O QUE APRENDEMOS SOBRE SEGURANÇA CIBERNÉTICA EM 2017

Quatro lições para ajudar você a moldar sua estratégia no próximo ano

vmware® | intel®

Novas ameaças, novas oportunidades

Para o mundo dos negócios, 2017 foi um ano de grandes mudanças. As organizações começaram a mapear o cenário digital e fazer reivindicações. Ataques mal-intencionados logo surgiram. Apesar do momento propício para novas oportunidades de crescimento e inovação, foi um ano em que líderes de negócios e de TI enfrentaram uma série de ameaças.

O que aprendemos nesse processo? Há grandes aprendizados que podem ajudar aorientar sua estratégia de segurança a partir de 2018:

1. A superfície de ataque continua a crescer
2. Os ataques superam a proteção
3. Novas ameaças exigem a adoção de uma nova abordagem
4. A escassez de pessoal de segurança cibernética eleva o grau de risco

1 A superfície de ataque continua a crescer

Dispositivos, usuários, aplicativos e dados proliferam rapidamente. Apesar dos ganhos para os negócios (em termos de flexibilidade, maior produtividade e incentivo à inovação), isso também abre caminho para invasores mal-intencionados. Assim, os líderes de TI se esforçam para determinar como novas iniciativas e tecnologias podem deixar a empresa exposta. É uma tarefa sem fim.

Não adianta correr atrás das ameaças. São tantas que seria difícil rastreá-las. As organizações de TI precisam adotar uma abordagem proativa que permita estar à frente das ameaças emergentes. Este tipo de abordagem envolve o entendimento profundo sobre as vulnerabilidades específicas de um negócio, aliado ao conhecimento contínuo de tendências relativas a ameaças. Isso permite ajudar as equipes a criarem uma estratégia intuitiva de proteção do data center. Além das ferramentas certas, esta abordagem permite à TI combater ameaças de igual para igual.

Estima-se um crescimento anual de 7,9% no mercado de segurança da informação, chegando a US$ 120,2 bilhões até 2021[1]

1 Gartner, Forecast Analysis: Information Security, Worldwide, 3Q17 Update, dezembro de 2017

2 Os ataques superam a proteção

Apesar do maior investimento em segurança, ainda há muitas violações, e nenhuma empresa ou setor está imune a elas.

O amplo uso da criptografia afeta a detecção de ameaças. E as ameaças avançadas de estados-nações dificultam ainda mais a tarefa de líderes de segurança de proteger a infraestrutura e os dados. Nas organizações modernas, não se trata mais de pensar na probabilidade de violações de segurança, e sim em quando elas vão ocorrer.

Gastar mais não é a solução. Para proteger os dados, os usuários e a marca, você precisará abordar a segurança de outra forma.

+27,4%

Aumento no número médio anual de violações da segurança em 2017[2]

+22,7%

Aumento no custo da segurança cibernética em 2017[2]

2 Accenture Security, 2017 Cost of Cybercrime Study, dezembro de 2017

3 Novas ameaças exigem a adoção de uma nova abordagem

Os data centers, a tecnologia de nuvem, os aplicativos e os dispositivos evoluem. O mesmo ocorre com as ameaças. As soluções de segurança convencionais voltadas para outra era não conseguem dar conta dessas ameaças. Os invasores modernos assumem várias formas e disfarces que não podem ser detectados. Em vez de correr atrás das ameaças, a TI precisa focar em prevenção para lidar com vetores de ameaças e reduzir a superfície de ataque.

Antes, a TI costumava adotar a tática de caça ao mal. Hoje, sabe-se que isso consome a energia da empresa para prevenção de ataques. Ao usar estratégias como privilégio mínimo, a TI pode manter uma postura proativa até mesmo contra ameaças sofisticadas.

O conceito de privilégio mínimo permite que o usuário, dispositivo, processo ou aplicativo acesse as informações necessárias e nada mais. Além disso, os aplicativos são cuidadosamente monitorados no estado pretendido e em estados do tempo de execução, a fim de agilizar a identificação de alterações. Alertas automáticos impedem adulterações e alterações inesperadas.

4 A escassez de pessoal de segurança cibernética eleva o grau de risco

Em 2017, a ISACA lançou um relatório de segurança cibernética indicando que havia uma crise de trabalho em trabalhadores de segurança capacitados. 64% dos líderes de TI e de negócios pesquisados disseram que metade, ou menos, dos candidatos estão qualificados para ocupar um cargo de segurança em aberto. Hoje, o setor reconhece que não há gente suficiente que saiba o que fazer para manter a segurança.[3]

A alta rotatividade em cargos de segurança também é um problema em muitas organizações. Essa rotatividade pode levar a uma perda de conhecimento institucional básico; quando saem de uma empresa, os profissionais levam consigo informações e habilidades valiosas. Na falta deles, outros talvez não consigam propor orçamentos estendidos ou as soluções de segurança necessárias para a organização.

A escassez de talentos coloca a empresa em desvantagem, pois sua capacidade de responder a novos desafios depende de pessoas aptas e dispostas a enfrentar esses desafios. Sem profissionais qualificados para impedir o crescente número de ataques, as organizações se tornam alvos fáceis para ameaças.

Educação contínua e processos estabelecidos, unidos a automação e estruturas, podem ajudar as organizações a reter talentos e reduzir riscos.

3 ISACA, State of Cybersecurity 2017, 2017

A equipe de segurança é pressionada por expectativas às vezes absurdas da organização. Diante da inevitabilidade de uma intrusão, ou buscando maiores desafios, os operadores e líderes de segurança mudam de emprego com grande frequência. Essa rotatividade tem um enorme impacto sobre o conhecimento institucional. Os mais experientes e requisitados assumem funções lucrativas (ou saem quando ocorre uma violação), e não sobra ninguém para defender um maior orçamento para investimento em programas de segurança.[4]

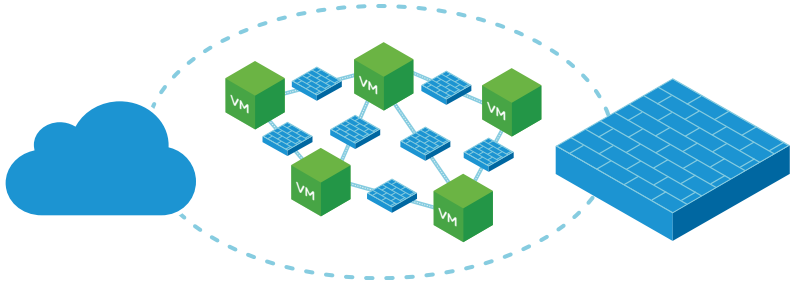
4 Gartner, How to Respond to the 2018 Threat Landscape, novembro de 2017

Adote uma ação estratégica: recomendações da VMware para 2018

Apesar de parecer intimidador, o cenário de ameaças não é invencível. Essas práticas recomendadas de profissionais de segurança da VMware ajudarão você a fortalecer a postura de segurança e manter a organização protegida nos próximos meses e anos.

Dê ênfase à detecção e prevenção

A definição de um comportamento de aplicativo conhecido serve como linha de base para detecção e prevenção de ameaças. Se o comportamento se desviar desta configuração reconhecida, medidas responsivas poderão ser ativadas automaticamente.



Use a segmentação para reduzir a superfície de ataque

Para evitar que as ameaças se espalhem rapidamente, mantenha máquinas virtuais e cargas de trabalho individuais separadas. Ao criar restrições, você pode limitar o alcance de uma ameaça. A microssegmentação, habilitada pela virtualização de redes, impede a propagação lateral e a eficácia de um ataque. Ao impedir que ameaças usem o tráfego leste-oeste, você pode detectar, isolar e eliminar um ataque antes que ele se espalhe.

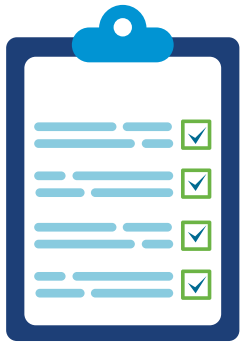
Adote uma ação estratégica: recomendações da VMware para 2018

Use a inteligência contra ameaças

As melhores soluções de inteligência contra ameaças são exclusivas de cada empresa. Não existe uma única abordagem que dê conta de tudo. Uma estratégia personalizada emite um alerta de alta confiança, levando a equipe de TI a responder de forma acionável.

Mantenha a higiene cibernética básica

Aplique patches e fortaleça os sistemas para afastar ameaças. A segurança da informação deve priorizar esforços de aplicação de patches para operações de TI e compartilhar os motivos do patch. Isso ajuda a aumentar a cooperação e reduzir os atritos. Aplique patches sempre que possível e use a detecção em todos os lugares.



Planeje a aquisição de novas tecnologias de segurança

Nem toda solução de segurança funcionará para seus negócios. A TI precisa garantir que novas tecnologias tratem de ameaças específicas nos negócios. Isso pode ser gerenciado com os conjuntos de habilidades das equipes existentes. Se profissionais de segurança não sabem usar uma ferramenta, não vale a pena investir nela.

Mantenha sua empresa segura hoje e sempre

Proteger os dados sempre foi uma parte importante de qualquer negócio. E agora mais do que nunca. O cenário de ameaças continua evoluindo, e a TI deve ser capaz de antecipar ameaças e estar sempre à frente.

A VMware e a Intel transformam a segurança ao oferecer medidas de segurança abrangentes com base em software e hardware em infraestrutura e endpoints de aplicativos, maximizar a visibilidade e o contexto da interação entre usuários e aplicativos, alinhar controles e políticas de segurança aos aplicativos protegidos e permitir a inserção de serviços de segurança adicionais de terceiros para oferecer uma proteção mais inteligente.

COMECE A TRANSFORMAÇÃO DA SEGURANÇA

Saiba mais sobre as soluções VMware >

Junte-se a nós on-line:

vmware® | intel®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel.: +1-877-486-9273 Fax: +1-650-427-5001 www.vmware.com
Rua Surubim, 504 4º andar CEP 04571-050 Cidade Monções – São Paulo – SP Tel.: (11) 5509-7200 www.vmware.com/br