Microsoft

Criar uma empresa resiliente e confiável

O trabalho híbrido veio para ficar. Embora existam novos desafios, também existem novas possibilidades de reinventar a maneira como pensamos sobre segurança. A seguir, conheça alguns conselhos e informações que darão a você, como líder na segurança da sua empresa, mais argumentos para tomar melhores decisões e estimular os clientes a estabelecerem uma relação de confiança.

Tendências e riscos na segurança cibernética

Tudo o que você precisa levar em consideração ao tornar uma decisão sobre a arquitetura de segurança em sua empresa, de acordo com as pesquisas de 2021 Gartner CIO Survey e 2020 Gartner CISO Effectiveness Survey.

1 Malha de cibersegurança

Uma abordagem moderna da arquitetura que permite implantar e distribuir a segurança onde é mais necessário.

2 Painéis cibernéticos inteligentes

Os conselhos estão formando comitês dedicados que se concentram na discussão de questões de segurança cibernética, aumentando o poder de escrutínio e ajudando os CISOs a melhorar sua comunicação e tomada de decisões.

3 Consolidação de fornecedores

78% dos CISOs têm 16 ou mais ferramentas em seu portfólio de provedores de cibersegurança;

12% têm 46 ou mais;

80% das organizações estão interessadas na estratégia de consolidação de fornecedores.

Grandes fornecedores de segurança estão respondendo com produtos mais integrados.

4 Identidades seguras

"Segurança de identidade em primeiro lugar" agora representa a forma como funcionarão todos os profissionais da informação - independentemente de estarem em locais remotos ou no escritório.

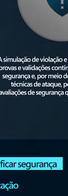
5 Gerenciar identidades de máquina como um recurso de segurança crítico

Conforme o número de dispositivos aumenta, os certificados de máquina garantirão melhor a transformação digital.

6 Trabalho remoto agora é apenas trabalho

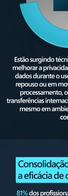
64% dos funcionários agora podem trabalhar em casa, e 0,5 estão trabalhando em casa.

7 Simulação de ofensas e ataques



A simulação de violação e ataque (BAS) oferece provas e validações contínuas dos controles de segurança e, por meio de uma variedade de técnicas de ataque, permite melhores avaliações de segurança quase em tempo real.

8 Técnicas de computador que melhoram a privacidade



Estão surgindo técnicas de computação para melhorar a privacidade (PEC) para proteger os dados durante o uso, em vez de quando em repouso ou em movimento, para permitir o processamento, o compartilhamento, as transferências internacionais e as análises seguras - mesmo em ambientes nos quais não são confiáveis.

Simplificar segurança

Qualificação

Muitas empresas têm arquiteturas de segurança complicadas com uma pilha de soluções de endpoint. Podemos ajudá-lo a fortalecer sua segurança:

- Eliminar silos difíceis de supervisionar
- Automatizar processos manuais intensivos
- Simplificar o gerenciamento com soluções

82% das organizações que consolidam seu portfólio de segurança relatam um risco menor de violação.

Consolidação para alcançar a eficácia de custo

81% dos profissionais de segurança relatam sentir pressão para cortar custos. Ao consolidar suas soluções de segurança, você será capaz de:

- Reduzir os custos de licenciamento substituindo até 40 produtos diferentes
- Reduzir os custos das operações de segurança
- Reduzir os custos de implementação ao aumentar a eficiência da integração e a ganhar acesso de valor mais rápido

Caso de sucesso

O Caribbean Development Bank melhora a segurança e permite o trabalho remoto graças às soluções da Microsoft.

O banco consolida sua transformação digital ao descontinuar várias soluções de terceiros e ao centralizar o gerenciamento de dispositivos em uma plataforma única e fácil de usar. Isso garante o acesso a aplicativos de produtividade com recursos analíticos avançados, bem como recursos de cumprimento normativo que fornecem uma forte proteção da identidade e dos dados.

Seus administradores podem agora adicionar e atribuir aplicativos móveis a grupos de usuários, configurar aplicativos para serem executados com configurações específicas habilitadas e atualizar sistemas e aplicativos - tudo com segurança avançada e automatizada.

> *Assim que começamos a aproveitar as soluções em nuvem, nossa equipe de TI teve tempo para se envolver de forma mais proativa com os usuários empresariais, permitindo que eles se concentrassem em soluções automatizadas e na construção de aplicativos rápidos e fluxos de usar.*
>
> Julio Lima, CIO, Caribbean Development Bank.

> *Ao implementar as soluções de segurança da Microsoft e mover nossas operações para a nuvem, alcançamos um desempenho que, de outra maneira, só seria possível se a grande maioria de nossa equipe estivesse totalmente dedicada ao reconhecimento e prevenção de ameaças*
>
> Angus Aird, Chefe de Prestação de Serviços, Caribbean Development Bank.

Benefícios:

- Maior visibilidade e controle sobre os dados
- Redução de footprint do seu aplicativo em mais de 30%
- Melhora na análise para identificar e combater ameaças cibernéticas em todos os serviços em
- Migração de 90% dos aplicativos antigos do banco para máquinas virtuais no Azure

Um olhar mais amplo

Se você não pode olhar para o seu negócio como um todo, isso abre brechas para vulnerabilidades. Procure soluções que:

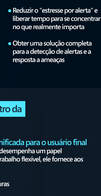
- Dê a você a máxima visibilidade de todo o seu patrimônio digital
- Use inteligência artificial integrada para tornar a detecção de ameaças mais inteligente e rápida
- Reúna dados de todas as fontes

Desenvolver fundações sob o conceito de higiene cibernética

- Mantenha-se atualizado com a clareza dos dados
- Atualizar os patches
- Usar a autenticação multifator (MFA) e o início de sessão único
- Implementar uma abordagem de Zero Trust

Faça uma avaliação Zero Trust para analisar seu cenário de identidade de usuário existente e aprender como implementar uma estratégia Zero Trust eficiente.

Aproveitar a inteligência



Fornece as equipes de segurança melhores ferramentas e treinamento para detectar ameaças e reduzir o risco interno.

- Capacitar a equipe ajuda as pessoas a se concentrarem nos principais incidentes de segurança
- Reduzir o "estresse por alerta" e liberar tempo para se concentrar no que realmente importa
- Obter uma solução completa para a detecção de alertas e a resposta a ameaças

Fazer das pessoas o centro da estratégia cibernética

Oferece uma experiência unificada para o usuário final

Uma vez que o trabalho remoto desempenha um papel fundamental nas estratégias de trabalho flexível, ele fornece aos funcionários:

- Ferramentas familiares e seguras
- Acesso a aplicativos e dados a partir de seus próprios dispositivos
- Segurança fácil de usar com início de sessão único e MFA

Conexão constante

Mantenha contato com parceiros e clientes sem comprometer a segurança. Aplique os recursos de segurança que você usa dentro da sua empresa, como MFA, a todas as identidades externas, como MFA, a todas as identidades externas.

> A temática da cibersegurança deve estar cada vez mais presente nas agendas dos altos executivos e conselhos de administração. Afinal, com o mundo virtual e o real cada vez mais conectado, é essencial tomar medidas para aumentar a resiliência operacional contra os ciberataques. A questão não é se sua empresa será atacada ou não, mas sim o fato de que existirão apenas dois tipos de empresas: as que foram atacadas e sabem que o foram e as que não sabem.
>
> Marcelo Zillo, Consultor Chefe de Segurança, Microsoft América Latina

Investir na criação de equipes diversas

Cultivar uma equipe cibernética diversificada pode gerar inovação. Empresas com visão de futuro buscarão:

- Empregar mais mulheres e pessoas de minoria étnicas
- Crie equipes com uma faixa etária e distribuição geográfica mais ampla
- Eliminando a lacuna de habilidades digitais com melhor treinamento e uma cultura de segurança cuidadosamente desenvolvida

Construir uma organização com a tecnologia mais recente, guiada por uma abordagem centrada nas pessoas e protegida por segurança integrada está inteiramente ao seu alcance.

Microsoft