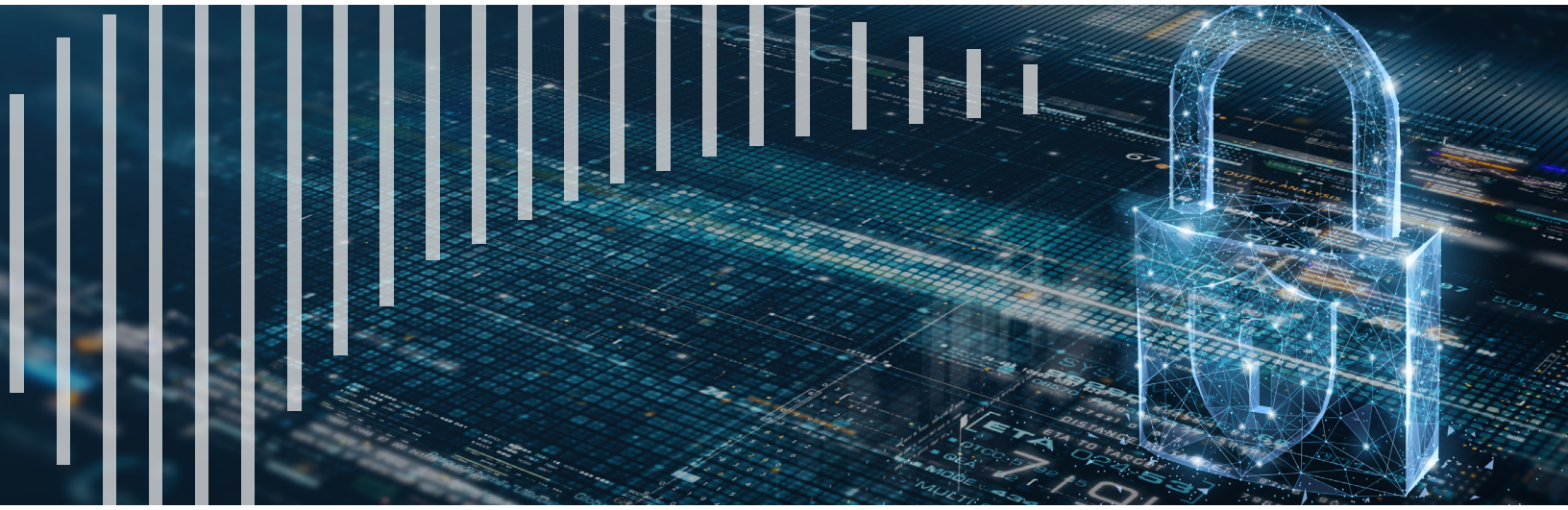
SONICWALL®



RESUMO EXECUTIVO

Ameaças em evolução – Estratégias em evolução

Introdução

O panorama da segurança cibernética em constante evolução está mudando rapidamente e as empresas precisam evoluir com ele.

A realidade da TI distribuída, expandindo-se drasticamente, está criando uma explosão sem precedentes de pontos de exposição para cibercriminosos e autores de ameaças sofisticados explorarem.

Com ambientes híbridos e inteiramente remotos se tornando cada vez mais comuns, os vetores de ataques cibernéticos também estão se ampliando cada vez mais pelo fluxo de novos pontos de exposição. As ameaças comuns e os ataques em múltiplos estágios estão se tornando cada vez mais difíceis de se detectar. Muitas organizações estão em busca de meios para reforçar sua segurança cibernética e ficar à frente dos malfeitores. Existem várias estratégias e tecnologias que as empresas podem aproveitar para obter uma postura de segurança mais forte para proteger sua organização.

Implemente a autenticação multifatorial

A autenticação multifatorial (*Multi Factor Authentication* – MFA) é absolutamente indispensável, tanto para uso pessoal quanto empresarial. A MFA atua como uma barreira adicional entre as redes e os criminosos cibernéticos. A habilitação da MFA pode tornar os ataques mais desafiadores e até mesmo proibitivos para os autores das ameaças em termos de custos. A MFA pode impedir ataques comuns, como os de phishing, key loggers, força bruta e ataques man-in-the-middle (MITM). Existem vários tipos de MFA:

- Baseado em dispositivo pessoal: Pode ser algo como uma mensagem de texto ou um aplicativo autenticador
- Baseado em hardware: utiliza uma peça de hardware, como um token USB, Smart Card ou RSA
- Biológica: pode ser por meio da leitura de impressão digital ou de retina

Assim como ocorre com qualquer tecnologia ou software, as empresas devem conduzir pesquisas e utilizar protocolos de testes adequados para implementar a política de MFA correta para atender as suas necessidades de segurança.

Aprenda a avaliar melhor os riscos

Para desenvolver uma estratégia de segurança eficaz, as empresas devem saber como avaliar riscos com precisão, o que difere de uma organização para a outra. Uma agência governamental pode estar protegendo ativos globais e questões de defesa nacional. Uma empresa de pequeno porte pode estar promovendo a reputação de sua marca e mantendo seus ativos financeiros protegidos. Não importa o tamanho da sua organização, muitos profissionais de segurança buscam o suporte do National Institute of Standards and Technology (NIST) para se certificarem de que estão aplicando as melhores práticas em termos de normas e regulamentos. Embora os frameworks possam estabelecer uma base sólida, as organizações precisam avaliar seus riscos específicos conforme seus ambientes específicos. As empresas devem ter uma perspectiva ampla, juntamente com detalhes diferenciados sobre seu próprio risco. Líderes de diversos departamentos podem apresentar suas perspectivas. Profissionais de segurança cibernética podem descobrir de que outros departamentos têm perspectivas diferentes, porém igualmente válidas, em relação aos riscos. Uma vez que a organização tenha completa compreensão dos riscos em todo seu ecossistema, os profissionais de cibersegurança poderão mapear um roteiro para implementar uma postura de segurança mais forte.

Lide com a lacuna de habilidades

As empresas precisam de profissionais qualificados para defenderem a infraestrutura da organização contra ataques cibernéticos. À medida que a complexidade da rede aumenta, a demanda por profissionais de suporte com know-how sólido

aumenta na mesma proporção. A maioria das organizações descobre que precisa de pessoal altamente qualificado para proteger o hardware, o software e as redes da empresa com eficácia contra os criminosos cibernéticos. Atrair os melhores talentos é um imperativo dos negócios, mas muitas organizações podem enfrentar desafios para formar a equipe. Contratar e reter profissionais de segurança cibernética provou ser uma tarefa assustadora. A SonicWall tem uma grande rede de parceiros, que pode ser utilizada para ajudar empresas de todos os portes a atingirem suas metas e objetivos de segurança.

Escolha a tecnologia certa

Os meios de defesa e segurança avançaram, o que aumentou os recursos das equipes de gerenciamento de TI para proteger seus ativos e manter as redes seguras. Uma estratégia sólida inclui a proteção em múltiplas camadas e cobertura perfeita em todas as superfícies de ataque.

Os autores das ameaças estão tentando atacar a sua organização utilizando uma variedade de aplicativos, dispositivos, redes e infraestruturas cada vez maior. Eles estão atacando com tudo, desde o phishing e variantes de malware nunca vistas antes a ataques de ransomware e em canais secundários, IoT e muito mais – todos os quais podem ser especialmente difíceis de detectar.

A SonicWall ajuda você a eliminar pontos cegos e assegurar a presença de uma força de trabalho "sem limites", em todos os ambientes. Você pode ver tudo, em todos os lugares, e agir rápido nos eventos que importam.

Nosso Capture Security Center elimina a visibilidade em silos. Utilizando um painel de controle único, você pode ver cada uma das superfícies de ataque nas diversas infraestruturas de TI (on-premises, nuvem, endpoints e Secure Network as a Service).

A visibilidade em tempo real e 24 horas por dia revela vulnerabilidades no panorama geral, no momento em que ocorrem, sempre sabendo quais são e o que estão tentando violar. As medições de riscos personalizadas minimizam ainda mais a exposição e priorizam as ações conforme o perfil de risco, enquanto análises acionáveis e relatórios aceleram o tempo de resposta e ajudam a modelar sua estratégia.

A inspeção profunda de memória em tempo real (*Real-Time Deep Memory Inspection™* – RTDMI) patenteada da SonicWall bloqueia ameaças desconhecidas, de dia zero, no gateway – mesmo as que se ocultam por criptografia e as que não apresentam um comportamento doloso. A tecnologia foi desenvolvida para se compreender como os autores das ameaças estão atuando. As ameaças de dia zero não têm uma assinatura de ataque até serem utilizadas pela primeira vez, o que propicia a vulnerabilidade das empresas. O RTDMI detecta essas ameaças e proporciona um nível de visibilidade que permite que você veja essas mudanças no comportamento dos criminosos.

Espere mais dos fornecedores

As organizações precisam saber que seus fornecedores estão adotando medidas de segurança adequadas ao desenvolverem seus produtos. O ideal é que os fornecedores tenham sistemas instalados, como por exemplo, para análise de composição de software e testes estáticos de segurança de aplicativos. É imprescindível ter visibilidade quanto ao processo de desenvolvimento para compreender sua exposição aos riscos e a múltiplas vulnerabilidades. Os autores das ameaças sabem que o perímetro será o ponto mais difícil de acessar na organização. Eles buscam vulnerabilidades em toda a organização – incluindo softwares e hardwares de terceiros. As empresas podem criar questionários de fornecedores que avaliem os padrões que os fornecedores devem atender para consideração. A triagem entre diversos fornecedores, por meio de questionários, fornece uma ampla gama de dados para decidir que fornecedores se enquadram melhor à sua empresa. A exigência de fornecedores



mais qualificados pode ajudar as organizações a fortalecerem sua postura global de segurança cibernética.

Conclusão

Os autores das ameaças estão mudando constantemente seus planos de ataque, para se infiltrar em empresas e causar o máximo de estrago possível. Em um mundo em que os criminosos cibernéticos estão constantemente mudando seus métodos de ataque para pegarem as organizações desprevenidas, essas mesmas organizações podem implementar estratégias que as manterão um passo à frente.

- Implemente a autenticação multifatorial para dificultar a infiltração dos agentes de ameaças nas redes.
- Desenvolva estratégias de avaliação de riscos melhores para se certificar de que a empresa está protegida em todos os possíveis pontos de entrada.
- Contrate e treine profissionais altamente qualificados para otimizar e manter todos os sistemas de segurança.
- Escolha a melhor tecnologia para todas as redes, endpoints e pontos de acesso, mantendo dados e usuários protegidos.
- Defina requisitos rigorosos para os fornecedores, de forma a assegurar que a empresa não esteja importando vulnerabilidades de hardwares e softwares de terceiros.

Finalmente, é responsabilidade de cada organização determinar as estratégias de segurança cibernética que funcionam melhor em seu ambiente. Para saber mais sobre como desenvolver, escalonar e gerenciar a segurança em ambientes em nuvens, híbridos e tradicionais, entre em contato com um Especialista em segurança da SonicWall hoje mesmo.



Sobre a SonicWall

A SonicWall fornece segurança cibernética sem limites na era da hiperdistribuição, em uma realidade de trabalho onde todos estão remotos, móveis e inseguros. Ao conhecer o desconhecido, oferecer visibilidade em tempo real e possibilitar economia disruptiva, a SonicWall preenche as lacunas de cibersegurança para grandes empresas, governos e PMEs em todo o mundo. Para obter mais informações, visite www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consulte nosso site na internet para obter informações adicionais.
www.sonicwall.com

© 2023 SonicWall Inc. TODOS OS DIREITOS RESERVADOS.
SonicWall é uma marca registrada da SonicWall Inc. e/ou de suas afiliadas nos EUA e/ou em outros países. Todas as demais marcas e marcas registradas são de propriedade dos respectivos titulares. As informações deste documento foram fornecidas em relação aos produtos da SonicWall Inc. e/ou de suas afiliadas. Nenhuma licença, expressa ou implícita, por preclusão ou de qualquer espécie, para qualquer direito de propriedade intelectual será concedida por meio deste documento ou em relação à venda de produtos da SonicWall. Salvo na forma estabelecida nos termos e condições, conforme especificado no contrato de licenciamento deste produto, a SonicWall e/ou suas afiliadas presumem isenção de responsabilidade, qualquer que seja, e de qualquer garantia expressa, implícita ou prevista em lei relacionada a seus produtos, incluindo, entre outras, a garantia implícita de comerciabilidade, adequação a um objetivo específico ou não violação. Em hipótese alguma, a SonicWall e/ou suas afiliadas se responsabilizam por qualquer tipo de dano direto, indireto, consequencial, cominatório, especial ou eventual (incluindo, entre outros, danos por lucros cessantes, interrupção de negócios ou perda de informações) decorrentes da utilização ou da incapacidade de utilizar este documento, mesmo se a SonicWall e/ou suas afiliadas foram orientadas da possibilidade de ocorrência de tais danos. A SonicWall e/ou suas afiliadas não fazem qualquer declaração nem oferecem garantias em relação à precisão ou integridade do conteúdo deste documento, e reservam para si o direito de realizar alterações nas especificações e descrições de produtos a qualquer momento e sem aviso prévio. A SonicWall Inc. e/ou suas afiliadas não assumem qualquer compromisso pela atualização das informações contidas neste documento.

ExecBrief-EvolvedThreats_EvolvedStrategies-A4-JK-7925