WEBROOT SecureAnywhere®

minitel NEXT

Proteção DNS: A camada de cibersegurança mais negligenciada

Como podem os MSPs proteger o perímetro de rede dos seus clientes?

Introdução

O acesso não controlado à internet é uma atividade de elevado risco para qualquer negócio, especialmente se forem PMEs, que constituem a base de clientes dos MSPs (managed service providers). Infelizmente, ter apenas uma solução de segurança endpoint não é suficiente para garantir que os utilizadores estão protegidos contra os ciberataques modernos. Remediar ataques que se infiltraram a rede é uma tarefa complicada e morosa e, por isso, os MSPs apostam cada vez mais em serviços capazes de parar as ameaças antes que entrem na rede empresarial.

DNS (domain name system) é uma designação convencional para serviços, computadores e quaisquer outros recursos ligados à internet ou a redes privadas. Os servidores DNS traduzem inputs baseados em texto para o endereço de IP que direciona os dispositivos e serviços para o site desejado. Ao redirecionar o tráfego dos utilizadores finais através de uma solução de segurança para as camadas de domínio, baseada na cloud, os MSPs podem impor e ajustar políticas de acesso à web, garantir a conformidade com os regulamentos de proteção de dados e parar quase instantaneamente 90% das ameaças antes de entrarem na rede.

Ao aliar a tecnologia endpoint à proteção DNS, os MSPs asseguram aos clientes uma proteção abrangente, capaz de deter as ameaças modernas, sem custos elevados ou sobrecargas que afetem a largura de banda na rede. Contrariamente aos servidores proxy e às appliances de segurança web, cuja configuração e gestão podem ser muito dispendiosas, as soluções DNS são leves, fáceis de instalar e manter, tornando-as ideais para os MSPs, que devem não só considerar o custo inicial da solução, mas também o tempo de instalação, configuração e manutenção da solução de segurança.

Claro que nem todas as soluções DNS são criadas da mesma forma. Durante a seleção da solução, os MSPs devem considerar:

- **Eficácia:** A solução garante uma proteção eficaz, tempo real, baseada na inteligência de ameaças mais avançada e atual?
- **Fácil de utilizar:** A instalação e implementação são rápidas? A configuração é simples? É escalável?
- **Flexibilidade:** Inclui uma política de gestão que assegure HR e a conformidade com o GDPR? Pode utilizá-la para aplicar políticas de acesso à internet e melhorar a produtividade dos utilizadores finais?

A proteção DNS é essencial. Porquê?

Em todo o mundo, as organizações enfrentam problemas de segurança de rede que estão rapidamente a agravar-se. De acordo com o Global Threat Landscape 2018, 87% dos MSPs dizem ter tido servidores ou serviços indisponíveis com um ataque DDoS, em 2017.

Da mesma forma, o relatório do Efficient IP que inquiriu cerca de 1.000 organizações em todo o mundo, concluiu que cerca de 75% das empresas foram alvo de ataques DNS.

Refere também que quanto melhor é a segurança das empresas, mais criativos e eficazes se tornam os hackers e os seus ataques via DNS foram um dos meios de entrada.

À medida que o DNS se tornou fundamental, a sua arquitetura ficou mais aberta e tipicamente não monitorizada, tornando-se um alvo ideal para os hackers aproveitarem esta vulnerabilidade de todas as formas possíveis:

- **C&C (Botnet Command & Control):** Utilizado para ataques DDoS, roubo de dados, spam, acesso não autorizado e criação de contas falsas para ligação ao servidor
- **APT (Advanced Persistant Threat Attacks):** Concebidos para se espalharem, adaptarem e esconderem na infraestrutura IT para um ataque estratégico, a longo prazo.
- **Ransomware:** Cada vez mais comum, utiliza frequentemente comunicações baseadas em DNS com servidores C&C para atacar e iniciar o resgate.
- **Ameaças baseadas na web:** Mais de 85% dos links infetados são baseados em sites legítimos, mas comprometidos.

Existem ainda muitos outros tipos de ataque baseados no DNS e, infelizmente, muitas empresas deixam as portas 80 e 443 desprotegidas para permitir que o tráfego DNS chegue ao seu destino, comprometendo toda a rede.

Escolher uma solução DNS: Eficácia

Quando um MSP seleciona uma solução de segurança de domínio, a prioridade número um é garantir a proteção comprovada do seu cliente. No passado, os web proxies eram muito utilizados para o mesmo propósito, mas tinham inúmeras desvantagens:

- Deployment inconveniente, exigindo hosting e gestão;
- Configuração de servidores de políticas muito complexa;
- Filtros web pouco eficazes, que omitem sites recentemente comprometidos;
- Escalabilidade para diferentes locais muito dispendiosa;
- Causa atrasos ao analisar conteúdos do site.

Pelo contrário, as soluções baseadas em DNS não têm estes problemas de complexidade na instalação e de escalabilidade, não sendo necessário servidores on-premise, para além de serem muito mais simples de utilizar.

Como analisam apenas as camadas superficiais do domínios, tomam decisões e aplicam políticas numa fração do tempo, comparativamente às soluções baseadas em proxies.

A eficácia da solução DNS é determinada pela amplitude, profundidade e frequência dos updates da inteligência de ameaças e maior será a sua capacidade de identificar, alertar e prevenir ameaças de sites duvidosos ou maliciosos.

Escolher uma solução DNS: Facilidade

Quando a solução de segurança é standerizada para vários clientes, o tempo de manutenção é reduzido, libertando o departamento de IT e aumentando a sua eficiência.

Dedicar mais tempo à gestão com consolas separadas para as várias soluções, pode aumentar significativamente o volume de trabalho do técnico.

Se os MSP conseguirem ser mais eficazes, a sua rentabilidade também aumenta. Por isso, a solução de proteção DNS ideal integra na consola de segurança endpoint já existente, simplificando a implementação e gestão de tarefas, comparativamente às soluções DNS stand alone.

Este último ponto é digno de atenção: gastar tempo a gerir consolas de gestão separadas para várias soluções de segurança pode aumentar substancialmente o fluxo de trabalho técnico dos MSPs.

A implementação inicial deverá ser feita em apenas alguns minutos, necessitando apenas

de direcionar o tráfico da internet dos clientes através do serviço de proteção de domínio DNS, para verificar e controlar os seus acessos web.

A possibilidade de personalizar políticas de acesso para cada cliente, utilizando políticas globais ou site-based é uma funcionalidade chave que os MSP deveriam exigir.

Escolher uma solução DNS: Flexibilidade

Enquanto que o principal objetivo de uma solução de proteção DNS é garantir o máximo de segurança, deveria também permitir aos MSPs a flexibilidade necessária para acomodar políticas personalizadas para cada cliente, indo ao encontro das suas necessidades específicas.

Esta capacidade de gestão de políticas é particularmente útil para alcançar a conformidade legislativa das empresas clientes, com as disposições legislativas específicas da indústria como é o caso do GDPR.

Para maior utilidade, a solução de segurança DNS deve ainda incluir um vasto conjunto de políticas pré-definidas e filtragem granular, para gerir adequadamente os níveis de acesso dos utilizadores a sites perigosos ou indesejáveis.

As políticas de produtividade podem ajudar os clientes dos MSPs a aumentar a eficiência dos utilizadores, limitando as distrações online. Para além disso, podem utilizar políticas que bloqueiam tráfego indesejável como, por exemplo, o streaming de media para melhorar dramaticamente a largura de banda.

Outras funcionalidades chave que os MSPs devem procurar são:

- **Personalização das páginas bloqueadas:** permite utilizar as páginas bloqueadas dos MSPs ou específicas dos clientes.
- **Whitelist/Blacklist:** Criação de overrides personalizados para os clientes.
- **Designação de políticas diferentes por IP/utilizador:** permite garantir a segurança da rede do cliente e aplicar políticas mais granulares à network interna e externa.
- **Proteção da WiFi de visitantes:** Muitas organizações oferecem ligação de rede WiFi a visitantes e clientes (cafés, lojas, ginásios, aeroportos, clínicas, etc.) - estes pontos de acesso são igualmente vulneráveis a ataques e exigem a o mesmo nível de proteção que as redes empresariais, mas o preço que reflete o número de utilizadores é muitas vezes desconhecido. É necessário procurar uma solução que possa também proteger os visitantes dos clientes.

A resposta do Webroot com uma camada de segurança DNS

O **Webroot SecureAnywhere® DNS Protection** é uma solução simples mas eficaz para prevenir que a utilização diária da internet se torne num enorme risco de segurança. A proteção DNS é instalada em rápidos minutos, não requer hardware on-site ou software e é integrada diretamente na **consola Global Site Manager** para MSPs, a mesma que utilizam para gerir toda a proteção **Webroot SecureAnywhere**.

A proteção DNS permite que os administradores configurem as políticas com grande detalhe. Utilizando o menu intuitivo para preencher alguns detalhes do cliente e do IP e efetuando o simples teste de validação do serviço, podem garantir que tudo está operacional e funciona corretamente.

É possível atribuir políticas diferentes a cada IP de cada cliente, por isso, garantir a segurança das redes, proteger uma rede de visitantes WiFi ou aplicar políticas granulares é simples e rápido.

O **Webroot SecureAnywhere® DNS Protection** é baseado na **Webroot® Threat Intelligence Platform** - uma plataforma de segurança avançada e baseada em cloud, com um mecanismo de análise contextual que correlaciona as informações para uma percepção profunda do panorama digital em que os clientes se inserem.

Esta plataforma avançada de aprendizagem máquina faz continuamente a análise da internet e compara-a com as informações que recolheu dos seus milhões de outros clientes, possibilitando uma resposta rápida e adequada, mesmo a ameaças desconhecidas (ataques Zero-Day), numa escala sem precedentes.

O **Webroot DNS Protection** confere uma camada adicional de segurança e filtragem web contra sites infetados com malware ou spyware, permitindo que os parceiros ofereçam um controlo muito mais granular sobre os acessos aos sites dos clientes. Protege em tempo real contra ameaças, acessos não autorizados e ataques DDoS, melhorando drasticamente a visibilidade e controlo.

Em particular, a filtragem URL do Webroot DNS Protection baseia-se no **Webroot BrightCloud® Web Classification,** a maior base de dados deste tipo, que classifica mais de 600 milhões de domínios para update em tempo real. O Webroot analisa e categoriza mais de 5.000 URLs por segundo, com scans da totalidade do espaço IPv4 e IPv6 em utilização, classificando mais de 95% da internet pelo menos 3 vezes por dia. Analisa e classifica continuamente mais de 4 mil milhões de endereços IP, 27 mil milhões de URLs e descobre mais de 45 mil URLs maliciosos, 6.000 novos sites de phishing e 100 mil novos endereços IP maliciosos por dia (Estes serviços de inteligência são utilizados por mais de 65 fabricantes de renome, no mundo inteiro, especializados em rede e segurança.

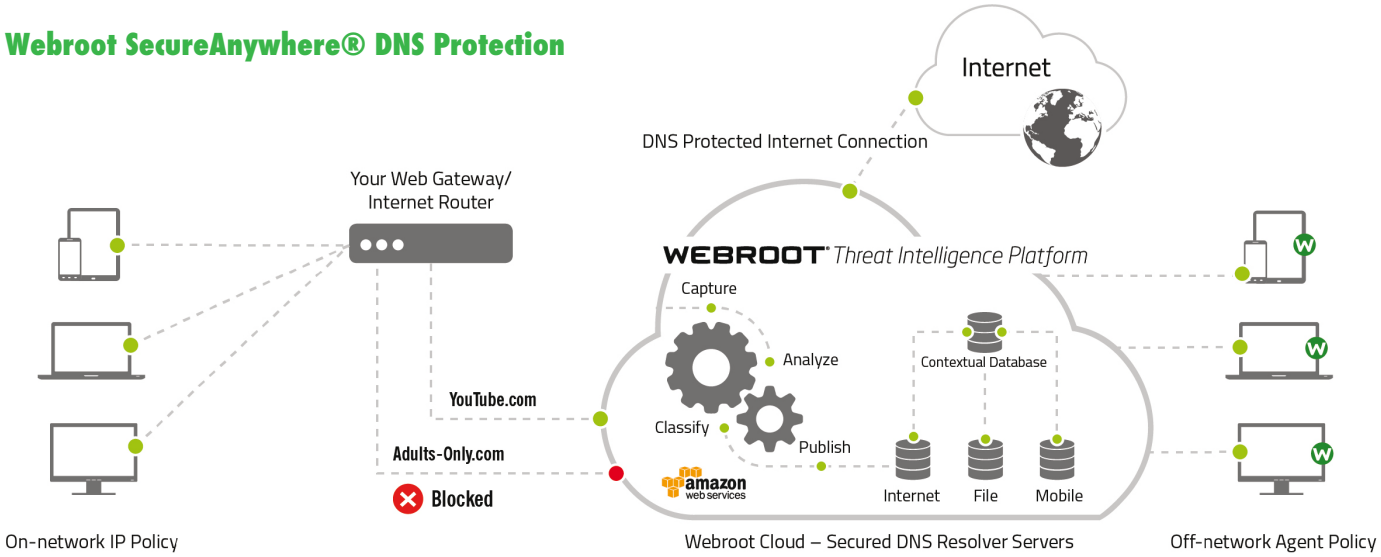
Uma das coisas que torna o Webroot tão eficaz é que, em vez de se focar apenas num tipo específico de dados, analisa as ligações entre diferentes objetos da internet, assegurando que nenhum objecto é descontextualizado, utilizando um modelo de análise de 'culpado por associação', para compreender não só o nível de risco, como também o potencial para atividades maliciosas futuras.

Por exemplo, se um utilizador utilizar uma aplicação móvel que tente aceder à lista de contactos e transferi-la para um endereço IP, o comportamento malicioso da app vai impactar negativamente a pontuação da reputação do endereço.

Esta funcionalidade de correlação de objetos, aliada ao histórico de milhões de análises anteriores garantem que o Webroot consegue prever com sucesso fontes futuras de ameaças emergentes.

O Webroot disponibiliza mais de 80 categorias de URL aos MSPs, para que possam adaptar eficazmente as políticas aos seus clientes. Ao utilizar a inteligência e serviços do Webroot para detetar e bloquear automaticamente os sites maliciosos e filtrar sites indesejados, pode reduzir drasticamente o número de ameaças de malware que infectam os endpoints.

Webroot SecureAnywhere® DNS Protection



Conclusão

As ameaças são cada vez mais sofisticadas e evoluídas e apenas uma estratégia de cibersegurança em camadas consegue garantir a segurança dos endpoints.

Ao utilizar uma solução baseada em cloud que estenda a proteção dos endpoints à network, os MSPs podem assegurar que a maioria das ameaças da internet são bloqueadas antes de entrarem nos endpoints dos clientes.

Com proteção DNS e endpoint para os dispositivos ligados à rede, os MSPs conseguem disponibilizar uma segurança potente e eficaz aos seus clientes, que não só é fácil de gerir, como tem custos reduzidos.

Desde 1997 que o Webroot disponibiliza globalmente as suas soluções de segurança. Qualquer que seja a solução ou serviço, os clientes Webroot contam com mais de 20 anos de experiência em cibersegurança e inteligência de ameaças.