicativos de segurança de terceiros que verifiquem o dispositivo regularmente à procura de conteúdo mal-intencionado
- Monitore os aplicativos que serão registrados como administradores de dispositivos
- Para dispositivos com gerenciamentocorporativo, crie uma lista negra dos aplicativos proibidos

5. Segmentação de rede

A maioria dos ransomwares tentará se disseminar do endpoint até o servidor/armazenamento aonde os dados e aplicativos de missão crítica residem. Segmentar a rede e manter os dispositivos e aplicativos críticos isolados em uma rede separada ou LAN virtual pode limitar a disseminação.

6. Backup e recuperação

Outra proteção para não ter de pagar taxas é uma estratégia eficiente de backup e recuperação. Faça o backup dos dados de forma regular. Se houver um backup remoto, haverá uma perda menor de dados no caso de infecção. Dependendo da rapidez em que o comprometimento for detectado, até onde ele se disseminou e o nível aceitável de dados perdidos, a recuperação a partir de um backup pode ser uma boa opção. Entretanto, essa opção de compra para uma estratégia de backup inteligente está alinhada à criticidade dos seus dados e às necessidades dos seus negócios em relação aos Recovery Point Objectives (RPO) e Recovery Time Objectives (RTO). Recupere grande parte de seus dados críticos no menor tempo possível. Por fim, apenas ter uma estratégia não é suficiente. O teste periódico da recuperação de desastres e da continuidade dos negócios é tão importante quanto.

7. Ataques criptografados

Ter o firmware empresarial correto, capaz de verificar todo o tráfego, independentemente do tamanho do arquivo, também é de extrema importância. Com o rápido aumento no tráfego criptografado por SSL, conforme indicado pelo Relatório de ameaças da Dell Security, há sempre o risco de fazer o download de malware criptografado invisível aos firewalls tradicionais. Por isso, é importante garantir que o firewall/IPS possa descriptografar e inspecionar o tráfego criptografado sem reduzir significativamente a velocidade da rede.

Outra recomendação é mostrar as extensões de arquivos ocultos. Por exemplo, às vezes o malware pode entrar no sistema através de um ícone de .pdf ou .mp3, mas ser, na verdade, um arquivo .exe.

Uma abordagem eficaz para o bloqueio de ransomware requer uma ampla coordenação de gerenciamento, tecnologia e treinamento de segurança.

8. Monitoramento e gerenciamento

O firewall empresarial deve ser capaz de monitorar tanto o tráfego de entrada como o de saída, além de bloquear a comunicação com os endereços IP da lista negra conforme o ransomware tenta estabelecer contato com seus servidores de controle e comando.

Se for detectada uma infecção por ransomware, desconecte imediatamente o sistema infectado da rede corporativa. Assim que uma nova variante de malware é detectada, o firewall deve ter um processo de gerenciamento centralizado e atualização automática para implantar atualizações e políticas de forma rápida e consistente em todos os nós. Além disso, é crucial atualizar o software e os sistemas operacionais regularmente.

Conclusão

As soluções SonicWALL e One Identity conseguem aprimorar a proteção em sua organização ao inspecionar todos os pacotes e governar todas as identidades. Dessa forma, seus dados são protegidos onde quer que eles estejam, além do compartilhamento de inteligência para mantê-lo seguro contra diversas ameaças, inclusive ransomware.

Saiba mais sobre nossos firewalls de próxima geração.

Para obter mais informações

Sobre a Dell Security

As soluções da Dell Security ajudam na criação e manutenção de uma base de segurança sólida com soluções interconectadas que abrangem toda a empresa. Desde endpoints e usuários a redes, dados e identidades, as soluções da Dell Security mitigam riscos e reduzem a complexidade para que seus negócios evoluam. www.dell.com/security

Se você tiver dúvidas sobre o possível uso destematerial, entre em contato com:

Dell
www.dell.com/security

Consulte nosso site para obter informações sobre osescritórios regionais ou internacionais.