A segurança começa na borda:

Guia de segurança do comprador de 2019

A segurança é a base da inovação para os negócios digitais.

Trata-se de uma alegação ousada; uma que nem sempre foi aceita como verdade. Num passado não tão distante, a segurança digital era vista como uma central de custos. Esses dias estão no passado.

A segurança é essencial para o sucesso de qualquer negócio digital. No entanto, se há algo com o qual você sempre pode contar, é que as incursões relacionadas à segurança são inevitáveis. E não é novidade para ninguém que essas interrupções podem ter consequências péssimas além do tempo de inatividade. As violações de segurança minam a confiança e prejudicam a reputação.

Resumidamente, não se trata mais de uma opção. Como CIO, CISO ou outro líder de segurança ou TI, você sabe que é sua função ser o agente central que enfatiza a relação entre os negócios e os riscos digitais. É de sua responsabilidade encontrar o talento e a tecnologia para garantir a proteção de seus ativos digitais.

De acordo com o Gartner, até 2020, 100% das grandes empresas deverão relatar seus riscos de cibersegurança e de tecnologia à diretoria pelo menos uma vez ao ano. Em 2018, esse número era de 40%. Seja você líder de uma grande empresa ou de uma empresa menor, parte da sua estratégia contínua de segurança, de gerenciamento de riscos e de conformidade estará fornecendo a solução de segurança mais eficaz para a sua empresa.

Sabemos disso. É mais fácil na teoria do que na prática. Para ajudar, compilamos este guia para que você encontre a solução certa para sua empresa expandir a resiliência, conquistar a confiança e gerar receita.

Líder em segurança, conheça a si próprio.

A pergunta que não quer calar: qual é a melhor solução para mitigar os riscos? Para responder a esta pergunta, você deve primeiro responder a algumas outras: quem somos no nosso setor? Quais são nossos requisitos? Quais são os frutos que queremos ver como resultado desta aquisição? Veja por onde começar:

Avalie seu risco.

Uma boa avaliação de riscos observa rigorosamente a postura de segurança atual de uma organização. Ela primeiro identifica as ameaças potenciais à organização e classifica cada uma delas com base na probabilidade de ocorrência, bem como no possível impacto, caso ocorra.

Após a sinalização de possíveis ameaças, a próxima etapa consiste em identificar as vulnerabilidades, como um servidor da Web que executa um sistema operacional sem patch com falhas de segurança conhecidas ou largura de banda de rede insuficiente para absorver um ataque DDoS. Além disso, conforme as empresas migram aplicações para a nuvem, isso muda a forma como os funcionários as acessam. Não é mais viável fornecer acesso irrestrito com base em um modelo de segurança desatualizado, idealizado em torno da falsa ideia de um perímetro inacessível.

Agora, você deve concentrar seus esforços em áreas em que as ameaças e vulnerabilidades se sobrepõem. Depois, vem uma análise das lacunas. De quais controles precisamos, que ainda não temos, para mitigar essas ameaças?

A segurança não deve atrapalhar os negócios. Pelo contrário, ela deve facilitá-los.

Lembrete: a experiência do usuário e a segurança não precisam estar em conflito.

A segurança não deve atrapalhar os negócios. Pelo contrário, ela deve facilitá-los. Atualmente, não se tolera uma experiência de usuário insatisfatória. Se o seu trabalho é proteger um varejista on-line ou a entrega OTT de uma organização, os usuários finais esperam perfeição, sem tempo de inatividade e sem atrasos.

Contudo, muitas vezes, ao proteger a rede, as experiências do usuário são afetadas de maneiras adversas. Como diz o velho ditado: em um nível fundamental, a experiência e a segurança do usuário estão em conflito. Não precisa ser assim.

As soluções de segurança que introduzem falhas na experiência do usuário são apenas um exemplo. Outras armadilhas incluem segurança que interrompe desnecessariamente as aplicações ou que limitam os desenvolvedores. Alguns provedores de segurança até impedem que as equipes internas implantem suas aplicações no provedor de nuvem de sua escolha. Novamente, não precisa ser assim.

Seu próximo fornecedor de segurança deve atender a esses 4 elementos essenciais.

Depois de responder às perguntas acima e ter uma boa noção de seus objetivos, é hora de focar nos fornecedores em potencial. Nesta fase, concentre-se primeiro nos seguintes elementos críticos que qualquer plataforma de segurança deve oferecer:

A plataforma: o valor de uma plataforma de segurança depende de você e de suas necessidades de negócios. Faça a si mesmo estas perguntas ao determinar os elementos essenciais que uma plataforma deve fornecer para você: o que a plataforma de segurança significa para você como líder de segurança? Quais recursos ela oferece a você? Ela permite que você cresça mais rapidamente? Como ela protege seus ativos? Qual é a facilidade (ou dificuldade) de gerenciamento?

Serviços e suporte: seu próximo fornecedor deve aproveitar os especialistas em segurança altamente treinados que oferecem análises de ameaças e estratégia personalizada. Para muitas organizações, a proteção contra ameaças de segurança amplas e em constante evolução é uma questão que vai além do que apenas tecnologia. Diante dos objetivos de negócios da concorrência e de um orçamento de TI limitado, pode ser que você não tenha tempo, recursos ou equipe de especialistas necessários para fornecer a melhor segurança possível para seus websites, aplicações e APIs. Os serviços de segurança gerenciados podem ajudar a reduzir o tempo de resposta e, ao mesmo tempo, aumentar a qualidade de mitigação ao aproveitar uma abordagem coletiva entre você e o fornecedor.

Conformidade: certifique-se de que qualquer fornecedor que você esteja considerando tenha todas as normas de conformidade apropriadas para o seu setor, incluindo o Regulamento Geral de Proteção de Dados (GDPR) da UE, o Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI DSS), o Ato de Portabilidade e Responsabilidade de Seguros de Saúde de 1996 (HIPAA), o Programa Federal de Gestão de Riscos e Autorizações (FedRAMP), ISO 27002, o Controle da Organização de Serviços (SOC) 2 Tipo II entre outros.

Por fim, a solução cobre todos os requisitos? Existem certas funções que qualquer fornecedor de segurança deve dominar e oferecer para sua conveniência. Estes são os itens essenciais básicos que você deve considerar em seu processo de seleção do fornecedor.

- ❑ Atenuação de DDoS
- ❑ Segurança de aplicações
- ❑ Segurança da API
- ❑ Prevenção contra phishing
- ❑ Proteção contra preenchimento de credenciais
- ❑ Detecção de bots
- ❑ Acesso seguro a aplicações
- ❑ Proteção contra malware

Uma solução de segurança deve proteger seu pessoal e suas aplicações, além de defender contra bots e fraudes.

Quais são os principais benefícios que cada solução deve oferecer?

Uma solução de segurança deve oferecer três principais benefícios à sua organização: **escalonamento, visibilidade e inteligência** - tudo isso enquanto protege seus funcionários e aplicações e defende contra bots e fraudes. Uma nova solução deve ajudá-lo a mudar para um modelo Zero Trust para proteger seu pessoal, a receita e as experiências dos clientes contra bots e fraudes e, talvez o mais importante, proteger aplicações e APIs - os pilares da experiência digital moderna.

Escalabilidade: à medida que os ataques aumentam de tamanho e velocidade, é fundamental que qualquer solução que você esteja considerando possa acompanhar a evolução das ameaças. Em 2018, um ataque DDoS de 1,3 Tbps, feito por reflexão do memcached, ameaçou causar muitos estragos. O ataque recorde foi mais do que o dobro do tamanho do notável ataque de botnet Mirai em 2017.

Estamos vivendo em um mundo onde o tráfego de bots mal-intencionados continuará atingindo níveis sem precedentes. Os hackers da atualidade usam bots para fazer verificações pré-ataque, explorar vulnerabilidades e executar uma série de ataques, como injeção de código, DDoS e truques para adivinhar senhas, contra suas propriedades na Web. Esses bots também cometem fraudes via preenchimento

de credenciais, fazendo e cancelando compras repetidamente, mantendo e/ou consumindo inventário, capturando websites, roubando informações e uma série de outras atividades indesejadas. Nos piores casos, um bot mal-intencionado pode causar interrupções de aplicações e API, causando prejuízos à receita.

O melhor método de remoção de grandes quantidades de tráfego indesejado é eliminar o tráfego na *borda*, antes que ele chegue aos seus websites. No entanto, para complicar o problema, o tráfego de bots legítimo é uma parte necessária da Internet. Proteger-se contra bots mal-intencionados e poder gerenciar o tráfego legítimo de bots é um atributo essencial de qualquer solução a ser considerada.

Há também o problema de **escalonamento para gerenciar aplicações corporativas.** E a manutenção e o suporte de aplicações altamente distribuídas ficam ainda mais difíceis com o aumento das expectativas dos usuários. As aplicações estão onipresentes o tempo todo. Elas são altamente distribuídas entre uma força de trabalho distante e, em alguns casos, pelo mundo todo.

Além disso, as aplicações são cada vez mais arquitetadas e montadas a partir de fontes diferentes: estruturas, scripts, várias fontes de conteúdo e a execução do código em tempo real que acontece a partir de uma infinidade de lugares. Você precisa de uma solução que possa escalonar para atender a essa distribuição.

Visibilidade: se você não tiver visibilidade sobre os ataques, não poderá obter informações úteis sobre como proteger melhor seus clientes em tempo real e mitigar as ameaças no futuro. As plataformas de segurança mais fortes interagem com bilhões de dispositivos e centenas de milhões de endereços IP todos os dias, e sofrem bilhões de ataques DDoS anualmente. A solução escolhida precisa ter esse tipo de alcance para trazer visibilidade do cenário de ameaças existentes.

Uma frase comum a respeito de violações graves é que "os hackers conseguiram trabalhar sem serem detectados por X meses". E "após os bandidos conseguirem invadir, eles eram capazes de circular pela rede sem restrição." Procure uma solução que possa fornecer uma combinação entre registro e controle de acesso mais granular a aplicações, com proteção contra ameaças baseada em DNS. Isso lhe dará mais visibilidade e reduzirá o tempo para detecção das violações.

Além disso, uma solução de segurança deve dar visibilidade após um ataque, além de fornecer suporte em tempo real. Uma central de operações de segurança deve oferecer um único ponto de contato em tempo real para suporte a ataques e resposta a incidentes em tempo real contra uma ampla variedade de ameaças. Após um ataque, ela deve ir além de painéis de controle de nível superior e oferecer visibilidade granular a perícias pós-ataque e análises de causa-raiz.

Talvez seja preciso investigar se uma plataforma em potencial permite ou não gerenciar várias soluções por meio de um único portal unificado para dar visibilidade a ataques e controle de políticas. Ela também deve permitir a integração com a sua ferramenta SIEM (Segurança da informação e gerenciamento de eventos) atual para um maior nível de atenção e visibilidade em todas as suas soluções de segurança.

Inteligência: além da capacidade da rede, sua próxima solução precisa fornecer a experiência necessária para a crescente ameaça de ataques DDoS volumétricos. Uma solução diferenciada deve ser capaz de fornecer mitigação de DDoS em zero segundo por meio de uma central de operações de segurança, com especialistas do setor que fornecem serviços de monitoramento, depuração e mitigação de DDoS contínuos.

Proteger suas aplicações, APIs e usuários requer mais do que apenas ter capacidade, exige inteligência contra ameaças. A inteligência artificial e o aprendizado de máquina desempenham um papel importante na entrega de inteligência, os quais você pode usar para melhorar sua postura de segurança. Procure plataformas com ampla visibilidade da Internet, ótima capacidade de escalonar e distribuição global, combinadas com recursos de ponta em ciência de dados.

Um fornecedor capaz de oferecer tudo isso deve oferecer também proteção adaptável contra ameaças e acesso e inteligência aprofundada contra ameaças, aproveitando mecanismos de aprendizado de máquina completos. A análise estatística, de tendências e de padrões de dados estruturados e não estruturados deve ser feita por pessoas e algoritmos para identificar e mitigar novos vetores de ataque antes que qualquer coisa.

Ao implantar a segurança na borda, você protege seus ativos variáveis que estiverem mais próximos do ataque e aproxima as experiências digitais dos usuários.

8 recursos que sua solução de segurança deve oferecer para sua organização.

Até agora, fornecemos uma estrutura para dar início ao seu processo de seleção de plataforma de segurança e áreas críticas nas quais você deve se concentrar enquanto faz a sua pesquisa. Agora, vamos ao que interessa. Quais são os principais recursos que sua próxima solução de segurança deve oferecer para você?

Manter sua empresa funcionando: o desempenho é fundamental, mas a disponibilidade é essencial. O tempo de inatividade e as interrupções têm um efeito prejudicial sobre a receita, a produtividade e a reputação, ou seja, os motivos pelos quais sua empresa existe. Segurança é inegociável quando se trata de negócios digitais e inovação. Sua próxima solução de segurança deve permitir uma mitigação rápida e precisa. Ela deve ser capaz de identificar e eliminar ameaças. Ponto final.

Proteger suas aplicações e APIs: as APIs são os blocos de construção das aplicações modernas e o tecido conjuntivo entre as empresas que potencializam experiências de usuário modernas e perfeitas. As organizações precisam de centenas de APIs, ampliando a superfície de ataque além dos limites tradicionais. Toda API é um ponto potencial de falha em termos de segurança, estabilidade e escalabilidade. A resposta é um Web Application Firewall (WAF) baseado na nuvem que fornece uma camada de segurança entre as implantações de nuvem e os consumidores que desejam acessar os dados, protegendo websites e APIs contra ataques direcionados oportunistas e persistentes.

Manter um ambiente Zero Trust: você precisa de uma plataforma de segurança que forneça uma estrutura que ofereça aplicações e dados somente a usuários autenticados e autorizados, permita a inspeção em linha e o registro de tráfego, impeça malware e violações baseadas em DNS, proteja os usuários finais contra ataques de phishing, possa identificar e bloquear o tráfego de bots, conectar-se a aplicações de SaaS modernas, bem como a aplicações de data center herdadas, integrar-se perfeitamente a um WAF para mitigar ataques à camada de aplicações e fornecer acesso sem cliente. Tudo isso garantindo que as aplicações sejam confiáveis. Em resumo, você precisa de uma plataforma que se adapte especificamente à sua empresa e que instaure apenas interações permitidas entre seus dados e seus usuários.

Fornecer segurança na borda: ao implantar a segurança na borda, você protege seus ativos variáveis que estiverem mais próximos do ataque e aproxima as experiências digitais dos usuários. Basicamente, você está implantando um único painel de vidro, uma extensão da sua infraestrutura, que fica entre você (seus usuários, suas experiências digitais) e a natureza variável do ambiente digital atual. De certa maneira, é uma questão de topologia física. Num momento em que os usuários esperam experiências digitais perfeitas sob demanda, empurrar as interações para a borda, mais perto da fonte dos dados que estão sendo gerados, não só proporciona uma melhor experiência, como também é a melhor localização para construir proteções entre sua empresa e seus usuários e consumidores de experiências digitais amplamente distribuídos.

Superar ameaças avançadas: algumas ameaças são projetadas especificamente para superar as ferramentas de segurança. Sua nova plataforma de segurança precisa ser capaz de estar um passo à frente e superar essas ameaças avançadas. É fundamental que qualquer fornecedor de segurança sustente sua tecnologia com especialistas em segurança que pesquisem a fundo os métodos dos hackers. As soluções de segurança devem aproveitar a tecnologia e o conhecimento humano para acompanhar ou até mesmo antecipar o próximo ataque de dia zero.

Simplificar seus controles de segurança: sua próxima solução de segurança deve trazer agilidade a você, aproveitando a automação e os scripts (orquestração). Nossa ideia é que a segurança digital é a base da inovação nos negócios e, portanto, do crescimento. Você precisa de uma solução que lhe permita extrair valor mais rapidamente, ajudando a aumentar a eficiência durante a transformação digital.

Fornecer suporte 24 horas por dia, 7 dias por semana: em sua organização, não basta contar exclusivamente com ferramentas anti-DDoS automatizadas ou reservas de largura de banda para detecção e proteção contra DDoS. É melhor poder ter acesso a uma equipe de mitigação especializada 24 horas por dia, 7 dias por semana e 365 dias por ano. Uma central de operações de segurança sempre ativa, com presença global para responder a ataques sempre e onde eles acontecem, juntamente com centros de depuração distribuídos globalmente, garantem uma posição de segurança mais robusta, capaz de rebater até mesmo os maiores e mais sofisticados ataques. A combinação entre pessoal e tecnologia pode fazer a diferença entre mediocridade e excelência. Veja se a sua empresa necessita ou não de serviços gerenciados.

Proteger a sua marca e inspirar a confiança do cliente: essencialmente, a confiança é a força vital de sua empresa. E é o que está em jogo quando é sua responsabilidade proteger sua empresa e reduzir os riscos.

Os líderes de segurança devem ajudar a equipar seus negócios digitais com a mentalidade, os recursos e o planejamento para se recuperar de interrupções inevitáveis. Falhas em qualquer parte do ecossistema podem ter um efeito cascata e prejudicial sobre a empresa. Como a segurança não é mais apenas uma central de custos, você tem a oportunidade de permitir a transformação digital, gerar receita e solidificar você e sua equipe como a base da empresa e da inovação.

A Akamai protege e entrega experiências digitais para as maiores empresas do mundo. A plataforma de borda inteligente da Akamai cerca tudo, da empresa à nuvem, para que os clientes e seus negócios possam ser rápidos, inteligentes e protegidos. As principais marcas mundiais contam com a Akamai para ajudá-las a alcançar a vantagem competitiva por meio de soluções ágeis que estendem a potência de suas arquiteturas multinuvem. A Akamai mantém as decisões, aplicações e experiências mais próximas dos usuários, e os ataques e ameaças cada vez mais distantes. O portfólio de soluções de segurança de borda, desempenho na Web e em dispositivos móveis, acesso corporativo e entrega de vídeo da Akamai conta com um excepcional atendimento ao cliente e monitoramento 24 horas por dia, sete dias por semana, durante todo o ano. Para saber por que as principais marcas mundiais confiam na Akamai, visite www.akamai.com, blogs.akamai.com ou @Akamai no Twitter. Nossas informações de contato globais podem ser encontradas em www.akamai.com/locations. Publicado em 05/19.