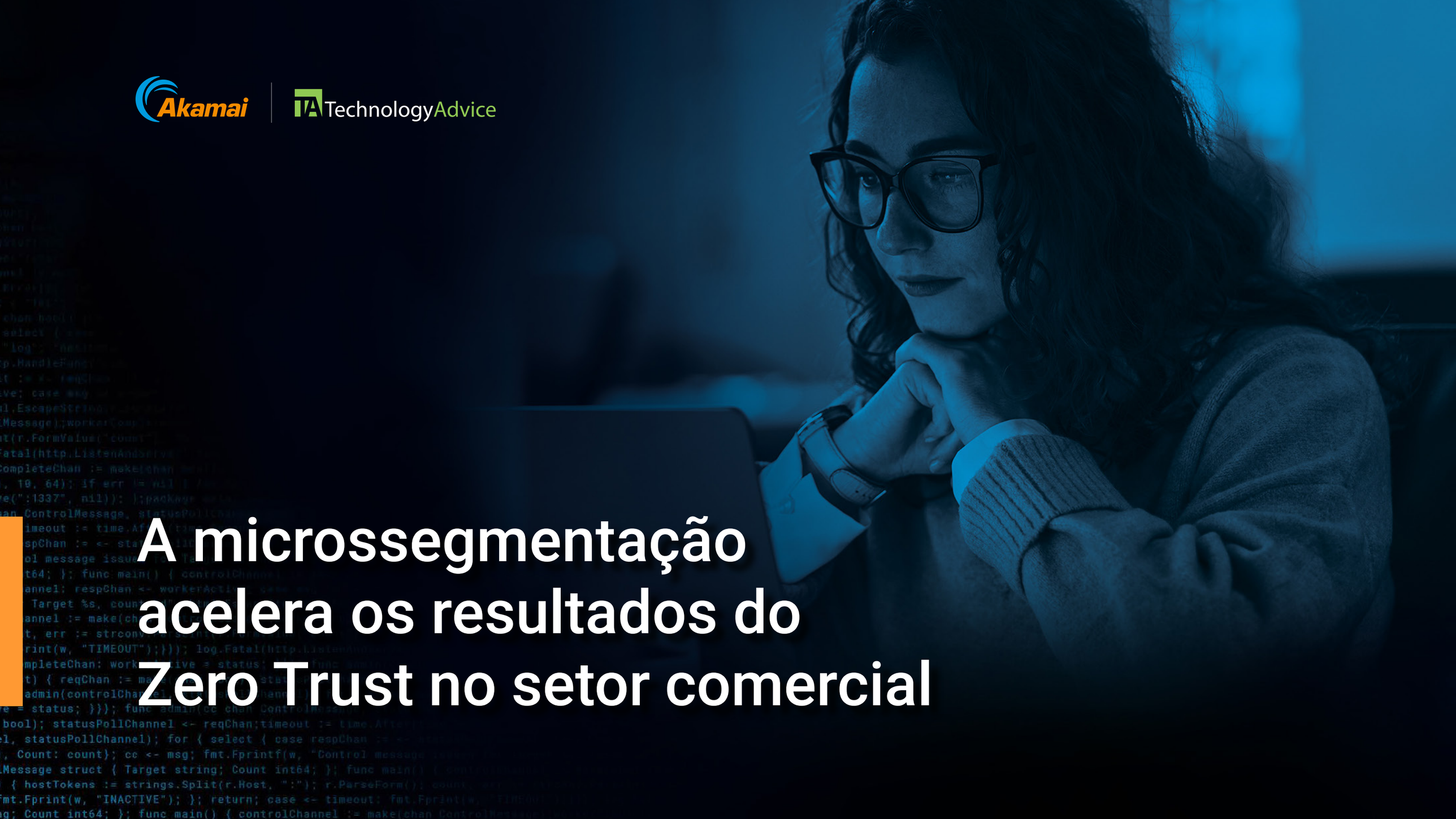


A microssegmentação acelera os resultados do Zero Trust no setor comercial

Organizações de comércio nos setores de varejo, viagens e hospitalidade são alvos atraentes para cibercriminosos. Gangues de ransomware e fraudadores tentam monetizar dados financeiros ou confidenciais de empresas. De acordo com o Relatório de informações do setor RH-ISAC, os tipos mais comuns de informações visadas para roubo incluem informações de cartão de crédito e de pagamento, informações de identificação pessoal (PII) de programas de recompensa ou fidelidade e propriedade intelectual.

Já dentro da linha de visão de um invasor, essas organizações e suas equipes de segurança devem lidar com muitos pontos de invasão em potencial na rede para que os agentes de ameaça implantem ransomware e outros tipos de malware. Todas as organizações enfrentam problemas de e-mails de phishing, credenciais de VPN roubadas e explorações de "dia zero", mas muitas empresas de comércio precisam gerenciar riscos adicionais que são introduzidos por quiosques, dispositivos de Internet das coisas, tablets na loja, terminais de PDV, Wi-Fi para convidados e outros. Adicionando complexidade, cada local de varejo, que deve estar aberto ao público para fazer negócios, expõe uma empresa a uma superfície de ataque físico e a uma grande variedade de outras ameaças.

Dados lucrativos e inúmeros vetores de ataque aumentam as apostas dos defensores corporativos na correção da principal causa de acidentes, o erro humano, que representa 82% dos incidentes de segurança. O aumento das análises regulatórias do setor de cartões de pagamento (PCI) ou das regulamentações governamentais (GDPR, SEC etc.) aumenta a pressão e consome ainda mais os recursos e orçamentos de segurança de TI já sobrecarregados.

Embora a eliminação de todos os riscos seja impossível, as organizações de comércio de hoje devem adotar uma mentalidade de "violação presumida" para detectar e interromper rapidamente a disseminação de uma infecção inevitável ou o contorno das defesas do perímetro. Com as soluções de segmentação Zero Trust da Akamai, as empresas de comércio protegem seus aplicativos, servidores e ambientes de rede com mais rapidez e facilidade, além de evitar tanto a criptografia prejudicial quanto a exfiltração de dados confidenciais.

A microssegmentação, um recurso mais bem desenvolvido por uma abordagem definida por software, fornece uma base para estruturas de segurança Zero Trust que oferecem três recursos principais para organizações de comércio. Primeiro, a microssegmentação limita naturalmente as consequências potenciais de uma infecção por ransomware, bloqueando o movimento lateral. Em seguida, ela pode ajudar a reduzir o custo de alcançar e manter a conformidade com PCI. Por fim, a microssegmentação permite a visibilidade granular e a cobertura necessárias para proteger ecossistemas modernos, porém mais complexos, em ambientes híbridos, de várias nuvens e de microsserviços, bem como na infraestrutura legada.

Limite possíveis consequências do ransomware

Um clique em um link de phishing de e-mail, configurações incorretas de segurança, portas RDP abertas ou credenciais comprometidas regularmente dão abertura para que os invasores comecem a explorar a rede em busca das preciosidades de sua organização enquanto se preparam para executar um ataque de ransomware. As empresas vítimas de um evento bem-sucedido de criptografia em massa (e possível dupla extorsão por meio da exfiltração de dados) sofrem vários níveis de perda financeira e de danos aos negócios.

Perdas diretas nos negócios podem ocorrer imediatamente, pois os pedidos online e as operações da loja diminuem ou desaceleram até serem interrompidos, de forma que os clientes não conseguem mais comprar itens ou fazer reservas em hotéis ou companhias aéreas. As operações de comércio eletrônico podem não ser capazes de processar, cumprir ou enviar pedidos existentes, pois sistemas e servidores críticos ficam inacessíveis ou offline na tentativa de limitar a propagação de um ataque.

Perdas indiretas nos negócios começam com constrangimento público e danos à reputação da marca se dados confidenciais da empresa ou do cliente forem comprometidos. Como tática favorita, as gangues de ransomware publicam ataques e vazam dados em websites do tipo "name and shame" (nomeie e envergonhe) para provar e extorquir ainda mais vítimas e adicionar pressão para receberem pagamento. Os requisitos recentes da SEC também forçam as organizações a notificar a SEC dentro de quatro dias sobre impactos materiais relativos aos negócios, o que alimenta as manchetes e causa danos à reputação.

Os custos de recuperação de despesas legais, resposta a incidentes, perícia forense de dados e correção de violações diretamente relacionados à recuperação de ransomware serão altos, pois consultores e equipes de TI trabalharão para recuperar dados, restaurar backups e colocar os sistemas novamente online. E essas despesas podem ainda ser excedidas por custos de litígio ou penalidades e multas regulatórias originadas pela violação de informações confidenciais. Os prêmios de seguro cibernético podem aumentar drasticamente, os pagamentos de reivindicações por prejuízos causados por ransomware podem ser negados ou a cobertura pode ser totalmente retirada.

Há muita coisa em risco e não surpreende que os ataques de ransomware tenham sido citados como a principal preocupação de risco dos CISOs de varejo e hospitalidade para 2024, e que os líderes de segurança estejam dispostos a investir em controles que ajudem a reduzir os riscos depois que os invasores tiverem estabelecido uma posição. Mas, para que o ransomware se espalhe, os invasores devem ser capazes de girar e de se mover lateralmente depois de terem conseguido acesso inicial para obter o máximo impacto. O Relatório de Defesa Digital da Microsoft de 2022 aponta que 93% dos incidentes de ransomware resultaram de controles de movimento lateral inadequados, que permitiram que os agentes de ameaça bloqueassem aplicativos e infraestrutura críticos, e que o tempo médio para um invasor começar a se mover lateralmente de um ponto de extremidade dentro da rede corporativa é de apenas uma hora e 42 minutos.

Os dados recentes do Estado de segmentação da Akamai mostram que as organizações de comércio eletrônico relataram o maior número de ataques de ransomware nos últimos 12 meses em comparação com outros setores da indústria. É por isso que os CISOs e os especialistas em segurança estão recorrendo a ferramentas de segurança baseadas em Zero Trust, como a microssegmentação, para reduzir o risco de uma infeção por ransomware bem-sucedida, minimizar as superfícies de ataque e "romper" a cadeia de destruição de ransomware.

Ao detectar e bloquear a exploração por meio de movimentos laterais, os invasores terão dificuldade em acessar os ativos de TI necessários para escalar privilégios, localizar informações confidenciais e propagar ataques de ransomware em larga escala. Ao aplicar princípios de acesso de privilégio mínimo a cargas de trabalho críticas em toda a infraestrutura de comércio, a solução de microssegmentação reconhecida por analistas da Akamai permite uma visibilidade profunda dos fluxos de dados leste-oeste de aplicativos e cargas de trabalho, e proteção granular por meio de políticas definidas por software para restringir o movimento lateral e interromper os agentes de ameaça em seus caminhos.

Até mesmo as principais empresas de seguro cibernético entendem o valor da microssegmentação. Com ransomware impulsionando as compras e o aumento de sinistros, muitas seguradoras foram forçadas a aumentar os requisitos de controle de segurança e o processo de análise, aumentar os prêmios, às vezes até 96% em relação ao ano anterior e reduzir os limites de cobertura de pagamento de resgate para compensar perdas significativas. Algumas empresas estão até mesmo sendo precificadas fora do mercado de seguro cibernético ou não conseguindo realizar cobertura total. Embora o seguro cibernético sozinho não impeça uma invasão prejudicial e consequências financeiras, existem controles de segurança, como a microssegmentação, que permitem que as organizações atendam mais facilmente aos mais recentes requisitos de subscrição.

"Com um único agente em uma máquina, resolvemos definitivamente o problema de um ataque de ponto de extremidade por movimentação lateral."

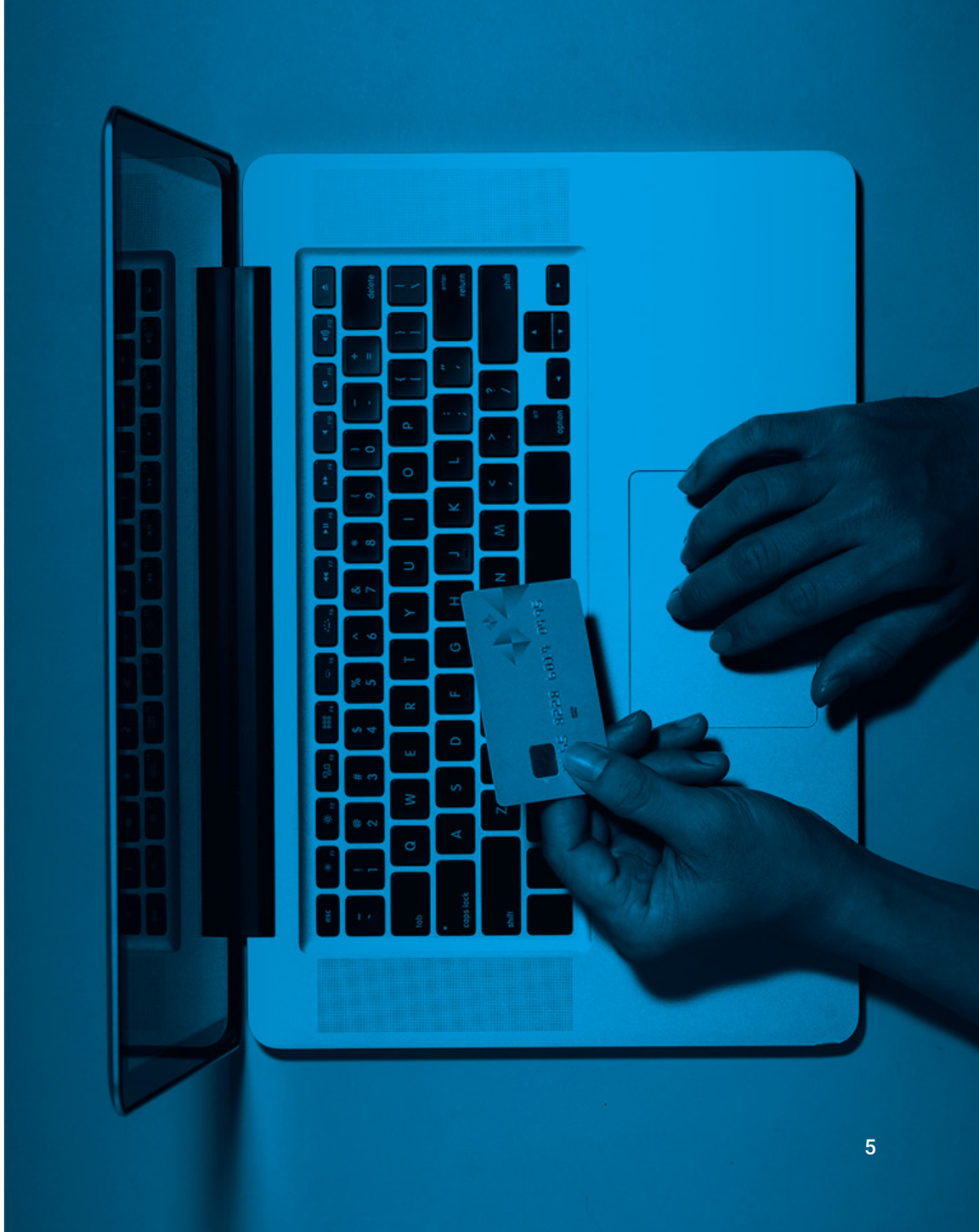
Arquiteto de infraestrutura,
Varejo global e fabricante de bens de consumo

Reduzir o escopo das auditorias de conformidade com PCI

Como as organizações de comércio eletrônico bem sabem, alcançar e manter as contas de conformidade com o PCI representa uma parte considerável dos orçamentos anuais de governança, risco e conformidade, e pode sobrecarregar significativamente os FTEs e os recursos de segurança. O PCI DSS (Padrão de segurança de dados do PCI) requer auditorias contínuas de políticas e controles de segurança para proteger o ambiente de dados do titular do cartão (CDE). O escopo do PCI, que se refere à identificação de pessoas, processos e tecnologias que interagem com a segurança dos dados do titular do cartão ou que poderiam de alguma forma afetá-la, também pode aumentar drasticamente os custos associados à realização de uma auditoria de PCI.

Embora a segmentação de rede não seja um requisito oficial do PCI DSS, as organizações comerciais vêm há anos usando métodos tradicionais de segmentação de rede, como VLANs, ACLs e firewalls internos, para ajudar a reduzir o escopo, o custo, o risco e a dificuldade de manter a conformidade. No entanto, à medida que os ambientes de TI das empresas modernas de varejo se tornaram mais dinâmicos em arquiteturas híbridas, de várias nuvens e de microsserviços, as tecnologias e técnicas de segmentação legadas não conseguem acompanhar o ritmo, gerando sobrecarga operacional, complexidade e tempo de inatividade de aplicativos, bem como brechas de segurança.

Isso ocorre porque os métodos de segmentação legados são difíceis de gerenciar e de manter, consumindo recursos para garantir que sistemas, redes e aplicativos dentro dos limites do CDE estejam protegidos e controlados adequadamente. À medida que as organizações operam do data center e da nuvem aos ativos baseados em contêiner, muitas não têm grande visibilidade dos fluxos de comunicação de aplicativos e sistemas e têm dificuldade para manter os padrões de configuração de firewall necessários para o PCI.



Isso leva a práticas de segmentação ruins que podem criar brechas de segurança e resultar em uma falha na auditoria do PCI. É por isso que as organizações de comércio estão recorrendo à segmentação definida por software para impor mais facilmente a separação entre o CDE e os sistemas fora do escopo nas infraestruturas, reduzir o escopo de uma auditoria do PCI e acelerar a conformidade, possibilitando a segmentação e a imposição até a Camada 7 de processo, que é muito além do que as ferramentas legadas podem suportar. O agente leve da Akamai não requer firewall, alterações de rede ou reinicializações para servidores e opera independentemente da infraestrutura subjacente. Isso possibilita que não haja tempo de inatividade do aplicativo e oferece a capacidade de evitar alterações de controle ou janelas de manutenção.

Como a segmentação definida por software dissocia a segurança da infraestrutura subjacente e dos sistemas operacionais, a segmentação pode ser realizada independentemente sem mexer na rede ou no aplicativo. Ao adotar essa abordagem, as organizações de comércio alcançam visibilidade granular de rede e ativos nos ambientes, com uma solução que atua como um firewall distribuído de inspeção dinâmico, para obter cobertura completa. E, com menos esforço e recursos necessários para implantar e gerenciar, combinados com uma melhoria de cerca de 95% na produtividade do SecOps, as organizações podem adotar uma postura de segurança mais forte e, ao mesmo tempo, evitar as muitas dores de cabeça causadas pela conformidade com o PCI. Como bônus adicional, nossa solução permite que as organizações de comércio aproveitem as visualizações históricas e em tempo real da rede para validar a conformidade durante as auditorias.

> “A segmentação definida por software nos permitiu criar e aplicar políticas de segmentação no nível dos processos, melhorando significativamente nossa postura de segurança e a capacidade de atender aos requisitos técnicos do PCI DSS.”
>
> Engenheiro sênior de infraestrutura, The Honey Baked Ham Company

Ganhe visibilidade e cobertura em toda a Internet das coisas até a infraestrutura legada

Desde a interrupção da disseminação do ransomware até o gerenciamento dos controles de segurança de conformidade com o PCI, as organizações de comércio também enfrentam a complexidade adicional de proteger locais físicos, como lojas, instalações de produção e depósitos de distribuição. Para as companhias aéreas, os sensores e dispositivos da Internet das coisas possibilitam o monitoramento em tempo real e a manutenção preditiva dos sistemas de aeronaves para melhorar o desempenho e a segurança. E organizações de hospitalidade implantam dispositivos acionados pela Internet das coisas para possibilitar quartos de hotel inteligentes projetados para melhorar a experiência do cliente e a eficiência operacional.

É claro que muitos desses locais e ambientes contêm uma infinidade de ativos de Internet das coisas (IoT) ou de tecnologia operacional (TO) que não podem executar agentes de segurança baseados em host, tornando-os ainda mais propensos a vulnerabilidades de hardware e software. Uma pesquisa da Forrester de 2023 sobre o estado da segurança da Internet das coisas indicou que 33% dos líderes globais seniores de segurança citaram os dispositivos de Internet das coisas como o alvo número um para ataques cibernéticos externos. Portanto, as organizações precisam implantar uma solução de segmentação com funcionalidade sem agente que possa proteger ambientes de IoT e de TO e minimizar o risco de um agente de ameaças explorar uma vulnerabilidade de dispositivo na tentativa de obter acesso à infraestrutura de TI mais ampla.

Esse tipo de solução deve ser capaz de monitorar continuamente dispositivos recém-conectados e bloquear automaticamente a comunicação de dispositivos não sancionados com a rede. Por meio da impressão digital integrada do dispositivo, a solução da Akamai detecta e classifica automaticamente os dispositivos conectados em grupos lógicos que formam a base de políticas de segurança escaláveis e abstratas. As políticas de segmentação podem ser criadas para dispositivos de IoT e TO por meio de uma interface unificada e, como outras políticas, elas seguirão o dispositivo com impressões digitais independentemente de onde estejam localizados (mesmo quando os dispositivos estão em roaming para novos locais de rede) ou de quantos existirem no ambiente.

As políticas baseadas em Zero Trust são impostas por ACLs de switches de rede sem precisar de um agente, eliminando as lacunas de imposição que podem criar riscos em implantações de IoT e de TO. Estabelecer esses limites seguros ainda permite conexões necessárias com sistemas de gerenciamento de TI, servidores de atualização dedicados e servidores de registro para reduzir o atrito com a segurança. Nossa solução permite que você descubra, visualize e mapeie todos os sistemas de IoT e TO juntamente com sua infraestrutura de TI para ter uma visão única dos ativos da sua empresa.

Além de proteger os ativos de Internet das coisas/TO e outros pontos de extremidades isolados, muitas organizações de varejo dependem notoriamente de sistemas, servidores e aplicativos executados em sistemas operacionais e infraestrutura legados ou que não possuem mais suporte que não podem ser corrigidos, criando um risco significativo. Muitos desses servidores legados não podem ser removidos porque ainda estão gerando receita para a organização ou servem como a espinha dorsal da empresa, especialmente para empresas de comércio eletrônico que não foram desenvolvidas na nuvem. Com a mais ampla cobertura e compatibilidade líderes do setor, os agentes da Akamai são executados em sistemas operacionais modernos e legados, fornecendo visibilidade total dos fluxos de rede até os processos individuais e níveis de serviço para sistemas operacionais Windows e Linux, juntamente com cobertura para pontos de extremidade MacOS.

Outras soluções fornecem apenas visibilidade parcial para sistemas operacionais legados, sem óptica para sistemas Microsoft Windows anteriores ao Windows Server 2008 R2. Isso ocorre porque o agente das soluções tradicionais de microssegmentação depende de um firewall do Windows para aplicar políticas, o que só estava disponível em sistemas posteriores a 2002. Os agentes para sistemas Linux são compatíveis apenas com a visibilidade de Camada 4, sem regras de nível de processo da Camada 7 para ambientes Linux, e dependem de iptables para aplicar políticas. A funcionalidade do Akamai Guardicore Segmentation é compatível com todos os sistemas operacionais Windows e Linux, novos e legados, pois nossa solução não depende da infraestrutura subjacente.

Simples, rápido, intuitivo e mais seguro

Da sede à loja de varejo e do data center à nuvem e além, a microssegmentação é fundamental para a adoção do Zero Trust para assegurar e proteger ativos de TI críticos.

A simplicidade do Akamai Guardicore Segmentation reduz drasticamente o tempo e o nível de esforço para implantação e aplicação, monitoramento e resposta a incidentes em comparação com métodos de segmentação de rede tradicionais mais lentos. Qualquer alteração na política pode ser implementada rapidamente e não exigirá alterações complexas na rede, que podem ser críticas durante temporadas de pico de vendas, promoções, lançamentos de produtos ou outros eventos de mais alta visibilidade.

Conclusão: assim como você não pediria a seus clientes, convidados ou passageiros para escolher entre qualidade e segurança, uma boa solução de microssegmentação não pedirá que você escolha entre segurança e agilidade. É hora de parar de segmentar da forma mais difícil.

Quer saber mais?

Descubra como reduzir sua superfície de ataque, proteger aplicativos críticos e simplificar a conformidade com o Akamai Guardicore Segmentation, parte do portfólio Zero Trust da Akamai.

Saiba mais

TechnologyAdvice | Akamai

A Akamai protege a experiência dos seus clientes, sua força de trabalho, seus sistemas e seus dados ajudando a integrar a segurança a tudo o que você cria, em qualquer lugar que você cria e entrega. A visibilidade da nossa plataforma em relação às ameaças globais nos ajuda a adaptar e desenvolver sua postura de segurança para permitir Zero Trust, interromper ransomware, proteger aplicações e APIs ou combater ataques DDoS, dando a você a confiança para inovar, expandir e transformar continuamente o que é possível. Saiba mais sobre as soluções de computação em nuvem, segurança e entrega de conteúdo da Akamai em akamai.com e akamai.com/blog, ou siga a Akamai Technologies no X, antigo Twitter e no LinkedIn.