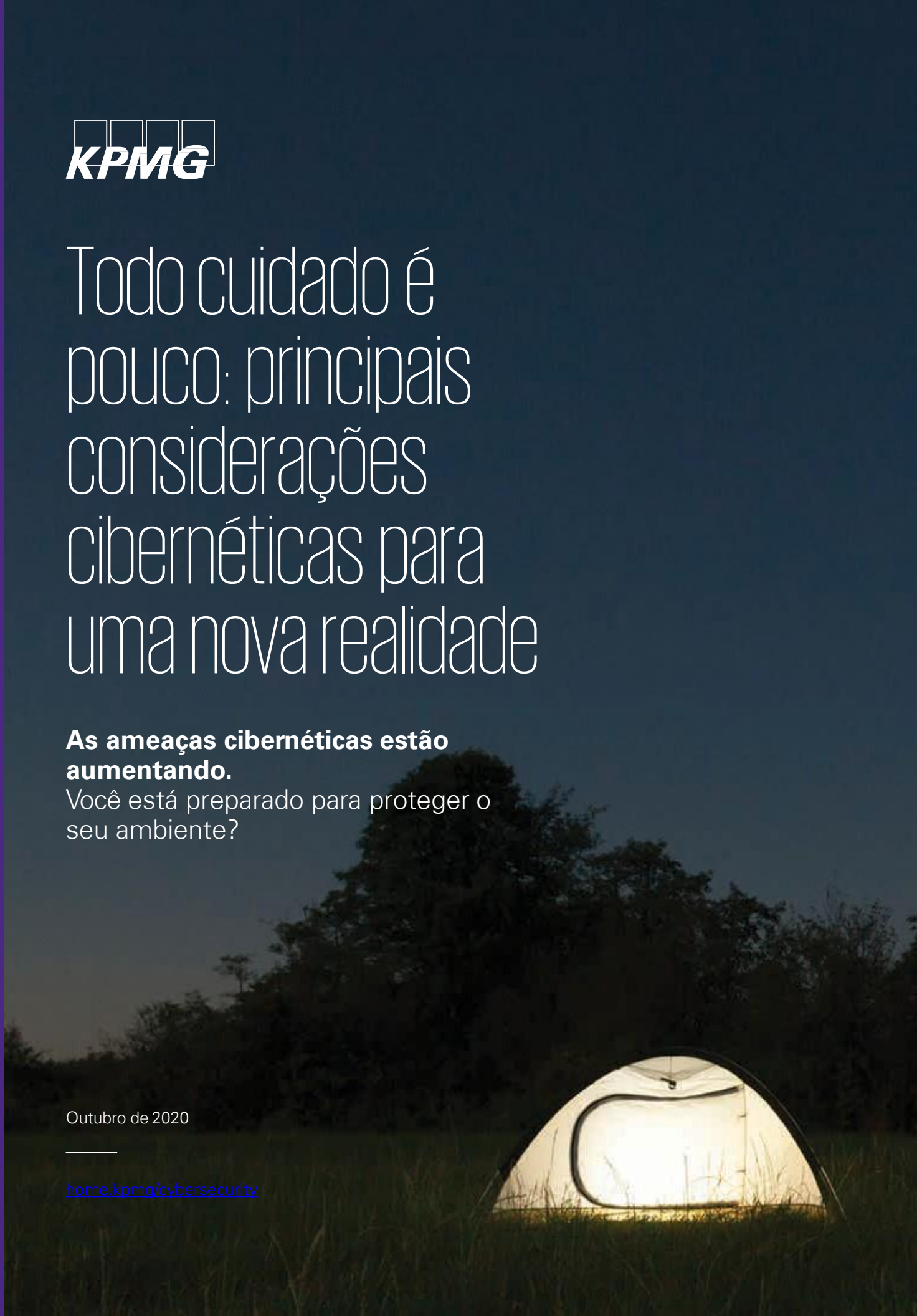

Todo cuidado é pouco: principais considerações cibernéticas para uma nova realidade

As ameaças cibernéticas estão aumentando.
Você está preparado para proteger o seu ambiente?

Outubro de 2020

home.kpmg/cybersecurity

©2021 Copyright de uma ou mais entidades da KPMG International.
As entidades da KPMG Internacional não prestam serviços a clientes. Todos os direitos reservados.

O mundo mudou drasticamente em 2020. Os negócios já estavam mudando e a quarta revolução industrial está bem avançada. No entanto, a COVID-19 acionou os instintos de sobrevivência das empresas, que aceleraram sua digitalização para ter sucesso na nova realidade. A ideia de que os dados se tornaram a força vital da organização foi reforçada conforme os conselhos buscam explorar o potencial da nossa economia digital, criar novas experiências para os clientes, transformar seus serviços e gerar eficiências e reduções de custos na esteira da pandemia. O futuro está sendo criado a partir de uma fusão de novos modelos de negócios, novas tecnologias e novas parcerias.

Neste mundo em constante mudança, existem empresários inescrupulosos que estão ganhando dinheiro nesta nova economia. Infelizmente, eles são cibercriminosos e estão do lado errado da lei. Eles representam novos desafios para negócios legítimos, e as empresas precisam pensar de forma diferente sobre como proteger sua vantagem competitiva e desenvolver novos modelos com o objetivo de se tornarem e permanecerem seguras.

Os profissionais de segurança cibernética precisam demonstrar que podem proteger a base dos negócios transformados com uma agilidade de raciocínio e de ação que reconhece o ritmo e a velocidade com que os criminosos cibernéticos atuam.

As organizações precisam contar com o tipo de talento colaborativo — em toda a empresa — capaz de assumir uma postura proativa e de enfrentar esses problemas de frente. O Chief Information Security Officer (CISO) não consegue fazer tudo sozinho. Novas parcerias são necessárias. A tecnologia é uma oportunidade, não uma ameaça, enquanto a segurança cibernética está se tornando um fator essencial para os negócios.

Selecionamos oito considerações cibernéticas importantes que provavelmente moldarão a maneira pela qual as organizações abordam a segurança na nova realidade e solicitamos que nossos profissionais compartilhassem seus insights e experiências para ajudá-lo a enfrentar os desafios futuros.

> **A resiliência cibernética contínua e bem-sucedida exigirá o alinhamento estratégico das estratégias cibernéticas, com resposta a incidentes, continuidade dos negócios e planejamento da recuperação de desastres.**
>
> **Temos que envolver toda a empresa — do front-office ao back-office.**
>
> **— Akhilesh Tuteja**
> Segurança Cibernética Global
> Colíder da KPMG International

Endereçando o déficit de segurança

Alinhamento dos objetivos de negócios com as necessidades de segurança

Confiança digital e autenticação do consumidor

A equipe de segurança em evolução

A próxima onda de regulação

Cloud transformation

Automatização da função de segurança

Desafiando as premissas da resiliência

©2021 Copyright de uma ou mais entidades da KPMG International.
As entidades da KPMG Internacional não prestam serviços a clientes. Todos os direitos reservados.

Endereçando o déficit de segurança

A pandemia da COVID-19 gerou um grande choque no modelo de trabalho da maioria das organizações. Na corrida para acelerar sua transformação digital, as verificações usuais dos controles de segurança e privacidade precisaram ser colocadas em segundo plano. Nos próximos meses, as empresas que se ajustarem à nova realidade precisarão começar a reexaminar seu ambiente de tecnologia e restabelecer o controle.

O cenário conforme o enxergamos

Quando se trata de mudanças tecnológicas, as equipes de segurança preferem adotar uma visão estratégica. No entanto, para as empresas que foram forçadas a adotar soluções de trabalho remoto e de infraestrutura em nuvem rapidamente, integrar novos fornecedores de tecnologia no curto prazo e mudar para canais de comércio digital para manter seus fluxos de receita, as considerações de segurança e privacidade, compreensivelmente, ficaram atrás da necessidade de assegurar o negócio.

A poeira baixou. As empresas atualmente estão se adaptando à nova realidade do trabalho remoto e começando a entender algumas das características mais permanentes da mudança. Algumas pessoas começarão a trabalhar nos seus escritórios novamente quando isso for seguro — mas muitos funcionários vão preferir continuar trabalhando em casa. A equipe terá se acostumado com as novas ferramentas de colaboração e com a infraestrutura virtual, enquanto os clientes sempre ficarão felizes em ter a opção do comércio e pagamentos digitais.

Cabe à equipe de segurança restabelecer o controle sobre o novo conjunto de tecnologias que foi implementado durante a pandemia, garantir novos canais de dados e pagamentos e adaptar seus controles ao novo modelo de trabalho. Porém, no longo prazo, essa é uma chance de reavaliar as operações da função de segurança.

As empresas agora têm expectativas maiores quanto à eficiência da equipe de segurança. Elas viram como a segurança conseguiu agilizar imediatamente suas verificações no que tange a novos fornecedores, desenvolvimento de novas aplicações e novas ferramentas de colaboração. Poderão estas empresas extrair algumas das lições aprendidas nessa fase e aplicá-las para otimizar a segurança por projeto (security-by-design) na nova realidade? Com o aumento das pressões de custo, a busca por velocidade, agilidade, escalabilidade e eficiência nos processos de segurança é maior do que nunca.

As organizações mais bem-sucedidas equilibrarão a necessidade de abordar a eficiência e de permanecerem estratégicas.

Esse é o momento perfeito para se concentrar em eliminar desperdícios, limpar os dados e avaliar o valor das suas estruturas de governança, processos e tecnologias e controles gerais. Isso é eficaz na redução do risco? Reflita sobre o futuro das soluções cibernéticas na sua organização e preste atenção às iniciativas que enriquecem seus dados, fazendo com que você detecte e responda mais rapidamente às ameaças cibernéticas. Fique perto do negócio que você está possibilitando e dos clientes que está protegendo.

— Leah Gregorio
Managing Director
KPMG nos EUA

©2021 Copyright de uma ou mais entidades da KPMG International.
As entidades da KPMG Internacional não prestam serviços a clientes. Todos os direitos reservados.

O que acreditamos que você deve fazer a esse respeito

Comece entendendo os seus ativos. O ambiente digital da sua organização pode ter crescido significativamente durante a pandemia como parte das medidas de transição para o trabalho remoto. Converse com os líderes dos departamentos, execute ferramentas de detecção e descoberta e analise os documentos de compras — você precisa entender se alguma nova solução de software foi adquirida pelas equipes de negócios para uso durante o trabalho remoto, quais novos serviços em nuvem foram criados e quais aplicações e dados esses serviços estão mantendo, e se houve novos dispositivos de terminais (endpoint devices), como laptops, celulares, discos rígidos etc., fornecidos para apoiar as equipes sem o seu conhecimento.

Uma vez que você tiver uma visão de como é o novo ambiente, cabe às equipes de segurança e privacidade trabalharem em conjunto para analisar os controles da infraestrutura nova e antiga e entender se eles estão de acordo com a política e o apetite de risco da organização. Conforme os gaps no compliance começam a surgir, trabalhe com a empresa para corrigi-los. Particularmente para as aplicações voltadas para o consumidor, é fundamental lembrar a empresa que a marca e, portanto, a receita agora está vinculada à confiança que os consumidores depositam na segurança e na privacidade dos seus dados pessoais.

Reflita também sobre seus processos-padrão de monitoramento de segurança e da privacidade. Você precisou pular as atividades de garantia do business-as-usual para novos fornecedores, analisar o código para novos produtos de consumo ou restringir adequadamente as funcionalidades de ferramentas de colaboração e conferência? Determine onde estão os gaps e evidencie as atividades que você realiza para remediá-los — os órgãos regulatórios podem estar curiosos para entender como você enfrentou os desafios.

Comece a planejar no longo prazo. Pergunte aos líderes de negócios, às equipes de desenvolvimento e aos fornecedores se houve algo que eles gostaram nas atividades de segurança durante a pandemia. Analise os processos por conta própria; houve algum caso em que você percebeu que um processo otimizado ou um conjunto diferente de controles ainda permitia gerenciar seu risco cibernético? Reflita sobre como incorporar as lições aprendidas nas operações futuras.

Alinhamento dos objetivos de negócios com as necessidades de segurança

Diversas organizações investiram pesadamente em segurança cibernética, tanto em ferramentas quanto em pessoal. Conforme as empresas sentem o impacto econômico da pandemia, o esforço para reduzir esses custos aumenta. Nesse sentido, o custo da segurança tornou-se um foco importante — talvez tão importante quanto a própria segurança. Em um esforço para gerenciar custos e assegurar que as prioridades de negócio e a segurança estejam alinhadas, as empresas estão automatizando partes significativas da sua funcionalidade cibernética, implementando processos de gerenciamento de riscos cibernéticos digitalizados para garantir que sigam as principais estratégias operacionais e de negócios da organização.

O cenário conforme o enxergamos

Ao analisar muitos modelos de risco, percebemos que o conceito de cenários de risco orientados para o negócio está ausente. Certamente, a pandemia revelou uma desconexão importante entre a percepção das empresas sobre o valor da tecnologia e os riscos cibernéticos que surgem com a adoção. A perspectiva do negócio precisa acompanhar a perspectiva da equipe de segurança cibernética, e esse não é o caso em muitas organizações. A identificação desses cenários de risco deve ser liderada pela empresa.

O processo seria muito mais efetivo se fosse fundamentado por um modelo que permitisse que os líderes de negócios entendessem melhor o impacto que os controles de segurança podem ter nesses cenários de risco. Muitas empresas não obtêm esse insight de maneira consistente, dificultando a formulação de um relacionamento contínuo e transparente entre os controles e o negócio.

Na comunidade cibernética, tentamos planejar os piores cenários, mas muitos incidentes acontecem sem que sejam percebidos, sem serem arrasadores ou gerarem grandes danos às empresas. Com base nessa perspectiva, vemos muitas empresas trabalhando para incorporar a segurança não apenas na segunda linha de defesa, mas também na primeira. Porém, com a primeira linha mais focada operacionalmente e a terceira linha orientada pela auditoria.

As organizações de maior porte gastaram, nos últimos 10 a 15 anos, muito dinheiro em segurança de TI. A pandemia demonstrou o papel crescente da segurança cibernética na nova realidade. No entanto, há uma necessidade de cumprir esse papel sem aumentar o custo. Isso exige que as empresas desenvolvam um novo modelo baseado em risco, focado na redução de custos por meio de uma abordagem automatizada à segurança e na alocação das pessoas certas nas funções adequadas.

Vimos inúmeras situações em que as considerações de segurança são excessivas e restritivas, inibindo o crescimento das empresas e, por outro lado, exemplos em que os controles são muito frouxos. É necessário haver um alinhamento mais próximo da segurança com o negócio para assegurar que o nível e o tipo correto de segurança sejam aplicados para maximizar a efetividade de custos e a abrangência.

— Hartaj Nijjar
Principal
KPMG no Canadá

Alinhar a postura de segurança cibernética de uma organização com seus objetivos gerais de negócios é fundamental para proteger as empresas contra violações e intrusões. Os líderes de segurança são responsáveis pela implementação de estratégias de segurança cibernética eficazes e impactantes de maneira eficiente e pelo gerenciamento do custo da segurança.

— Wilhelm Dolle
Principal
KPMG na Alemanha

O que acreditamos que você deve fazer a esse respeito

Reflita holisticamente sobre onde você precisa investir. Considere quais cenários de risco precisam estar em vigor e quais controles são os mais relevantes. Sejam quais forem os planos das empresas para a transformação digital antes da pandemia, atualmente elas estão entendendo a necessidade de acelerá-los na nova realidade, ao mesmo tempo que se preocupam com as pressões de custo. Isso sugere que elas também devem explorar a automação dos seus processos de gerenciamento de riscos e cibernéticos.

Muitos incidentes seriam detectados facilmente se as políticas e controles de segurança estivessem incorporados aos negócios. Em resumo, as empresas são incentivadas a integrar a segurança cibernética nas três linhas de defesa, em vez de atuar em 'silos'. Aproveite a inteligência sobre as ameaças de várias funções, como fraudes e crimes financeiros, e integre manuais e ferramentas para responder rapidamente às mudanças no cenário de ameaças cibernéticas e nos padrões de ataque.

Torne a segurança uma prioridade de ponta a ponta. A ação fundamental é estabelecer um diálogo contínuo entre a organização de segurança e o resto da empresa para garantir que a segurança esteja alinhada com o negócio em termos de planejamento estratégico e operacional.

Para esse fim, implemente abordagens de engenharia — como *secure by design e privacy by design* — que visam a introduzir a segurança na mentalidade diária da equipe de DevOps conforme ela cria novas aplicações e serviços.

Em última análise, esperamos ver os profissionais de segurança cibernética deixarem de ser percebidos como uma função orientada para a TI. Dessa forma, a equipe cibernética precisa estar orientada para o negócio e consciente das necessidades da empresa. Caso contrário, esse aperto de mão compartilhado entre o negócio e a equipe de segurança cibernética nunca vai se solidificar.

©2021 Copyright de uma ou mais entidades da KPMG International.
As entidades da KPMG Internacional não prestam serviços a clientes. Todos os direitos reservados.

Confiança digital e autenticação do consumidor

O mundo do comércio digital e do setor bancário mudou drasticamente este ano. Com isso, um novo conjunto de expectativas em torno das funcionalidades e da conveniência é esperado do setor financeiro, com a confiança sendo um componente fundamental da lealdade. Muitas grandes marcas globais estão se sentindo ameaçadas conforme as lojas físicas estão caindo no esquecimento. Quem reinar supremo em termos da experiência digital do cliente provavelmente conquistará a maior participação de mercado.

O cenário conforme o enxergamos

Em última análise, os clientes provavelmente irão para onde as interações são mais fáceis e onde eles se sentem protegidos e seguros.

No ambiente atual, a maneira de oferecer uma experiência superior ao cliente é reduzir os atritos. E, para os clientes que esquecem uma senha, o envio de um PIN para um dispositivo móvel via mensagem de texto que precisa ser reinserido e confirmado é um atrito.

Como resposta, muitas empresas estão adotando uma abordagem baseada em aprendizado de máquina que permite entender as características e padrões de comportamento típicos e únicos dos seus clientes, como impressões digitais ou de voz, além de diversas características biométricas físicas. As empresas financeiras, especificamente, estão trabalhando para entender como os clientes interagem com elas: como e quando eles geralmente efetuam o login, os tipos de transações que realizam, a faixa de valores que eles tendem a sacar ou transferir etc. Esses elementos podem ser agregados para produzir um 'instantâneo' exclusivo do cliente.

Para qualquer empresa que mantém uma interface, tudo se resume a otimizar a jornada do cliente, estabelecer confiança e manter a jornada curta e eficiente o suficiente para manter o engajamento. Se os clientes sentirem que estão saltando "obstáculos" percebidos demais, provavelmente levarão seu negócio para outro lugar. Embora o cliente precise estar feliz e desfrutar de uma jornada sem atritos até o resultado desejado, o fornecedor do produto ou serviço é responsável por garantir que toda a jornada seja segura.

As empresas precisam começar a repensar a maneira pela qual coletam dados e os disponibilizam para fazer a correlação com cenários de ameaças específicos. A ideia dos data lakes certamente não é nova, mas os dados que são coletados, como eles são mantidos em segurança, e assegurar que apenas as pessoas mais relevantes possam acessar e aproveitar esses dados são fatores fundamentais.

— Charlie Jacco
Principal da
KPMG nos EUA

Nos últimos anos, tem havido um foco primordial, principalmente nos EUA, nos centros de fusão de segurança. Isso significa tornar-se orientado para os dados na maneira como você trabalha para detectar incidentes de segurança e possibilitar um processo de resposta rápida, que é mais enxuto, adapta-se continuamente ao cenário de ameaças e procura permanecer um passo à frente dos maus agentes.

— AlexAnisie
Diretor da
KPMG no Reino Unido

©2021 Copyright de uma ou mais entidades da KPMG International.
As entidades da KPMG Internacional não prestam serviços a clientes. Todos os direitos reservados.

O que acreditamos que você deve fazer a esse respeito

Em primeiro lugar, as empresas — independentemente do setor — devem trabalhar para conectar as equipes de dados, autenticação e fraude de maneira sistemática e programática. Entenda os requisitos de governança, quais dados você está obtendo, quem é responsável por eles, de onde eles vêm e como serão utilizados. Construa uma cultura holística de segurança.

A partir daí, reflita sobre como oferecer uma experiência superior aos seus clientes, em que perguntas são feitas a eles para autenticação, facilitando a sua identificação, mas talvez exigindo mais informações para a realização de transações atípicas. Torne as interações diárias dos seus clientes as mais fáceis e indolores possíveis, mas adicione um pouco de atrito onde isso fizer sentido, algoritmicamente, com base em comportamentos comuns.

Priorize o entendimento das preocupações de privacidade e de dados no que tange a como e por quem seus dados serão usados. No futuro, muito provavelmente eles estarão na nuvem. Pense em como criptografá-los e protegê-los. Essa é uma questão que envolve toda a empresa e que pode ser solucionada pela tecnologia, mas, em última análise, baseia-se no desejo da empresa de que os clientes tenham uma melhor experiência de usuário ponta a ponta em todas as interações digitais com a empresa.

Além disso, as empresas fariam bem ao repensar a maneira pela qual avaliam os dados. A abordagem tradicional de aplicar um conjunto massivo de regras a vários conjuntos de dados não é mais sustentável. Ela está criando muitos falsos positivos e fazendo com que muitos casos de uso abram brechas que os fraudadores conseguem explorar. A ideia de aproveitar os algoritmos de aprendizado de máquina para analisar esses dados de maneira mais eficiente visando identificar tendências baseadas no comportamento é fundamental.

Finalmente, esteja atento à correlação entre pessoas e tecnologias em todo o processo de prevenção/detecção/resposta. Reconheça que o processo abrange toda a organização internamente, mas também afeta o mundo fora dos seus muros literais e figurativos, considerando que os problemas podem ser desencadeados por um terceiro. No final das contas, trata-se das lições aprendidas. Em se tratando da autenticação de usuários, reserve um tempo para analisar os incidentes anteriores e reintroduzi-los no seu protocolo de segurança para testes de estresse, em um esforço para evitar novas ocorrências.

A equipe de segurança em evolução

Nos últimos anos, houve uma grande tentativa de aumentar a importância da segurança cibernética no nível dos conselhos. Em 2020, muitos conselheiros estão bem cientes da agenda cibernética.

Embora entendam a importância do cyber, um dos maiores desafios para os profissionais de segurança é traduzir esse conhecimento em uma compreensão prática do que ele realmente significa para os negócios.

O cenário conforme o enxergamos

Em muitas empresas, a equipe de segurança cibernética continua sendo formada por um conjunto de profissionais de compliance técnicos e operacionais. Porém, há uma mudança acontecendo, com a transformação em um recurso mais estratégico e prospectivo que adota sua visão de mundo para afetar a dinâmica dos negócios.

Muitos Chief Information Security Officers (CISOs) e suas equipes, em diversos setores, estão trabalhando para se adaptarem à dinâmica da mudança nos negócios e se tornarem uma voz confiável e relevante no conjunto de estratégias. Eles também estão trabalhando para visualizar as prioridades operacionais específicas da organização e estabelecer parcerias com chefes de negócios internos para incorporar esses insights ao plano de segurança cibernética da empresa o mais rápido possível. Outro foco crítico da equipe de segurança, especialmente nas áreas de serviços financeiros e saúde, é atender aos requisitos regulatórios de maneira eficiente, tanto na perspectiva de tempo quanto de custo.

Os conjuntos de habilidades dos profissionais de segurança continuam evoluindo. De maneira geral, a equipe principal precisa aumentar sua perspicácia geral de negócios e o conhecimento dos produtos para poder articular melhor o risco cibernético em relação ao risco da empresa.

Aceite o fato de que o novo mundo é diferente. Não fique sentado dizendo: 'Eu pratico a segurança há 20 anos e a maneira como fazemos isso é A, B, C, D — não há outra forma'. Seja humilde o suficiente para perguntar: 'O que estamos realmente tentando fazer como empresa?' Em seguida, avalie a tecnologia disponível e elabore o melhor plano para o seu ambiente.

— Dani Michaux
Principal
KPMG na Irlanda

O CISO tornou-se o consultor interno confiável e um importante líder operacional. Entre as transformações digitais, um fator para extrair valor estendido dos ativos de dados, e as prioridades globais, todas as empresas podem se beneficiar com um executivo de segurança cibernética alinhado com o negócio e estrategicamente ciente, com uma equipe forte e focada para ajudar a proteger e capacitar a organização conforme ela avança nas novas fases de crescimento.

— Rik Parker
Principal
KPMG nos EUA

©2021 Copyright de uma ou mais entidades da KPMG International.
As entidades da KPMG Internacional não prestam serviços a clientes. Todos os direitos reservados.

O que acreditamos que você deve fazer a esse respeito

As equipes de segurança precisam sair da sua própria ilha, ouvir perspectivas diferentes e se comunicar mais com os líderes de negócios sobre o que a organização realmente precisa se preocupar nesse ecossistema em evolução.

Para empresas que estão passando por uma transformação digital — a maioria delas — a equipe de segurança cibernética deve procurar se inserir no meio dessas conversas sob uma perspectiva estratégica e se apresentar como o tecido conjuntivo entre o negócio, o digital e a segurança. Tenha objetivos comuns.

Identifique os tipos de dados que a empresa planeja colocar na nuvem. Entenda os tipos de interações que serão necessárias entre os ambientes de desenvolvimento e produção — em seguida, mapeie essas expectativas no plano de segurança.

Trabalhe em estreito contato com a área de comunicações corporativas e com as equipes que estão intimamente envolvidas com a experiência do cliente. Faça parte da estratégia de mensagens. Mesmo se um cenário de pior caso se concretizar, assegure que a organização continuará incutindo confiança nos consumidores.

Verifique o que a inteligência artificial (IA) pode fazer e o que realmente exige as nuances do raciocínio humano. Desafie-se a automatizar os controles básicos no seu ambiente de segurança. Busque atingir pelo menos 50%.

Finalmente, defenda a segurança cibernética como um recurso importante na agenda ambiental, social e de governança (ESG) da organização para demonstrar sua visão abrangente da governança de segurança cibernética e a capacidade de enfrentar uma ampla variedade de incidentes.

A próxima onda de regulação

Ao examinar o risco da tecnologia, você está falando sobre TI. No entanto, quando você fala sobre riscos cibernéticos, a propriedade e a responsabilidade ficam fora do departamento de tecnologia. A tendência que vemos na direção e magnitude das regulamentações baseadas em questões cibernéticas está migrando na direção de uma abordagem mais holística, com foco nas prioridades e responsabilidades do negócio, como atividades comerciais orientadas para o cliente, como construir confiança; tarefas operacionais middle-office e back-office; e funções de governança corporativa orientadas pelo Conselho. Em resumo, o foco está no gerenciamento da primeira linha de defesa, como deveria ser.

O cenário conforme o enxergamos

Em 2020 e além, esperamos continuar observando um aumento da regulamentação sobre diversos tópicos de vários órgãos regulatórios e, desde o início da pandemia, uma atenção especial tem sido dada, sem surpresa, à resiliência organizacional, na qual a cibernética desempenha um papel essencial. Na Ásia, especificamente, vimos novos regulamentos sobre segurança cibernética em que eles realmente usaram a palavra "cibernética". Anteriormente, os regulamentos naquela região usavam a palavra "tecnologia", que tinha uma conotação de TI. Essa maior precisão é um acontecimento bem-vindo.

Com tantos países emitindo regras para cumprir determinados elementos do Regulamento Geral de Proteção de Dados (GDPR), ou suas próprias leis de privacidade, estamos vendo — especialmente nas grandes empresas multinacionais — a criação de novos departamentos de gerenciamento de dados proativos. Essencialmente, as empresas buscam dominar a análise de dados como uma disciplina e entender não apenas onde os dados estão localizados na organização, mas também quem é responsável por eles, o que está sendo feito com essas informações e, talvez o elemento mais crítico, quais direitos e permissões os usuários têm em relação a esses dados. É mais importante do que nunca que as empresas acertem, já que a ética dos dados e os direitos de privacidade dos indivíduos continuam sendo um aspecto fundamental na nova realidade.

As empresas estão reconhecendo a necessidade de investimentos adicionais, não apenas em ferramentas e desenvolvimento de processos, mas em termos da falta de talentos cibernéticos, da governança cibernética e da estratégia de risco à configuração e manutenção. Ainda há um grande gap nessa área e, infelizmente, muitas empresas contratam profissionais de TI que não têm uma perspectiva de segurança cibernética em relação ao ambiente regulatório. O resultado são conselhos geralmente ineficazes ou bem intencionados, mas mal compreendidos ou implementados inadequadamente pela administração e pelo conselho.

> **Tornei-me um grande fã de simulações de ataque em várias camadas — as chamadas red teaming e ethical hacking. É fundamental testar suas operações de segurança para verificar se elas conseguem detectar diferentes tipos de ataques e, se eles estão sendo detectados, testar o plano e os procedimentos de resposta.**
>
> **Cada vez mais equipes regulatórias estão considerando esse fator nos seus processos principais.**
>
> **— Ton Diemont**
> Diretor
> KPMG na Arábia Saudita

> **Há três áreas — eu chamo isso de trilogia — nas quais os regulamentos cibernéticos estão focados: a tecnologia operacional subjacente; a terceirização de dados processados utilizando terceiros; e a resiliência, que significa a capacidade geral da empresa de detectar, responder e se recuperar de ataques cibernéticos.**
>
> **— Daryl Pereira**
> Principal
> KPMG em Cingapura

O que acreditamos que você deve fazer a esse respeito

Em relação ao modelo de três linhas de defesa, sugerimos incorporar as responsabilidades da segurança cibernética, bem como a função do CISO, na primeira linha — de preferência formalmente — e vincular essas tarefas a metas de desempenho anuais. A função do CISO, na sua essência, deve estar na primeira linha para cobrir a estratégia e a visão de segurança, e esse CISO deve ter um alinhamento hierárquico claro ou pelo menos funcional com as operações de segurança relacionadas ao monitoramento diário e à configuração das ferramentas.

A segunda linha (ou seja, risco de TI) deve apoiar políticas e normas de qualidade e resiliência do projeto e reportá-las de volta à administração e ao conselho. A terceira linha deve revisar e avaliar o trabalho das duas primeiras. Essa situação ideal procura estender as necessidades de segurança cibernética da empresa, incluindo a conformidade regulamentar, em toda a organização.

Também acreditamos que é fundamental instituir testes contínuos do seu programa de conformidade regulamentar em termos de projeto, implementação e efetividade para identificar onde melhorias são necessárias. Além disso, garanta que a resiliência cibernética operacional esteja incorporada à sua arquitetura e aos processos gerais para solidificar a segurança para a TI e OT.

Aloque um indivíduo que não seja estritamente um profissional de TI para supervisionar a conformidade regulamentar. De fato, os novos CISOs devem se sentir mais à vontade para falar o idioma do negócio, visando garantir que suas mensagens sejam entendidas e executadas. Esse indivíduo deve ter uma mentalidade ampla em relação ao modelo operacional da empresa — um Diretor de Risco, Diretor Financeiro ou Vice-Presidente Executivo seria o ideal, pois eles também têm uma perspectiva da agenda geral de riscos da empresa. Esse profissional seria o patrocinador ou defensor da segurança cibernética em toda a organização, trabalhando em estreita colaboração com o Diretor de Operações e o CISO.

Reserve algum tempo para unificar todos os seus requisitos regulamentares, de controles e políticas internas a vários regulamentos regionais e específicos do país, em uma única estrutura de controles unificados para ajudar a aumentar a efetividade dos seus esforços internos de governança, risco, compliance e testes. Procure sinergias entre os controles exigidos pelos regulamentos de privacidade, resiliência e segurança — você pode se surpreender com o que vai encontrar.

As empresas são incentivadas a mudar seu foco de sistemas e tecnologia para a informação. Identifique o que o torna competitivo no mercado. Isso pode ser a propriedade intelectual ou sua cadeia de suprimentos ou ainda seu poder de estabelecimento de preços. Seja o que for, é isso que você precisa proteger considerando uma perspectiva de segurança cibernética.

Cloud transformation

Um dos aspectos em que muitas empresas precisam trabalhar é alinhar a organização do CISO com o restante da empresa no que tange à maturação e eficácia da nuvem. A pandemia forçou muitas empresas a acelerar sua transformação digital, e a adoção da nuvem, que poderia ter levado 18 meses, foi concluída em questão de semanas. A segurança pode muito bem ter sido uma reflexão tardia, conforme as empresas se esforçavam para se preparar para a nova realidade. No futuro, o CISO e sua equipe de segurança devem desenvolver processos e ferramentas que são vitais para e totalmente alinhados com os fatores de negócios e a tecnologia necessária para oferecer suporte aos resultados de negócios desejados desde o início.

O cenário conforme o enxergamos

Historicamente, a área de TI é responsável pelo provisionamento de infraestrutura e, antes da nuvem, ela se concentrava principalmente nos non-cloud challenges (desafios fora da nuvem). A equipe de segurança é responsável por verificar a infraestrutura em busca de vulnerabilidades, mas geralmente não sabe o que verificar, pois geralmente há uma desconexão com a área de TI em uma lista atualizada de ameaças. O gerenciamento da infraestrutura e dos ativos relacionados sempre foi exigente, mas na nuvem, onde tudo é mais rápido e efêmero, envolver a área de segurança antecipadamente e elaborar o plano de provisionamento é um desafio que muitas empresas enfrentam.

Em termos da nuvem, em vários setores, a organização do CISO não está preparada para possibilitar os negócios, seja em termos de habilidades ou de talentos. Na nuvem, a prioridade é proteger as informações. O que estamos descobrindo cada vez mais é que a maneira pela qual os dados estão sendo implementados na nuvem não costuma ser necessariamente resiliente. Não estamos falando apenas de várias zonas de disponibilidade, mas da capacidade de recuperar ativos críticos se houver uma grande violação.

Em muitas empresas, estamos vendo dois campos que aparentemente atuam em extremos opostos do espectro de segurança. De um lado, os profissionais da velha guarda que trabalham na arquitetura de segurança há 20 anos ou mais, mas não se adaptaram totalmente à vida na nuvem. De outro, você conta com profissionais de segurança de última geração, familiarizados com a tecnologia atual e tentando promover e habilitar a mentalidade da nuvem para que a segurança possa ser incorporada por design e em escala. Na esteira da pandemia e da rápida aceleração da adoção da nuvem pelas empresas, fazer com que essas partes tenham um entendimento comum é uma prioridade.

As equipes de segurança precisam entender que não há problema na destruição, desde que você aprenda algo rapidamente e aplique esse conhecimento de uma maneira produtiva. Muitas organizações não têm confiança para pensar dessa maneira. Uma cultura de experimentação e aprendizado é o que atrairá o tipo de talento cibernético que as empresas precisam no atual mercado em rápida evolução. A nuvem permite criar e quebrar as coisas rapidamente, reconstruir e obter sucessos incrementais.

— Caleb Queern
Diretor
KPMG nos EUA

Cada vez mais, estamos descobrindo arquitetos de segurança com experiência em ciência da computação e com familiaridade no processo de programação. Eles percebem que precisam assumir a liderança e permitir que seus colegas usem esse novo conjunto de ferramentas em nuvem e apoiem a segurança no design. Portanto, estamos começando a ver a ponte entre a nuvem e a segurança — o papel do profissional de segurança na nuvem está começando a surgir, mas ainda são poucos e dispersos.

— Katherine Robins
Sócio
KPMG na Austrália

O que acreditamos que você deve fazer a esse respeito

Torne-se uma organização de aprendizado. O que atrai os talentos da nuvem, além do dinheiro, é a cultura. Os funcionários potenciais precisam saber que não estão entrando em uma organização clássica, avessa a riscos e que se movimenta lentamente. Você pode atrair grandes talentos da nuvem criando uma cultura aberta à inovação e à experimentação.

Da mesma forma, pense pequeno, mas aja rápido. Envie a mensagem de que você cria as coisas rapidamente, quebra as coisas ainda mais rápido, e depois as reconstrói com base no que aprendeu. Você já demonstrou que pode reagir rapidamente à pandemia. Agora é a hora de traduzir todas as lições aprendidas em business as usual. A segurança pode permitir o sucesso por meio de etapas incrementais. Por exemplo, comece a atuar com uma nova estratégia de proteção de contêineres em pequenas implementações e permita que a empresa se mova rapidamente.

Vire para a esquerda e desloque os controles o mais cedo possível no seu ciclo de testes de software, em um esforço para oferecer o máximo valor aos clientes e usuários. Aplique segurança — novamente, em pequenas implementações — o máximo possível no processo, o que normalmente envolve a infraestrutura como código. Faça isso acontecer, capacitando os desenvolvedores para programar as medidas de segurança necessárias sem o envolvimento da equipe de segurança, algo que a nuvem pode facilitar.

Valorize o código subjacente — a capacidade de ler a programação e de programar pode fazê-lo conquistar o respeito dos engenheiros de DevOps. Além disso, aproveite essa oportunidade para realmente entender onde você deve se inserir. Cada vez mais, é isso que vamos ver dos profissionais de segurança — a capacidade de programar, porque estamos nos afastando da função tradicional da arquitetura de segurança baseada em diagramas de avaliação e entregando-a a um designer de soluções ou arquiteto de soluções para posteriormente criar uma solução, que será enviada a um engenheiro para suportar a infraestrutura física.

Trabalhe para entender — e comunicar para toda a empresa — o vínculo entre capacitação do negócio, resiliência do negócio e proteção da informação. Isso não é muito diferente do que você faria no local, mas é um pouco diferente quando você obtém dados críticos das regiões na nuvem. Tornar esse cenário parte do seu DNA permite eliminar o "ruído" do ponto de vista das operações, para que você possa se concentrar nas maiores prioridades de segurança.

Automatização da função de segurança

Antes da COVID-19, já estávamos vendo uma migração para a automação das funções de segurança, da autenticação da identidade à detecção e resposta a ameaças. Ao longo de 2020, o ritmo com que isso está acontecendo aumentou. Um amplo conjunto de dados de 'conheça seu cliente' (know your customer) e de detecção de fraude está sendo coletado e analisado por muitos setores, incluindo os de serviços financeiros, comércio eletrônico/varejo, tecnologia, mídia e telecomunicações e automotivo, entre outros. Estas informações anteriormente estavam nos 'silos' de cada função.

Na nova realidade, as empresas estão começando a perceber que estão sentadas sobre um tesouro de dados que — caso mais bem organizados e disponibilizados de uma maneira mais eficiente — podem ser extraídos e analisados para diversas finalidades de valor agregado e até mesmo para aliviar o custo crescente da pressão causada pela COVID-19.

O cenário conforme o enxergamos

O impacto econômico da pandemia foi enorme para governos e empresas. Receitas foram perdidas para muitos e os orçamentos de investimento estão sob pressão crescente. No entanto, essas pressões representam uma oportunidade para as empresas; de se tornarem mais eficientes em todas as funções de negócios, incluindo a segurança. Portanto, as empresas estão trabalhando arduamente para automatizar funções que até muito recentemente eram totalmente manuais, reunindo conjuntos de dados historicamente diferentes.

As empresas não apenas estão mais habilitadas para confirmar que os clientes digitais são quem dizem ser, como também estão adquirindo informações mais profundas, como quem tem um vírus no seu computador, recebeu um e-mail de phishing recentemente e tentou entrar em uma rede na qual não tinha acesso.

Os profissionais de segurança estão combinando ferramentas de terceiros e soluções internas para automatizar o manual cibernético geral o máximo possível e alinhá-lo aos objetivos de desenvolvimento de negócios e de experiência do cliente da organização, assim como enfrentar o desafio do encolhimento dos orçamentos. As empresas estão procurando automatizar a primeira e a segunda linhas de defesa via nuvem para melhor responder às ameaças em toda a empresa sem que um ser humano precise realizar esse trabalho, confirmando simultaneamente que os controles de segurança que eles esperam ter estão de fato funcionando conforme o esperado.

Infelizmente, as equipes de segurança não estão sozinhas na adoção da automação. Os agentes das ameaças também estão automatizando, escalonando e mercantilizando seus ataques. Essas melhorias os ajudam a aumentar a velocidade na qual eles atacam as empresas. Isso apenas enfatiza a necessidade de automatizar a função de segurança e melhorar a capacidade das empresas de gerenciar suas ameaças cibernéticas em um ritmo acelerado.

Como os CISOs buscam reduzir gastos e aumentar a efetividade de suas equipes, a desativação automática de ativos digitais desatualizados deve se tornar um pilar da sua estratégia mais ampla. Da mesma forma, eles devem explorar a automação de manuais de instruções dos seus centros de operações de segurança, tomar decisões de fraude e resposta cibernética por meio de parcerias com os principais fornecedores de gerenciamento de informações de segurança e de eventos em nuvem.

— Anthony Gawron
Diretor
KPMG nos EUA

O que acreditamos que você deve fazer a esse respeito

Lembre-se sempre: quem controla os dados tem o poder. Com isso em mente, o primeiro passo é transferir os dados corporativos críticos de diferentes fornecedores externos que tantas empresas mantêm nos seus sistemas para um local centralizado e acessível.

Também sugerimos defender uma iniciativa de normalização de dados dentro da organização, para limpar e rotular adequadamente os dados, para que você entenda quais dados possui, como eles estão sendo publicados e quais recursos estão disponíveis nos conjuntos de dados.

As organizações nas fases iniciais de maturidade, em termos da normalização de dados, talvez não estejam preparadas para avançar diretamente para a extração de insights por meio da IA e do aprendizado de máquina.

Para essas empresas, é importante priorizar os casos de uso que elas desejam endereçar — detecção de fraudes, melhoria da experiência do cliente, melhoria na eficiência operacional, por exemplo — e determinar como vincular as ferramentas, tecnologias e análises avançadas corretas para aproveitar os dados assim que eles estiverem disponíveis.

Esses casos de uso podem ajudá-lo a determinar os dados que você precisa integrar. No entanto, mais do que isso, podem garantir que você se concentre em exemplos de alto impacto para demonstrar os benefícios iniciais a uma empresa potencial e ajudar a justificar o investimento para a próxima fatia de casos de uso.

Os provedores de serviços de nuvem podem ajudá-lo a conseguir fazer isso, fornecendo uma linha cada vez mais flexível de recursos de monitoramento de compliance e segurança, além de plataformas analíticas escaláveis e adaptáveis (e orquestração da segurança).

©2021 Copyright de uma ou mais entidades da KPMG International.
As entidades da KPMG Internacional não prestam serviços a clientes. Todos os direitos reservados.

Desafiando as premissas da resiliência

Os eventos deste ano mudaram fundamentalmente o cálculo da tecnologia e do planejamento da resiliência cibernética. A forma do ecossistema de tecnologia mudou; as atitudes em relação à resiliência evoluíram; e os órgãos regulatórios estão considerando novas abordagens para o planejamento da continuidade da cadeia de suprimentos. As empresas que se preparam para o futuro devem repensar sua abordagem para o entendimento, planejamento e execução dos esforços de resiliência, abrangendo as equipes de segurança, o negócio e o ecossistema operacional mais amplo.

O cenário conforme o enxergamos

Se houve um lado bom dessa pandemia para as equipes de segurança e infraestrutura, ele foi que as organizações atualmente entendem até que ponto a tecnologia sustenta a produtividade e a receita das empresas. Nas empresas dominadas pelo trabalho remoto e implementações em nuvem, não basta pensar na tecnologia como um facilitador dos negócios — ela é o negócio.

Embora haja uma valorização cada vez maior do papel da segurança na resiliência, a nova realidade abriu um novo conjunto de metas e desafios que exigem novas abordagens. Os novos modelos de infraestrutura virtual mudaram as prioridades dos agentes das ameaças — que atualmente estão sendo criativos no uso de técnicas de phishing e malware — e das equipes de continuidade de negócios em resposta às ameaças. Além disso, os novos modelos de trabalho estão forçando as equipes de Operações de Segurança (SecOps) a revisar seus manuais de incidentes, ferramentas de detecção e de resposta e padrões de mudança.

No nível dos conselhos, algumas das premissas fundamentais do planejamento da continuidade dos negócios foram questionadas. As empresas podem assumir que sua rede de fornecedores de resposta a incidentes, centros de dados e serviços de arquivamento está funcionando normalmente? Qual é realmente o pior cenário possível na realidade pós-pandemia? As organizações precisam ter uma visão muito mais holística das suas dependências tecnológicas e pontos únicos de falhas — incluindo terceiros e equipes off-shore. Além disso, considerando a arquitetura do negócio, a segurança precisa desempenhar um papel fundamental no delineamento e gerenciamento das ameaças.

Enquanto isso, os órgãos regulatórios estão prestando muita atenção. Com os estados-nação tornando-se mais ativos no cenário de ameaças cibernéticas e os ataques cibernéticos a muitos setores sendo utilizados para atender às agendas econômicas e geopolíticas, os governos estarão realizando um planejamento de resiliência no nível dos setores e dos estados-nação. As organizações que apoiam esses planos precisarão oferecer níveis sem precedentes de cooperação, transparência e confiança, trabalhando com concorrentes, fornecedores, órgãos regulatórios e autoridades policiais para garantir ecossistemas resilientes.

> **A pandemia demonstrou como as empresas se tornaram dependentes de sua infraestrutura de tecnologia. No futuro, a tecnologia terá um papel ainda mais importante. Conforme as empresas adotam novos modelos operacionais baseados na tecnologia, a equipe de segurança precisa reavaliar sua resiliência e planejamento de recuperação.**
>
> **— Nashikta Angadh**
> Principal
> KPMG na África do Sul

> **A área cibernética historicamente tem sido muito baseada em ativos, visando preservar as bases tecnológicas do negócio. Se ela puder migrar para uma abordagem mais holística e baseada em serviços, trabalhando lateralmente para focar no principal fator da continuidade do serviço, as equipes de segurança terão a oportunidade de elevar as metodologias do plano de continuidade de negócios cibernético para a governança de resiliência em toda a empresa.**
>
> **— Andrew Husband**
> Principal
> KPMG no Reino Unido

O que acreditamos que você deve fazer a esse respeito

Algumas ações fundamentais podem ajudar uma organização a atualizar suas atividades de planejamento da resiliência em preparação para a nova realidade. Comece questionando algumas das principais premissas que foram feitas no passado — sua lista de piores cenários incluía a pandemia? Qual poderá ser o próximo exemplo? Você pode contar com o suporte do seu ecossistema ou precisa de habilidades internas de resiliência de segurança?

Reflita sobre a mecânica da primeira linha de defesa. O que mudou nas operações de segurança na nova realidade — os analistas podem trabalhar da mesma maneira que trabalhavam anteriormente? Você precisa oferecer novas rotas de acesso às principais ferramentas de gerenciamento de incidentes e eventos de segurança (SIEM) para atender às novas maneiras de se trabalhar? As vias de comunicação também precisam ser atualizadas — você pode confiar na colaboração corporativa e de conferência? Como você interage com parceiros, a exemplo de provedores de nuvem? E como você gerencia a contenção de malware quando não pode garantir acesso imediato a um terminal, como faria no escritório?

Repense como você elabora seus manuais. A pandemia terá demonstrado a muitas empresas que várias das mesmas ameaças levam ao mesmo impacto fundamental na tecnologia e nos negócios. Ao redirecionar o foco do seu playbook para baseado em impacto, e não em cenários, será possível cobrir todas as bases de uma maneira muito mais eficiente. Isso também ajuda a equipe de segurança a tirar proveito da recém-descoberta valorização do impacto da infraestrutura de tecnologia pelas equipes de negócios.

Trabalhe com as equipes de negócios para entender as consequências de longo prazo da pandemia nos seus modelos de trabalho. Talvez esses modelos mudem suas prioridades, apresentando uma superfície de ameaça diferente. O ransomware pode começar a focar soluções de Infraestrutura de Desktop Virtual (VDI) em vez de bancos de dados, garantindo o resgate da produtividade dos negócios em vez dos dados — questione-se como adaptar seus esforços de resposta e recuperação aos novos modelos operacionais. E reavalie suas prioridades — você precisa se preocupar tanto com os cenários de "perda do edifício" tanto quanto antes, ou os cenários de "indisponibilidade de pessoal" agora são mais prováveis?

Finalmente, comece a estabelecer conexões externas. Conforme os ataques cibernéticos crescem em escala e complexidade, teremos que começar a contar uns com os outros. Desenvolva relacionamentos de apoio com órgãos regulatórios, autoridades policiais, colegas da indústria e fornecedores de upstream e downstream. A forma da tecnologia mudou, tanto global quanto localmente, e uma cultura de boa-fé de transparência e colaboração pode ajudar a aliviar as pressões sobre a infraestrutura e serviços críticos.

©2021 Copyright de uma ou mais entidades da KPMG International.
As entidades da KPMG Internacional não prestam serviços a clientes. Todos os direitos reserva

Como a KPMG pode ajudar

Na KPMG, nosso time global de profissionais de segurança cibernética oferece uma visão multidisciplinar do risco, ajudando-o a implementar a segurança em toda a sua organização, para que você possa antecipar o futuro, mover-se mais rapidamente e obter uma vantagem com uma tecnologia segura e confiável.

Não importa onde você esteja na sua jornada de segurança cibernética, as firmas-membro da KPMG têm experiência em todo o espectro — da sala do conselho ao data center. Além de avaliar sua segurança cibernética e alinhá-la às suas prioridades de negócios, vamos ajudá-lo a desenvolver soluções avançadas, implementá-las, monitorar riscos contínuos e ajudá-lo a responder a incidentes cibernéticos com eficácia.

Para inspirar a confiança das partes interessadas (stakeholders) e proteger o futuro, você não precisa apenas de especialização tecnológica avançada e um profundo conhecimento de negócios para tornar a segurança cibernética um fator estratégico da sua transformação contínua. Você também precisa de pessoas criativas que tragam uma mentalidade inovadora e implementação prática para o mundo automatizado.

A KPMG pode oferecer essa combinação incomum de pontos fortes e os utilizamos para ajudá-lo a obter uma combinação invejável de sua preferência: confiança, agilidade e vantagem competitiva.

Juntos, vamos criar um mundo digital confiável, para que você possa superar os limites do que é possível.

home.kpmg/cybersecurity

©2021 Copyright de uma ou mais entidades da KPMG International.
As entidades da KPMG Internacional não prestam serviços a clientes. Todos os direitos reservados.

Fale com o nosso time no Brasil

Leandro augusto
Sócio-líder de Cyber Security
da KPMG no Brasil
lantonio@kpmg.Com.Br

Rodrigo Milo
Sócio de Cyber Security
da KPMG no Brasil
rodrigomilo@kpmg.com.br

Samara Schuch
Sócia-diretora de Cyber Security
da KPMG no Brasil
samaraschuch@kpmg.com.br

©2021 Copyright de uma ou mais entidades da KPMG International.
As entidades da KPMG Internacional não prestam serviços a clientes. Todos os direitos reservados.

Contate-nos

Akhilesh Tuteja
Colíder Global de Serviços de Segurança Cibernética da KPMG Internacional e Principal KPMG na Índia
T: +91 (124) 254 9191
E: atuteja@kpmg.com

Leah Gregorio
Managing Director
Serviços de Segurança Cibernética da KPMG
KPMG nos EUA
T: +1 212 954 2369
E: lgregorio@kpmg.com

Hartaj Nijjar
Diretora
Serviços de Segurança Cibernética da KPMG
KPMG no Canadá
T: +1 416 228 7007
E: hnijjar@kpmg.ca

Wilhelm Dolle
Diretor
Serviços de Segurança Cibernética da KPMG
KPMG na Alemanha
T: +49 30 2068-2323
E: wdolle@kpmg.com

Charlie Jacco
Diretor
Serviços de Segurança Cibernética da KPMG
KPMG nos EUA
T: +1 212 954 1949
E: cjacco@kpmg.com

Alex Anisie
Diretora
Serviços de Segurança Cibernética da KPMG
KPMG no Reino Unido
T: +44 207 6941587
E: alexandra.anisie@kpmg.co.uk

Dani Michaux
Diretora
Serviços de Segurança Cibernética da KPMG
KPMG na Irlanda
T: +35317004769
E: dani.michaux@kpmg.ie

Rik Parker
Diretor
Serviços de Segurança Cibernética da KPMG
KPMG nos EUA
T: +1 404 222 3000
E: rikparker@kpmg.com

Ton Diemont
Diretor
Serviços de Segurança Cibernética da KPMG
KPMG na Arábia Saudita
T: +966118748500
E: antondiemont@kpmg.com

Daryl Pereira
Diretor
Serviços de Segurança Cibernética da KPMG
KPMG em Cingapura
T: +6564118116
E: darylpereira@kpmg.com.sg

Caleb Queern
Diretor
Serviços de Segurança Cibernética da KPMG
KPMG nos EUA
T: +1 512 320 5104
E: cqueern@kpmg.com

Katherine Robins
Diretora
Serviços de Segurança Cibernética da KPMG
KPMG na Austrália
T: +61 3 8663 8850
E: krobins@kpmg.com.au

Anthony Gawron
Diretor
Serviços de Segurança Cibernética da KPMG
KPMG nos EUA
T: +1 312 665 3379
E: agawron@kpmg.com

Nashikta Angadh
Diretora
Serviços de Segurança Cibernética da KPMG
KPMG na África do Sul
T: +27827191368
E: nashikta.angadh@kpmg.co.za

Andrew Husband
Diretor
Resiliência Operacional da KPMG
KPMG no Reino Unido
T: +44 207 6941040
E: andrew.husband@kpmg.co.uk

David Ferbrache
Diretor Global de Cyber Futures
Serviços de Segurança Cibernética da KPMG
KPMG no Reino Unido
T: +44 203 920 0492
E: david.ferbrache@kpmg.co.uk

A prestação de todos ou de alguns dos serviços aqui descritos pode não ser permitida para clientes de auditoria da KPMG e suas afiliadas ou entidades relacionadas.

home.kpmg/socialmedia

Ao longo deste documento, "nós", "KPMG" e "nosso" refere-se à organização global ou a uma ou mais firmas-membro da KPMG International Limited (a "KPMG International"), cada uma delas sendo uma pessoa jurídica separada.

Todas as informações apresentadas neste documento são de natureza genérica e não têm por finalidade abordar as circunstâncias de nenhum indivíduo ou entidade específico. Embora envidemos nossos maiores esforços para fornecer informações precisas e oportunas, não pode haver garantia que tais informações sejam precisas na data de seu recebimento ou que continuarão sendo precisas no futuro. Ninguém deve tomar ações com base em tais informações sem a consultoria profissional apropriada após um exame detalhado da situação específica.

©2021 Copyright de uma ou mais entidades da KPMG International. As entidades da KPMG Internacional não prestam serviços a clientes. Todos os direitos reservados.

KPMG refere-se à organização global ou a uma ou mais firmas-membro da KPMG International Limited (a "KPMG International"), cada uma delas sendo uma pessoa jurídica separada. A KPMG International Limited é uma empresa inglesa de capital fechado limitada por garantia e não presta serviços a clientes. Para mais detalhes sobre nossa estrutura, visite https://home.kpmg/xx/en/home/misc/governance.html

O nome e o logotipo KPMG são marcas registradas usadas sob licença pelas empresas-membro independentes da organização global KPMG.