Três dicas de práticas recomendadas para impedir ataques de ransomware

O número de ataques de ransomware explodiu nos últimos anos, infectando milhões de computadores e custando às empresas milhões de dólares. Recomendamos três melhores práticas que todas as organizações, independentemente do tamanho, devem empregar.

1. EDUCAÇÃO E CONSCIÊNCIA

Detestamos dizer isto, mas o seu maior vetor de ataque é também o mais fraco. Muito de seus funcionários nunca ouviram falar de phishing nem de um ataque man-in-the-middle, e os hackers sabem disso. É essencial que você eduque seus funcionários sobre os métodos de ataque mais comuns e como evitá-los, como:

- **Nunca clique em links fornecidos em um e-mail.** Digite ou copie o endereço no navegador para evitar abrir inadvertidamente um link mascarado para um site malicioso.
- **Tenha cuidado ao abrir anexos de e-mail.** Esse é um método de ataque comum de ransomware.
- **Ao acessar um site, preste atenção no URL**. Sites maliciosos comuns incluem URLs com endereços IP no início ou um suposto site seguro que não usa HTTPS.
- **Endereços de e-mail clonados são outro método de adquirir informações confidenciais**. Nunca envie informações pessoais via e-mail. Recomendamos simplesmente usar o telefone.
- **Nunca dê sua senha para alguém via e-mail.** Empresas legítimas nunca solicitam credenciais via e-mail.

2. BACKUP. BACKUP. BACKUP.

Apesar de evitar ameaças e ataques seja sempre o método ideal de defesa, você deve sempre ter um Plano B. Caso um ataque de malware avançado, especificamente ransomware, assuma o controle do seu sistema, realizar backups de dados regularmente pode lhe dar a tranquilidade de que os dados são recuperáveis. Eis algumas dicas para fazer backup das informações:

- **Backups off-line são essenciais.** Ransomwares modernos conseguem encontrar e criptografar o armazenamento em rede.
- **Simplifique os backups o máximo possível.** Crie um compartilhamento global que possa armazenar todas as informações mais importantes e aproveite partições de dados sempre que possível.
- **Automatize os backups sempre que possível.** Não deixe que um erro humano faça com que você perca um backup.

3. DEFESA APROFUNDADA

Ataques de ransomware buscam aproveitar todos os vetores de ataque possíveis. Quanto mais camadas de segurança houver em vigor, maior a chance que você tem de impedir um ataque que outra camada poderia deixar passar. Esses tipos de ataque conseguem se transformar em algo único, desviando-se de métodos tradicionais de detecção com base em assinatura. Eis algumas das camadas críticas de segurança que sua organização deve ter:

- **Proteja sua rede.** O ransomware usa a rede não só para se conectar a um servidor malicioso e obter a chave de criptografia, como também aproveita a rede para espalhar o ataque em uma organização.
- **Aproveite o ambiente de sandboxing para detonar ameaças de dia-zero.** O ambiente de sandboxing é uma excelente ferramenta para detonar malware desconhecido sem arriscar a segurança dos dispositivos.
- **Obtenha visibilidade em dispositivos de endpoint.** Ataques de ransomware frequentemente iniciam em dispositivos de endpoint. Ter visibilidade sobre a atividade de eventos desses dispositivos faz com que seja possível detectar e remediar as ameaças antes que o dano seja causado.
- **Conecte os pontos entre a rede e o endpoint**. Correlacionar dados de eventos da rede e do endpoint fornece uma avaliação abrangente do panorama geral de ameaças.

DICAS DE PRÁTICAS RECOMENDADAS

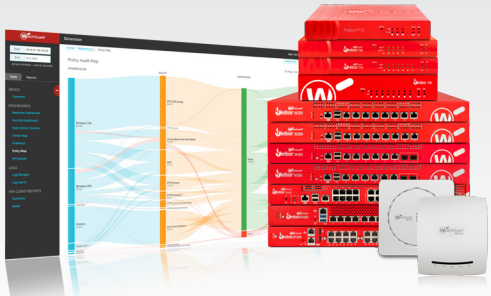
Com o WatchGuard Total Security Suite, organizações de todos os tamanhos agora podem se defender contra ameaças de malwares avançados, incluindo ataques de ransomware. O Total Security Suite é a primeira oferta de serviço de UTM que não só permite que organizações de todos os tamanhos detectem e corrijam ataques de ransomware, como também os impede. Ao combinar nossa tecnologia de WebBlocker, APT Blocker e Host Ransomware Prevention, a WatchGuard oferece o conjunto mais abrangente de serviços de segurança disponível em uma oferta disponível hoje no mercado.

Individualmente, cada uma dessas soluções pode proteger contra um estágio de um ataque de ransomware. O WebBlocker automaticamente nega aos usuários o acesso a sites maliciosos conhecidos, além de permitir a filtragem de URL, que pode bloquear também sites arriscados e inadequados. Com o APT Blocker, os usuários se beneficiam de recursos premiados de sandboxing para detectar ameaças suspeitas, detoná-las em um ambiente virtual e impedir que o ataque seja executado na rede. O Host Ransomware Prevention aproveita a análise comportamental para detectar especificamente ataques de ransomware e impedi-los antes que ocorra a criptografia de arquivos.

Produto	TOTAL SECURITY	Basic Security
Serviço de prevenção de intrusões (IPS)	✓	✓
Controle de aplicativos	✓	✓
WebBlocker	✓	✓
spamBlocker	✓	✓
Gateway AntiVirus	✓	✓
Reputation Enabled Defense (RED)	✓	✓
Descoberta de rede	✓	✓
APT Blocker	✓	
Prevenção contra perda de dados (DLP)	✓	
Dimension Command	✓	
Detecção e resposta a ameaças	✓	
Suporte	**Gold (24x7)**	Padrão (24x7)

A WatchGuard oferece um portfólio completo de soluções avançadas de segurança de rede para proteger as organizações, seus dados, funcionários e clientes.

- Dispositivos de segurança de rede
- Visibilidade de ameaças de rede
- Total Security Services
- Pontos de acesso sem fio seguros



Saiba mais em www.watchguard.com