Repensar a sua estratégia de cibersegurança para o novo mundo

5 passos para proteger a empresa e estar pronto para um futuro flexível

avanade

Repensar a sua estratégia de cibersegurança para o novo mundo

A pandemia de COVID-19 afetou todos os setores, organizações e pessoas. O que compramos, como vivemos e o modo como trabalhamos mudou para sempre e mais depressa do que poderíamos imaginar.

Muitas organizações tiveram de implementar novos modelos operacionais, para algumas desconhecidos, e introduzir rapidamente tecnologias de apoio a este novo ambiente para garantir a continuidade dos negócios.

Muitas organizações estão a repensar o caminho que irão seguir. Para o efeito, recomendamos que se concentre nestas prioridades fundamentais: contenção de custos, capacitação dos seus colaboradores, proteção das operações essenciais do seu negócio, apoio às necessidades dos seus clientes e resposta às mudanças que afetam a seu portefólio de produtos. Criar uma operação segura e resistente é essencial para conduzir estas prioridades

Alterações recentes, como o acréscimo de teletrabalho, significam que as organizações estão a enfrentar desafios de segurança, com uma superfície de ataque mais ampla e uma maior exposição a ameaças. Para muitas, a sua postura de risco alterou-se profundamente. Este é um tempo ideal para repensar a sua estratégia de segurança. Neste guia, delineamos alguns passos essenciais para o ajudar a fazer isso – para que possa proteger as operações fundamentais do seu negócio e permitir que os seus colaboradores trabalhem de forma segura neste novo ambiente.

Os agressores estão a aproveitar a crescente exposição e, de acordo com uma nova investigação da Microsoft, os hackers lançaram ciberataques relacionados com o coronavírus em **241 países** e **territórios**

"... encaramos estes tempos desafiantes como uma oportunidade de repensar a forma como realizamos negócios ... Este processo envolverá a transformação da sua empresa para que tenha uma experiência de cliente ainda melhor e operações ainda mais eficientes."

Centro de Investigação de Sistemas de Informação MIT Sloan
31 de março de 2020

Disrupção global **agrava** desafios de segurança

Nesta nova era, as organizações estão a deparar-se com diversos desafios de segurança:

Engenharia social

Os agressores estão a capitalizar os receios com a crise e estão a usar estratagemas relacionados com a COVID-19 para lançar campanhas de phishing e malware. Este tipo de ataques teve um pico acentuado e é provável que continue.

Teletrabalho (Trabalho remoto)

À medida que o teletrabalho aumentou, também aumentaram os riscos relacionados com a proteção de dispositivos pessoais, palavras-passe fracas, Wi-Fi doméstico com pouca segurança, os routers e os sistemas remotos de patching. Os colaboradores estão ainda a colaborar de diversas formas dentro e fora da organização, usando muitas vezes plataformas suscetíveis. Foram detetadas vulnerabilidades em ferramentas de colaboração que podem ser exploradas, dando origem a más experiências de utilização e preocupações sobre privacidade e confidencialidade. Os responsáveis pela segurança enfrentam também custos acrescidos com TI para apoiar as equipas de trabalho, com uma maior utilização de redes e de infraestruturas.

Falta de acesso seguro

Os métodos de gestão de identidade e de acessos não acompanharam as novas formas de trabalhar, incluindo trabalhadores em teletrabalho, dispositivos múltiplos e a impossibilidade de aceder a aplicações críticas. A quantidade de dados que está a ser partilhada também se multiplicou e, como consequência, muitas organizações estão a interrogar-se se possuem a infraestrutura e gestão de identidade certas para dar aos seus colaboradores um acesso seguro à informação de que necessitam. O teletrabalho e os modelos de negócio à distância tornar-se-ão o novo padrão. Os bens e serviços serão transacionados digitalmente através da economia de API, alargando ainda mais a superfície de potencial ataque e os riscos associados.

Falta de agilidade

A procura sem precedentes de acesso remoto a recursos da empresa colocou pressão adicional sobre os pontos de acesso e os serviços de rede privada virtual (VPN). Muitas organizações não foram capazes de dimensionar com segurança os sistemas e a infraestrutura de VPN existentes, de modo a satisfazer os requisitos evolutivos, o que afeta a experiência do utilizador e a capacidade para trabalhar.

> A **Microsoft** está a rastrear diariamente cerca de **60.000** anexos ou URLs **maliciosos** relacionados com a COVID-19

Navegar pelas vagas da mudança

Prevemos que as organizações passarão por três vagas de mudança. É fundamental que comece a adotar já as medidas de segurança certas para proteger as operações centrais do seu negócio, para que possa criar uma operação resistente e preparada para um futuro flexível.

Responder

Muitas organizações estão a começar a emergir desta primeira fase. Durante este tempo, as organizações têm estado focadas em garantir a continuidade do negócio criando condições para os colaboradores trabalharem e os clientes acederem a bens e serviços, mantendo as suas operações centrais e a cadeia de fornecimento.

Com a alteração para o teletrabalho, é importante compreender como a postura de risco da sua organização mudou.

Restabelecer

Já conseguimos ver muitos dos nossos clientes ir para além da fase de resposta, adotando uma mentalidade de restabelecimento, para gerir um negócio mais leve e ágil durante um período de desaceleração económica. É provável que isto envolva a reconfiguração do portefólio de produtos e a rápida criação de um modelo operacional para apoiar as necessidades do mercado e dos colaboradores.

Durante esta fase, recomendamos que realize uma avaliação de risco completa, para priorizar a forma de tratar os riscos de segurança identificados, começando pelas lacunas de segurança mais imediatas. Além disso, terá de planear uma framework de segurança baseada em arquiteturas de Zero-Trust e redução de custos.

Renovar

Ao longo dos próximos 12 a 18 meses, esperamos que as organizações venham a desviar cada vez mais a sua atenção para o modo como se podem renovar, crescer e posicionar para o futuro. Procurarão reinventar o seu modelo de negócio para gerir oportunidades novas e existentes com uma versão mais forte e resiliente da empresa.

Do ponto de vista da segurança, deverá procurar adaptar-se continuamente a contextos empresariais em mudança e manter-se em situação regular, garantindo que quaisquer alterações de modelos, tecnologia e processos respeitam os requisitos emergentes de compliance e regulamentação. Este seria também um tempo ideal para implementar um novo design de segurança, baseado num roadmap robusto que seja consistente com os requisitos do seu negócio e postura de risco.

5 passos para **repensar** a sua estratégia de segurança

À medida que vai passando por estas três fases, pode ser difícil saber por onde começar para garantir a adoção das medidas necessárias para proteger a sua empresa, agora e no futuro.

A seguir apresentamos cinco passos para o ajudar a começar.

#1. Adotar uma mentalidade e visão **Zero-Trust**

Este conceito está centrado na convicção de que uma organização não deve confiar automaticamente em tudo o que estiver dentro ou fora do seu perímetro – e que tudo tem de ser verificado antes de conceder acesso aos sistemas. A identidade de cada pessoa, conta de administrador, aplicação, bot e processo tem de ser validada e gerida através de um processo de governação.

Recomendamos também que considere ferramentas que tratem dos seus requisitos de governação e administração da identidade (IGA, na sigla em inglês). O acesso a serviços digitais de diversos locais e plataformas alvo deve ser avaliado continuamente para apoiar os objetivos de resiliência e continuidade do negócio.

avanade

Estudo de caso

A segurança liberta todo o potencial do local de trabalho

Desafio: O nosso cliente pretendia construir um local de trabalho preparado para o futuro e introduzir uma experiência de colaborador de vanguarda, com uma base segura.

Solução: Implementamos um local de trabalho moderno e seguro com tecnologia Microsoft 365, dotado de uma vasta gama de soluções, desde serviços de cloud seguros a um local de trabalho móvel e colaboração de primeira linha.

Resultados: A organização já consegue ver um negócio atrativo que resulta do projeto:

- Dois princípios de **segurança** chave – "Identidade como plano de controlo" e "Zero-Trust" – estão plenamente suportados.
- Os colaboradores são mais **produtivos** e podem aproveitar a mesma experiência de local de trabalho através de diversos tipos de dispositivo, de forma remota e segura.
- As plataformas de trabalho sempre verdes ajudaram o cliente a alcançar um tempo de comercialização mais rápido e as TI a garantir **eficiência**.
- A **experiência do colaborador** melhorou bastante, com uma colaboração mais intensa e a capacidade de tomar melhores decisões empresariais.

#2. Realizar uma avaliação do risco completa

Se, tal como muitas organizações, sofreu recentemente uma rápida mudança na arquitetura da sua empresa e a aplicação de novas ferramentas de colaboração e de trabalho, chegou a hora de realizar uma avaliação de risco do seu ambiente.

É difícil avaliar o risco de tudo desde o início, por isso um bom ponto para começar é identificar os ativos mais valiosos e compreender o que quer proteger. A partir daqui, poderá assinalar os riscos chave nesses ativos e lançar um plano tático para os resolver.

avanade

#3. **Priorizar** projetos, orçamentos e recursos de segurança

Compreender os riscos para o seu ecossistema que acabou de ser alterado permitir-lhe-á adotar uma abordagem ponderada e previdente da priorização, dos recursos e do orçamento do projeto de segurança.

Esta é também uma boa altura para rever ou desenvolver uma estrutura formal de governação da segurança para garantir que o seu novo modelo operacional é coerente com a sua nova postura de risco.

Como a maioria das coisas, a segurança não pode ser resolvida injetando capital sobre o problema. Uma abordagem baseada no risco irá ajudá-lo a focar o seu orçamento e recursos. Muitos dos nossos clientes já estão a priorizar a sua despesa em projetos de transformação digital e mitigação de cloud para apoiar o teletrabalho.

A IDC reportou recentemente que esperava recorrer a serviços profissionais e de gestão relacionados com a segurança para se manter sólido enquanto as organizações procuram manter as operações a funcionar durante a crise da COVID-19. Isto realça a importância da segurança como uma prioridade estratégica para as organizações em relação a outras áreas de TI.

A IDC acredita que a COVID-19 irá ajudar a evidenciar a importância de ter em vigor planos de resposta a incidentes e de resiliência para situações de crise.

Impacto da COVID-19 sobre as Projeções de Despesas com Serviços de Segurança da IDC, 2020 [a página da IDC mostra uma data de 13 de abril de 2020

#4. **Simplificar** e **reforçar** o seu panorama de segurança

Uma abordagem à segurança em layers, com as ferramentas certas, é essencial; mas procure **oportunidades** para cortar controlos desnecessários.

Arquiteturas de segurança excessivamente heterogéneas são difíceis de gerir, são caras e podem aumentar o seu risco de exposição, por isso, aproveite todas as capacidades integradas na plataforma do seu fornecedor de cloud.

Isto é especialmente útil quando tem de reagir rapidamente a situações como habilitar colaboradores para o teletrabalho. Certifique-se de que está a aproveitar totalmente as capacidades de segurança internas, como as incluídas no Microsoft 365, que ajudarão a reduzir custos desnecessários.

avanade

#5. **Renovar** para concretizar a sua visão de segurança a longo prazo

Recomendamos que implemente uma abordagem holística à segurança e faça dela uma parte integrante da transformação digital da sua organização desde o início.

Integre a segurança nas soluções e aplicações de TI, em vez de tentar resolver o problema com a última solução de cybertech; que, ao fim de pouco tempo, se pode tornar redundante.

Quaisquer que sejam os sistemas que implemente, certifique-se de que são seguros do ponto de vista das aplicações modernas e de cloud, e de que possui uma boa compreensão do nível de responsabilidade que o fornecedor assumirá para o tornar seguro na conceção.

A segurança deverá ser um facilitador de negócios, por isso tente equilibrar segurança e controlos para evitar adicionar barreiras e afetar negativamente a produtividade do colaborador. Isto permitirá que a sua organização opere de forma ágil e se prepare para o que vier a seguir.

Por fim, faça da criação de uma forte cultura de segurança uma prioridade. A formação e educação abrangentes e consistentes irão ajudá-lo a tratar os riscos de segurança inerentes ao comportamento do colaborador. Isto pode exigir uma abordagem à gestão da mudança assente na educação contínua e na formação baseada na função para as pessoas.

Porquê a **Avanade**?

Liderar o mercado atual exige um pensamento orientado para o exterior

Na Avanade, temos estado a ajudar ativamente os nossos clientes durante estes tempos difíceis. Desde o início da pandemia de COVID-19, migrámos mais de um milhão de contas de trabalho à distância para os nossos clientes. Agora estamos a orientar estas organizações para um novo modelo operacional seguro, que seja criado para as adaptar e proteger no futuro.

Somos especialistas em ajudar a proteger os seus ecossistemas Microsoft e de TI híbridos. Os nossos serviços de segurança proporcionam uma abordagem holística através de advisory, implementação e gestão de serviços. Podemos ajudá-lo a realizar uma avaliação de risco e a implementar uma arquitetura segura. Como fornecedor de serviços de segurança, podemos também reforçar a sua equipa de segurança e realizar a monitorização de eventos 24 horas/dia e providenciar apoio operacional permanente para o ajudar a manter-se à frente dos riscos de segurança.

Fornecemos metodologias comprovadas, especialização aprofundada e tecnologia de ponta, e somos o Parceiro do Ano da Microsoft Alliance SI há 14 anos.

AVANADE IS GOLD FOR MICROSOFT'S SECURITY COMPETENCY

MICROSOFT SECURITY 20/20 SECURITY ADVISORY OF THE YEAR WINNER

MICROSOFT PARTNER FOR OFFICE 365 FOR TEN CONSECUTIVE YEARS

MICROSOFT ALLIANCE PARTNER OF THE YEAR FOR 14 YEARS

avanade

Começar **hoje**

Se, como muitos clientes, teve de dimensionar rapidamente o teletrabalho, um bom ponto para começar é a nosso assessment de segurança e workshops.

Trabalharemos consigo para compreender os drivers do seu negócio, a infraestrutura e os processos existentes para apresentar uma avaliação holística do seu panorama de segurança e criar um plano para o ajudar a concretizar a sua visão de segurança a longo prazo.

Oferecemos o seguinte:

Avaliação de Segurança Microsoft 365 e Workshop

- Avaliamos o seu atual ambiente Microsoft 365 numa perspetiva de segurança para identificar lacunas e áreas de resolução.
- Apresentamos uma análise abrangente e um plano com base nos controlos e requisitos de segurança da sua organização.
- Um relatório e painel de controlo de Pontuação Segura que apresenta informações sobre proteção de dados e governação.
- Uma avaliação holística apresenta orientações sobre mitigação dos crescentes riscos de segurança.

Avaliação da Infraestrutura e Processo de Identidade

- Uma avaliação abrangente e descoberta automatizada de riscos.
- Avaliamos a sua infraestrutura para recomendar melhorias.

Contacte-nos para saber mais ou visite **avanade.com/security**

North America
Seattle
Phone +1 206 239 5600
America@avanade.com

South America
Sao Paulo
AvanadeBrasil@avanade.com

Asia-Pacific
Australia
Phone +61 2 9005 5900
AsiaPac@avanade.com

Europe
London
Phone +44 0 20 7025 1000
Europe@avanade.com

About Avanade

A Avanade é líder na prestação de serviços digitais inovadores e de serviços de cloud, soluções de negócio e experiências lideradas pelo design em ecossitemas da Microsoft. Com 38 000 profissionais em 25 países, somos a força do Accenture Microsoft Business Group, apoiando as empresas na captação de clientes e capacitação de colaboradores, na otimização das operações e transformação dos produtos, potenciando a plataforma da Microsoft Detida maioritariamente pela Accenture, a Avanade foi constituída em 2000 pela Accenture LLP e pela Microsoft Corporation. Saiba mais em www.avanade.com.

avanade


avanade