RELATÓRIO CONSULTIVO PARA EQUIPES DE SEGURANÇA

Principais recomendações para prevenir ransomware

O ransomware evoluiu de uma interferência de baixo grau para um negócio criminoso sofisticado e multimilionário que agora tem como alvo tanto indivíduos quanto empresas. É um modelo de negócios criminosos que usa software malicioso para sequestrar de forma criptografada seus dados pessoais. Embora seja um desafio cada vez mais urgente, é possível prevenir-se contra o ransomware com um treinamento apropriado, ajustes específicos no ambiente de TI atual e tecnologia de endpoint avançada.

O que é o ransomware?

Os invasores devem executar cinco passos para um ataque de ransomware ter sucesso:

1. **Comprometimento e controle do sistema.** A maioria dos ataques começam com spear phishing, ludibriando o usuário através de um e-mail fraudulento a abrir um arquivo anexo infectado que compromete o sistema. Isso pode afetar um único computador, celular ou uma empresa inteira.
2. **Impedir acesso ao sistema.** Uma vez infectado, um invasor pode tanto identificar e criptografar certos arquivos que provavelmente terão valor para a vítima, como documentos empresariais do tipo .doc, .xls e .pdf, quanto negar acesso total ao sistema por meio de telas de bloqueio ou táticas de intimidação.
3. **Avisar o dono do dispositivo sobre o comprometimento, valor do resgate e os passos a serem seguidos.** Apesar de aparentemente óbvio, os invasores e as vítimas geralmente falam idiomas diferentes e têm diferente nível de capacidade técnica, então os invasores têm que explicar para as vítimas em termos que elas possam entender o que aconteceu e, também, os passos a serem seguidos para destravar seus dispositivos.
4. **Aceitar o pagamento do resgate.** Um invasor precisa ter um meio para receber o pagamento do resgate enquanto evita rastreamento das autoridades policiais, o que explica o uso de moedas criptografadas anônimas, tais como bitcoin, para essas transações.
5. **Prometer a devolução de acesso total mediante recebimento do pagamento.** A impossibilidade de restaurar os sistemas comprometidos destruirá a eficácia do esquema, pois ninguém pagaria um resgate sem confiar que terá seus objetos de valor devolvidos.

QUEM CORRE RISCO?

Empresas na mira. Os ataques de ransomware podem ter um grande impacto público, pois as operações da organização vitimada podem ser seriamente afetadas ou totalmente interrompidas, o que pode ser ilustrado pelos recentes ataques a hospitais em todos os Estados Unidos. Os criminosos perceberam que essa é uma atividade lucrativa com poucas barreiras de entrada. Consequentemente, o ransomware tem superado outros modelos de crime cibernético. Além disso, os invasores estão se tornando mais sofisticados na sua capacidade de determinar o valor da informação comprometida, avaliar a vontade da organização em pagar e exigir resgates maiores.

Mais plataformas. Historicamente, enquanto os criminosos focavam exclusivamente nos sistemas Microsoft® Windows®, o surgimento do ransomware para Android™ e – conforme a Palo Alto Networks® descobriu recentemente – Mac® OS X® demonstra que nenhum sistema é imune a esses ataques. Quase todos computadores ou dispositivos com uma conexão de Internet são vítimas em potencial do ransomware, o que será uma preocupação mais urgente com o advento da Internet das Coisas (IoT) e da proliferação de dispositivos adicionais conectados à Internet, como tecnologia vestível e eletrodomésticos.

PREPARAR E PREVENIR

Os ataques de ransomware são rápidos – geralmente em questão de minutos após uma infecção – por isso, é fundamental tomar medidas e estabelecer controles que atenuem ou previnam ataques de ransomware. As próximas duas seções resumem as principais recomendações para fazer as duas coisas.

PRINCIPAIS RECOMENDAÇÕES PARA MINIMIZAR O IMPACTO DE RANSOMWARE

1. **Desenvolver e executar um plano para um programa de conscientização dos usuários finais**
   - Pode ser difícil obter aprovação para enviar lembretes de segurança regulares para toda a empresa, porém ter usuários finais mais inteligentes certamente resultará em menos incidentes de ransomware.
2. **Analisar/validar processos de backup de servidores**
   - Algumas organizações não percebem que seus backups estão comprometidos ou que foram configurados de forma inadequada, até que seja tarde demais. Você precisa deles para restaurar o serviço.
   - Comece com seus servidores de arquivos que a rede do host compartilha com departamentos essenciais.
3. **Analisar permissões da unidade de rede para minimizar o impacto que um único usuário pode ter**

   Analises de privilégio de usuários finais
   - Designe um gerente de projeto para organizar um esforço para avaliar permissões que os usuários tenham nas unidades de rede mapeadas. Implante o princípio do menor privilégio para minimizar o impacto que qualquer usuário individual possa ter nas unidades compartilhadas na rede da organização.
   - Dependendo do tamanho da organização, esse processo pode ser um esforço grande e complexo, por isso, comece com os locais da unidade de rede usados por departamentos essenciais.

   Analises de privilégio do usuário administrador
   - Examine as funções privilegiadas usadas pelas equipes de servidor, backup e rede para validar um acesso adequado.
   - Certifique-se de que sejam atribuídas contas normais e restritas aos administradores, separadas de suas contas altamente privilegiadas.
   - Exija que os administradores usem suas contras altamente privilegiadas apenas quando precisarem delas.
   - Elimine mapeamentos de unidade de rede automáticos das contas administrativas, sempre que possível.
   - Restrinja as contas administrativas de receberem e-mails.
4. **Documentar seu plano de resposta a incidentes para ransomware**
   - Você provavelmente já tem um plano de resposta a incidentes genéricos, mas você precisa estar especificamente pronto para o caso de um ransomware, porque isso exige um processo muito específico para a recuperação, muito diferente de outros incidentes de malware.
   - Casos em que todos os arquivos em toda a unidade de um departamento são criptografados podem se tornar bastante complexos, uma vez que diversas equipes precisam estar envolvidas – equipes de backup, equipe de servidor de arquivos, endpoint, equipe de diretório e outros. Quanto mais você planejar agora, mais rápido será seu tempo de resposta.

PRINCIPAIS RECOMENDAÇÕES PARA PREVENIR RANSOMWARE

1. **Desativar scripts de macro de arquivos do MS Office usando Política de Grupo AD**
   - De acordo com a Microsoft, 98% das ameaças que têm como alvo o Office usam macros. Desativar os scripts de macro dos arquivos do MS Office deterá ransomwares, como Locky.
   - A organização inteira pode não precisar das macros do Office, mas algumas pessoas precisarão. Ative as macros apenas para exceções ou determinados departamentos.
   - O Office 2016 tem um novo recurso que permite que os administradores impeçam macros de serem executadas em documentos Word, Excel e PowerPoint que sejam originárias da Internet. Por isso, se puder fazer a atualização, faça isso e ative esse recurso.
2. **Examinar seus processos de gerenciamento de patches mensais**
   - Muitas organizações lutam para aplicar patches em seus sistemas dentro de 30 dias após a liberação do patch mensal "Patch Tuesday" da Microsoft.
   - Analise seus processos de aplicação de patches e procure oportunidades para eliminar obstáculos.
   - Considere a implantação de um produto endpoint avançado que impeça explorações devido a patches ausentes e malwares.
3. **Examinar sua proteção de entrada contra spam/malware**
   - Certifique-se de você tenha uma configuração que bloqueie e-mails de entrada de acordo com as recomendações do seu fornecedor do servidor de e-mail (bloquear executáveis em anexos etc.).
4. **Implantar um firewall de última geração para proteger a rede**
   - Verifique se seu firewall bloqueia automaticamente ameaças conhecidas com base em informações de ameaças que são atualizadas constantemente.
   - Certifique-se de que seu firewall ofereça recursos de área limitada para que você possa deter ameaças desconhecidas (URLs e executáveis) antes que elas cheguem ao endpoint. Áreas limitadas são a melhor forma de detectar novas variantes de ransomware que estão constantemente aparecendo e se espalhando.
   - Configure seu firewall/proxy para exigir uma interação do usuário para a comunicação dos usuários finais com sites classificados como "não categorizados" (por exemplo, clicar em um botão "Prosseguir"). Muitos sites não categorizados são usados em campanhas de phishing direcionadas para distribuir malware. Esse processo de duas etapas evita que determinados tipos de ransomware façam a ligação externa para o servidor de comando e controle. Se isso não acontecer, talvez seus arquivos não sejam criptografados.
5. **Implantar uma proteção avançada de endpoint para proteger o endpoint**
   - Os antivírus tradicionais não são eficazes contra malwares avançados, como ransomware, que mudam constantemente para não serem detectados. Verifique se suas medidas de proteção de endpoint podem detectar malwares conhecidos e desconhecidos, assim como explorações conhecidas e desconhecidas, incluindo de dia zero.
   - Listas brancas podem funcionar para algumas organizações simples e menores, mas para organizações em crescimento com muitos aplicativos e complexidade, em pouco tempo, pode ser necessário muito trabalho para gerenciar a lista. A detecção de malware com base na técnica é muito eficaz na detecção de ransomware.
   - Certifique-se de que seus sistemas de proteção de endpoint estejam munidos de inteligência de ameaças em tempo real obtida de fontes internas e externas que ultrapassem limites organizacionais, regiões geográficas e setores.

PROCURANDO MAIS INFORMAÇÕES?

Ransomware: paloaltonetworks.com/solutions/initiatives/ransomware
TRAPS: paloaltonetworks.com/products/secure-the-endpoint/traps
NGFW: paloaltonetworks.com/products/secure-the-network/next-generation-firewall