Fatores-chave sobre segurança cibernética em 2022

Confiança por meio da segurança

Janeiro de 2022

Prefácio

A segurança cibernética refere-se ao que você pode fazer — e não ao que não pode

O cenário de ameaças está aumentando. Os criminosos cibernéticos estão mais especializados e usando ferramentas e tecnologias cada vez mais sofisticadas. Nesse ambiente instável, acredita-se que os diretores de segurança da informação (*Chief Information Security Officers* — CISOs) e suas equipes devem adotar uma mentalidade de capacitação — a segurança cibernética não significa mais apenas prevenção. Ela não é uma questão de dizer o que não pode ser feito: é mostrar o que pode ser feito — de maneira segura.

Mudança de paradigma dos CISOs: de executor a influenciador

Embora uma das principais lições da pandemia seja que algumas das melhores equipes de segurança cibernética são capazes de mudar rapidamente para capacitar suas organizações a trabalhar com segurança, de maneira remota e efetiva, a conclusão mais ampla e mais estratégica é que esse período fez com que as empresas repensassem como se relacionam e atendem seus clientes em um ambiente que prioriza o digital. Essa mudança de mentalidade para o foco no cliente levou a uma rápida transformação digital, que ajudou os clientes a se moverem no ritmo dos com segurança.

Sob este ambiente dinâmico, os profissionais de segurança cibernética, que antes eram apenas executores, estão se transformando em influenciadores. Os altos executivos estão atentos. De acordo com a pesquisa *KPMG 2021 CEO Outlook*, a maioria dos CEOs (75%) acredita que uma estratégia cibernética forte é fundamental para gerar confiança com os principais públicos de interesse.

No entanto, no contexto da transformação digital acelerada — que aumenta os riscos de um ecossistema de terceiros em constante crescimento — as equipes cibernéticas também reconhecem o desafio de proteger o ecossistema dos seus alidados e cadeias de suprimentos, com 79% indicando que isso é tão importante quanto construir suas próprias defesas cibernéticas da organização.

A maioria dos CEOs (58%) acredita que está bem preparada para um ataque cibernético. Na verdade, para quase todas as organizações, algum tipo de evento cibernético é considerado cada vez mais inevitável. As equipes de segurança devem estar preparadas para a inevitabilidade crescente de algum tipo de evento cibernético e prontas para responder, recuperar e restabelecer a confiança o mais rápido possível para mitigar os danos. Ao mesmo tempo, elas devem reconhecer que o risco nesse ambiente é um alvo em movimento e em evolução. Do Conselho ao alto escalão e do *front* ao *back office*, controles devem estar em vigor para proteger os ativos de alto valor da organização e dos clientes, as chamadas *joias da coroa*.

Ao longo dos anos — e particularmente como resultado da pandemia — descobriu-se que a falta de preparação das equipes de segurança da informação e o fato de serem, muitas vezes, excessivamente conservadoras, podem ser tão prejudiciais quanto o próprio evento. É por isso que é tão importante ter um plano, testar suas respostas de acordo com diferentes cenários e entender a profundidade e a amplitude dos incidentes cibernéticos potenciais. Essa é uma oportunidade para que as organizações em praticamente todos os setores reinventem suas estratégias de resposta e recuperação e para que mudem a segurança de forma efetiva.

No horizonte: oito prioridades dos CISOs

Os CISOs devem desempenhar várias funções simultaneamente, mas eles não podem estar em todos os lugares o tempo todo. Embora seja importante lembrar que a segurança é tarefa de todos, é ainda mais relevante reconhecer que a segurança é fundamental para construir e manter a confiança do cliente e das partes interessadas.

Olhando para 2022 e para os próximos anos, este estudo concentra oito temas principais que os CISOs devem priorizar nos níveis do Conselho e diretoria. Esses temas, com foco no ambiente regulatório sempre instável, podem ajudar os executivos a entender melhor como o espaço cibernético pode ajudar os negócios com um plano de segurança baseado na responsabilidade compartilhada.

Quer sejam ameaças persistentes avançadas, *ransomwares* ou ataques de backdoor, quer seja algo ainda novo, provavelmente sempre haverá novos perigos a serem enfrentados. No entanto, se os CISOs e suas equipes seguirem um conjunto disciplinado de princípios projetados com os objetivos principais da organização em mente, e se o plano estiver atualizado e flexível, será possível posicionar a organização para mitigar o impacto dos ataques cibernéticos.

Akhilesh Tuteja
Sócio-líder global de Cyber Security da KPMG na Índia

A KPMG identificou

Oito principais fatores-chave sobre segurança cibernética em 2022

Clique nos temas para obter mais informações.

Ampliar a conversa estratégica sobre segurança

Mudar o tema da conversa de custo e velocidade para segurança eficaz, para ajudar a entrega de maior valor para o negócio e melhor experiência para o usuário.

Atingir o fator-chave: talentos e conjuntos de habilidades críticos

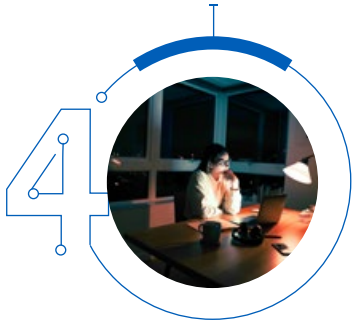
Transformar a postura dos CISOs e suas equipes de executores da segurança cibernética para influenciadores.

Adaptar a segurança para a nuvem

Aumentar a segurança da nuvem por meio da automação — da implementação à remediação, passando pelo monitoramento.

Colocar a identidade no centro do modelo *Zero Trust* (confiança zero)

A gestão de identidade e acesso (*Identitity and Access Management* - IAM) e o modelo *zero trust* deve estar implementada no local de trabalho hiperconectado atual.



Explorar a automação da segurança

Usar a implementação inteligente da automação da segurança para ajudar a gerar valor para os negócios.

Proteger a fronteira da privacidade

Migrar para uma abordagem multidisciplinar de gerenciamento de risco de privacidade que incorpore os conceitos de *privacy by design* e *security by design*.

Proteger além das fronteiras

Transformar as abordagens de segurança da cadeia de suprimentos — de manuais e demoradas para automatizadas e colaborativas.

Reformular a conversa sobre resiliência cibernética

Ampliar a capacidade de manter as operações, recuperar-se rapidamente e mitigar as consequências quando um ataque cibernético ocorrer.

Fator-chave 1

Ampliar a conversa estratégica sobre segurança

Alinhar os objetivos de negócios com as necessidades de segurança.

Os últimos dois anos redefiniram a maneira como vivemos, governamos e conduzimos os negócios. Proteger ativos e sistemas críticos e, o mais importante, dados proprietários sensíveis e de clientes não é mais um problema exclusivamente dos profissionais de segurança e de TI. Em vez disso, enfrentar e mitigar riscos para ajudar a manter a viabilidade estratégica e a sustentabilidade operacional de toda a organização é uma responsabilidade compartilhada que começa com o negócio.

Aumentar a visibilidade da sala de diretoria

A tecnologia digital atualmente alimenta e capacita as empresas de maneira muito similar à eletricidade durante a Revolução Industrial. Ela também tem a capacidade, caso seja insuficientemente protegida ou resiliente, de interromper as comunicações e as cadeia de suprimentos. Uma única violação de dados ou ataque de *malware* tem a capacidade traiçoeira de incapacitar transações em tempo real e interações de rede e, em última análise, interromper os negócios e afetar o crescimento da receita por dias, semanas ou até meses.

Os líderes seniores começaram a entender que o gerenciamento de risco cibernético para obter vantagens competitivas e sucesso de longo prazo começa na sala de diretoria e no alto escalão. Delegar a tomada de decisões estratégicas e o gerenciamento de riscos, especialmente o risco inerente à digitalização, já não é mais suficiente. As soluções de segurança modernas só podem obter excelentes resultados em termos de redução de riscos se os objetivos de negócios incluírem uma estrutura de segurança robusta incorporada.

O ambiente de negócios global atual é continuamente afetado por incertezas geopolíticas, ambientais, sociais e tecnológicas. O cenário de riscos cibernéticos resultante é alimentado por um volume cada vez maior de dados confidenciais trafegando por redes interconectadas e integradas. Os CISOs — dos quais se espera cada vez mais que falem a linguagem do Conselho, da empresa e da segurança — devem colaborar para construir resiliência por meio de investimentos pragmáticos em segurança para apoiar os objetivos de crescimento organizacional. Para esse fim, as equipes de segurança cibernética estão buscando diversas estratégias, como focar a automação e a melhoria dos seus portfólios de tecnologia da segurança, desenvolvendo, nos grupos de habilidades essenciais, profundidade para proteção contra uma escassez crescente de talentos, além de criar modelos de entrega que incorporem ecossistemas de aliados de segurança e de risco.

Qual é a sua jogada?

Para alinhar melhor a segurança com os objetivos estratégicos de negócios da organização, os CISOs e suas equipes devem ajudar a liderança em toda a empresa a obter um entendimento do que ocorre na área de *security by design* e de *privacy by design*. Recomenda-se mudar a conversa: de custo e velocidade, para uma arquitetura de segurança mais eficaz, com o objetivo de oferecer maior valor de negócio e experiência do usuário aprimorada. Os custos de interrupção de sistemas voltados para o consumidor ou dados comprometidos superam o que as equipes cibernéticas normalmente quantificam operacionalmente, e são ampliados pela degradação da confiança do consumidor e do investidor, o que pode ter um impacto duradouro.

Negócios digitalmente nativos ou maduros estão determinados a migrar rapidamente sua perspectiva de desenvolvimento que não enfatiza consistentemente os fundamentos de risco e segurança.

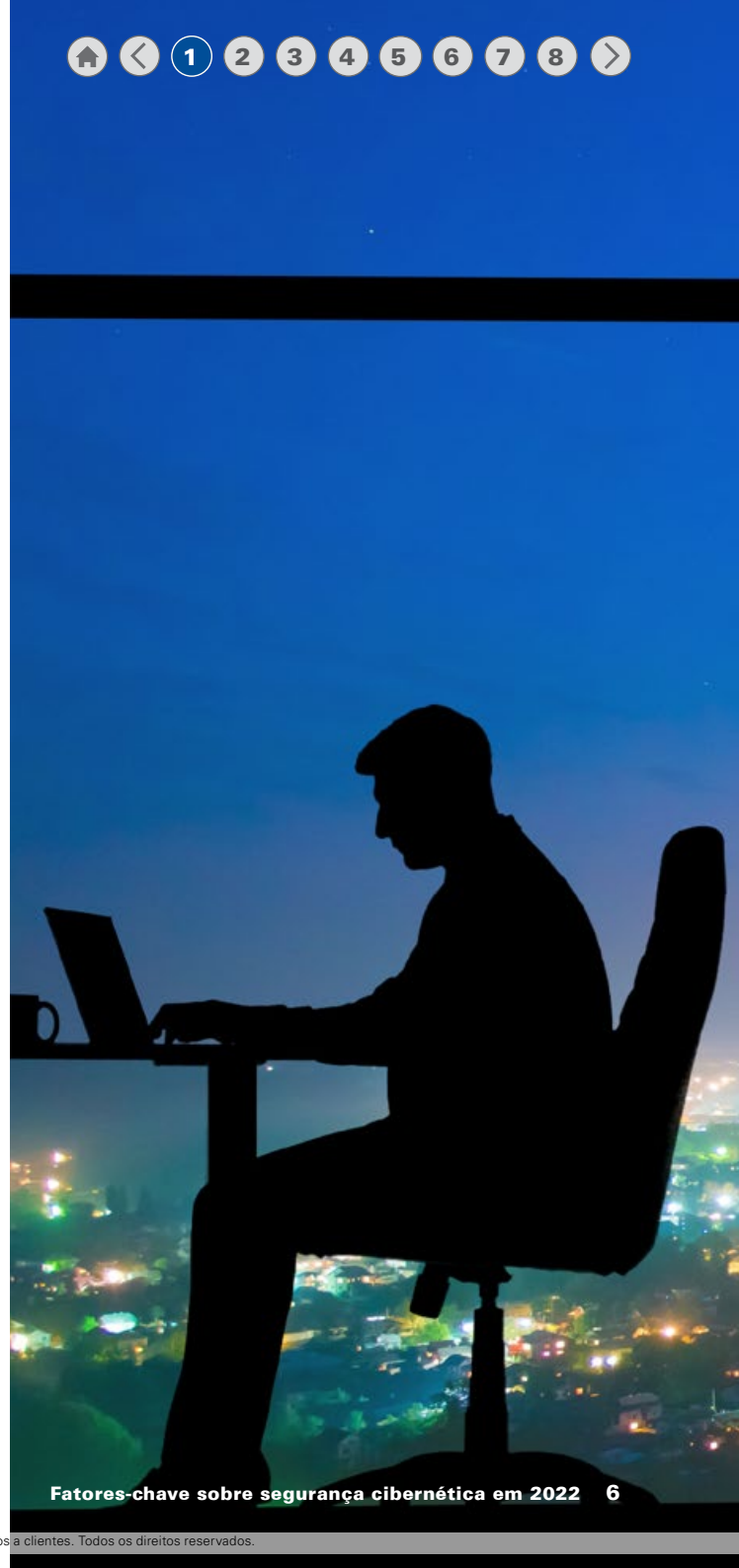
> *"A interpretação é um grande desafio para os CISOs: explicar a dinâmica de risco ao Conselho e aos comitês operacionais em termos de colaboração e cooperação. Eles devem articular que não estão tentando parar o negócio, e sim prestando o suporte necessário para aumentar a confiança dos seus consumidores, investidores e parceiros. A segurança deve ser um modelo de responsabilidade compartilhada, pertencente a todos."*
>
> **Rik Parker**
> Sócio de Cyber Security Services da KPMG nos EUA

As empresas precisam encontrar um equilíbrio. A velocidade no mercado é claramente essencial para a vantagem competitiva atualmente, mas é igualmente importante incorporar segurança aos processos de negócios, de uma maneira que permita à organização manter o ritmo, em vez de criar um gargalo em segurança da informação. O custo — na forma de clientes e investidores perdidos e de reputação manchada — de não focar a segurança adequadamente pode ser substancialmente mais alto do que dedicar um tempo para fazer isso da maneira correta.

A retenção e aquisição de talentos é outra área com lacunas, em que as organizações precisam avaliar se a automação e a alavancagem de aliados podem suplementar e complementar uma força de trabalho de segurança qualificada e cada vez mais diversificada. Há muitas empresas competindo por um conjunto limitado de talentos. Embora a comunidade cibernética possa trabalhar com as universidades para aumentar o fluxo de talentos e desenvolver funções mais atraentes para atrair e reter talentos, a indústria também deve procurar incorporar a tecnologia aos processos de negócios e ao planejamento, em um esforço para ajudar a reduzir o impacto de recursos em tarefas repetitivas. Isso provavelmente exigirá uma automação inteligente, quando possível, e criatividade nos modelos de entrega e aquisição de talentos onde não há.

A inteligência artificial (IA), e particularmente o *machine learning* (ML), em conjunto com ferramentas de segurança inteligentes e orquestradas, devem ser consideradas não apenas para isolar exposições e vulnerabilidades, mas também para automatizar as correções e remediações. Em um cenário ideal, as organizações deveriam tirar a inteligência artificial das mãos dos profissionais de desenvolvimento, automatizando o trabalho apropriado conforme o desenvolvimento está em andamento.

Além de ajudar a manter a velocidade durante o ciclo de vida de desenvolvimento de software, a IA pode ajudar as empresas a evitar a entrega de códigos ruins aos clientes, que poderiam então distribuí-los por meio de suas redes. Na prática, isso pode exigir transferir alguns controles e riscos para aliados externos. Esse ainda é um conceito difícil para os CISOs e os outros executivos de linha de negócios entenderem, mas espera-se que seja a tendência geral nos próximos anos, conforme o volume de desenvolvimento e o risco continuam aumentando.



> *“O CISO moderno deve pensar em múltiplas dimensões: como tecnólogo, comunicador, investigador, psicólogo, investidor e negociador. Ele precisa alinhar a segurança com a estratégia de negócios, abordar os incidentes como oportunidades e reestruturar a maneira como a equipe trabalha.”*

Akhilesh Tuteja
Sócio-líder global de Cyber Security da KPMG na Índia

Algumas ações fundamentais a serem consideradas para 2022

1. Mudar a mentalidade de segurança tradicional em torno da confidencialidade e disponibilidade de dados e começar a refletir sobre como se esforçar para assegurar a integridade e a resiliência.

2. Envolver os principais públicos de interesse organizacionais para que se comprometam com uma estratégia de segurança que pode proteger dados organizacionais e de clientes, gerenciar riscos e ser sensível às prioridades de negócios de curto e longo prazo.

3. Reformular a mentalidade no alto escalão no que tange à segurança, concentrando-se no risco empresarial prático e não na despesa e velocidade.

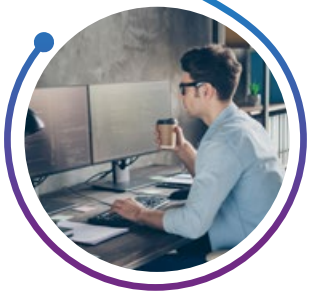
4. Pensar menos nos indicadores-chave de desempenho operacional (KPIs) e nos indicadores-chave de risco (KRIs) e se concentrar mais nos temas e tendências dos dados subjacentes: tipos de incidentes, lacunas nos programas internos e externos e atividades relacionadas a dados que estão em andamento, planejadas ou aguardando aprovação.

5. Construir relacionamentos com as principais áreas de negócios, aumentando a conscientização sobre a rapidez com que elas podem atingir os objetivos incorporando a segurança *versus* o que podem perder no caso de uma violação.

Saiba mais

Incluir a segurança cibernética no DNA da empresa
Os CISOs devem incorporar a segurança cibernética ao negócio — tornando-a uma responsabilidade de todos.

Proteger a nova realidade dos negócios
Os CEOs globais enfrentam seus medos e riscos de segurança cibernética.



Acabar com a ilusão da segurança cibernética
Porque a confiança é mais importante do que nunca.

Fator-chave 2

Atingir o fator-chave: talentos e conjuntos de habilidades críticos

Transformar a equipe de segurança cibernética: de executora a influenciadora.

Está se tornando cada vez mais aparente que os programas de segurança modernos, liderados por equipes de segurança com visão de futuro, capacitam as organizações a atuar com agilidade, buscar o crescimento e atender melhor os clientes. As estratégias e ferramentas de segurança cibernética representam a verificação constante, que possibilita que desenvolvedores e líderes de negócios atuem acompanhando o conhecimento que seus aliados de segurança aportam — algumas vezes pessoalmente, mas cada vez mais por meios automatizados.

Conforme o cenário de ameaças evolui, a abordagem da equipe cibernética está mudando

Talvez a maior mudança observada, em termos do relacionamento da equipe de segurança com o restante da organização — certamente na era da covid-19, mas mesmo retrocedendo vários anos antes do início da pandemia — é uma necessidade crescente de rapidez no lançamento de produtos e serviços no mercado, embora com um reconhecimento dos riscos envolvidos.

Com a pandemia em andamento, as organizações estão chegando a um ponto em que se espera que elas gerenciem uma maior presença digital e um ciclo de mudanças, enquanto continuam melhorando os recursos de segurança. Isso, por sua vez, impulsionou a transição para uma abordagem de *secure-by-design*, a necessidade de operacionalizar o desenvolvimento, a segurança e as operações (DevSecOps) e a transição fundamental da segurança ao longo do ciclo de vida de desenvolvimento de software (*Software Development Life Cycle* - SDLC).

Pensando na composição de um programa cibernético eficaz, há um elemento de liderança e um elemento de equipe. Em termos de liderança, os CISOs mais eficazes não passam muito tempo falando sobre tecnologia. Em vez disso, eles refletem mais e falam sobre a direção futura dos negócios, esforçando-se para garantir que os altos executivos e a sala de diretoria estejam cientes e alinhados com o plano de segurança, e vice-versa.

Falar sobre *firewalls*, gerenciamento de patches e prevenção contra perda de dados — apesar de todas as considerações críticas — faz os profissionais não relacionados à segurança pensarem. Cada vez mais, os CISOs e suas equipes estão entendendo e falando a linguagem do negócio. Eles devem comunicar como o programa de segurança cibernética da organização apoia e contribui para o crescimento dos resultados financeiros.

Quanto à equipe mais ampla, atualmente vemos um desemprego essencialmente negativo no espaço cibernético. Além da escassez de profissionais experientes para preencher todas as funções necessárias, as pessoas tendem a se movimentar nesse setor, uma vez que buscam experiências diferentes para fortalecer as habilidades existentes e adquirir novas competências.

De maneira mais ampla, há uma explosão da *gig economy*, onde parece que todos são subcontratados. Nos próximos anos, as equipes cibernéticas podem ter acesso a um conjunto de recursos confiáveis, de acordo

> *Como Mike Tyson celebremente afirmou, "Todos têm um plano até levar um soco na boca [1]". Um evento cibernético pode ser assim. As equipes cibernéticas precisam estar prontas para se levantar e responder de maneira fundamentada, estratégica e calculada.*
>
> **Fred Rica**
> Sócio-líder de Cyber Security Services da KPMG nos EUA

[1] BERARDINO, Mike. *Mike Tyson explains one of his most famous quotes.* South Florida Sun-Sentinel, 2012.

com as cargas de trabalho e a capacidade. Isso permitiria aos CISOs formarem equipes para atuar com um núcleo menor e mais estratégico, que pode ser ampliado e diminuído conforme necessário. A nuance desse modelo é a confiança. Deve haver uma avaliação de especialistas cibernéticos por outros profissionais confiáveis, dentro ou fora da organização, e que poderão assumir projetos confidenciais de segurança cibernética.

Essa mudança de mentalidade é o que está transformando a postura dos CISOs e de suas equipes de executores para influenciadores.

Qual é o seu plano?

A evolução da equipe de segurança envolve tanto a troca de mensagens quanto o design do programa. Os CISOs precisam mudar a narrativa, para que os desenvolvedores e as linhas de negócios aceitem o fato de que a equipe cibernética está lá para ajudar, e não para atrapalhar. Essa é uma mensagem simples, mas importante, que muitas vezes é esquecida ou não é bem transmitida.

De senhas e PINs à autenticação de dois fatores e treinamento de conscientização de segurança, os funcionários terão reclamações e as equipes cibernéticas devem dedicar algum tempo para ouvi-las, ser empáticas e inspiradoras. Elas devem comunicar claramente a importância de atuar com segurança e proteção em todos os aspectos do trabalho e de conectar o cumprimento — e o não cumprimento — das orientações com os resultados financeiros e a visão de futuro da organização.

As equipes devem trabalhar para mudar a percepção desses requisitos de punição para responsabilidade. Procurar maneiras de tornar a conscientização cibernética mais envolvente, interativa, divertida, e até mesmo semelhante a um jogo, talvez por meio da realidade aumentada (RA) ou da realidade virtual (RV). As equipes precisam deixar claro que o espaço cibernético não existe para ser um obstáculo, mas para manter todos seguros — e elas podem fazer isso simultaneamente.

Os CISOs devem analisar criticamente onde eles e a equipe cibernética gastam seu tempo, questionando o equilíbrio entre a estratégia, o planejamento, a construção e a execução (incluindo a reação). No espaço cibernético, é fácil se distrair com a tecnologia. No entanto, quando as equipes se concentram nos seus planos e princípios, as decisões tecnológicas tendem a se tornar um pouco mais óbvias.

A oportunidade está na combinação de automação, análise de dados e IA, especificamente ML, em um modelo de monitoramento de controles contínuo. Essa estrutura fundamenta os aspectos da ciência de dados dos sistemas de suporte à decisão e alinha os resultados cibernéticos em tempo real com o perfil de risco da organização e as atividades de resposta. O objetivo é capturar e analisar dados em tempo real com uma postura de segurança padronizada e dinâmica capaz de detectar e responder a uma mudança no cenário de ameaças ao vivo.

Os CISOs e suas equipes devem estar preparados para disrupções contínuas. Do ponto de vista da tecnologia, a segurança cibernética é a guardiã de um ecossistema digital mais amplo de vendedores, fornecedores e parceiros interconectados. Gerenciar esse ecossistema e se esforçar para garantir que ele seja seguro é um dos maiores desafios que as equipes de segurança cibernética enfrentam.

De maneira geral, os profissionais de segurança cibernética devem continuar desenvolvendo suas habilidades em uma direção de negócios mais estratégica e baseada em sistemas. Eles precisam adotar uma filosofia multimodal focada na padronização, automação e análise de dados. Como uma indústria, as equipes cibernéticas não devem apenas buscar atrair mais talentos em um sentido absoluto, mas estar abertas a uma gama mais diversa de talentos, quebrando as barreiras para a inclusão.

As organizações entraram em uma espécie de corrida armamentista de automação no espaço cibernético. Para se antecipar a isso, as equipes cibernéticas devem desenvolver uma mentalidade realista baseada em cenários para as ameaças que possam surgir de diversos setores e geografias.”

Matt O’Keefe
Sócio-líder de Cyber Security da região Ásia-Pacífico da KPMG na Austrália

Algumas ações fundamentais a serem consideradas para 2022

1. Mudar a narrativa. Parar de falar sobre tecnologia e começar a falar sobre negócios.
2. Não se limitar à definição tradicional de segurança cibernética; continuar estabelecendo relacionamentos com outras áreas da organização e construir uma rede de parceiros de negócios internos.
3. Incorporar a mentalidade de cenários, teste e capacidade de resposta às atividades regulares da função cibernética de uma organização.
4. Tornar o cumprimento das ações um resultado importante do seu programa de segurança, mais do que a razão de sua existência.
5. Ser um disseminador, ser apaixonado pelo que faz e motivador das pessoas em torno da importância da segurança.
6. Adotar a postura de que a segurança cibernética é uma parte importante do que a empresa faz, pois está no DNA da empresa. Ajudar a organização a mudar sua mentalidade sobre o papel da segurança.

Saiba mais

Formar os profissionais de segurança cibernética futuros
Combine a terceirização, trabalhadores da *gig economy* e automação para transformar o acesso às capacidades e aos recursos.

***Firewall* humano**
Superando o fator de risco humano na segurança cibernética.

Explorar a cultura ágil da equipe
Quatro estratégias para construir uma cultura de segurança responsável.

Fator-chave 3

Adaptar a segurança para a nuvem

Aumentar a segurança da nuvem por meio da automação — da implementação e monitoramento à remediação.

A segurança cibernética e a segurança em nuvem estão se tornando sinônimos. A única diferença é o ambiente de implementação. Todos os princípios sobre os quais os CISOs falaram durante anos — proteção de dados, gerenciamento de identidades e de acesso, gerenciamento da infraestrutura e das vulnerabilidades — são aplicáveis à segurança em nuvem. O que muda é o ambiente tecnológico. O local em que esses controles de segurança são implementados exige automação extrema, da implementação ao monitoramento e correção. O "o quê" e o "por quê" não mudaram muito, mas o "onde" e o "como" certamente mudaram.

Segurança na nuvem na era da transformação digital

Embora a transformação digital impulsione a adoção e o uso da nuvem, ela também coloca as instituições e empresas em maior risco cibernético. A falta de habilidades de segurança em nuvem significa que o negócio de proteção da organização atua com um déficit de confiança distinto. A nuvem pode estar em toda parte, assim como os *hackers* e outros criminosos.

Conforme a adoção da nuvem aumentou, o cenário mudou. O ambiente de nuvem exige maior dependência da automação, desde a implementação até o monitoramento e remediação. A intervenção manual cria níveis mais altos de relatórios de incidentes com base em configurações incorretas internas. De fato, de acordo com uma pesquisa da Aqua Security, 90% das organizações são vulneráveis a violações de segurança atribuídas a configurações incorretas da nuvem[2].

Em muitas empresas, a expectativa de que a equipe de desenvolvimento de nuvem também atue como equipe de engenharia de segurança pode ser observada. Isso não é realista ou sustentável de uma maneira eficaz. O ideal é que os engenheiros de segurança sejam grandes especialistas no assunto nessa disciplina crítica e tenham uma perspectiva relevante sobre a estrutura básica e as necessidades do ambiente de nuvem. Da mesma forma, os desenvolvedores de nuvem devem estar familiarizados com a função da segurança, mas passam a maior parte do tempo projetando sistemas, programando, analisando e mantendo o ambiente virtual. Certamente, as organizações devem esperar que os desenvolvedores de nuvem incorporem a segurança nos seus produtos em um grau muito maior, mas as equipes de desenvolvimento nunca devem ser a barreira de segurança.

Além disso, o conjunto de habilidades consistente com um roteiro de segurança tradicional não é necessariamente adequado para implementações e segurança em nuvem. É mais fácil para um desenvolvedor nativo da nuvem se atualizar sobre as práticas de segurança do que um profissional de segurança treinado da maneira tradicional entender as nuances do desenvolvimento da nuvem. No mundo atual, o código aberto, a infraestrutura como código e as ferramentas correspondentes para provisionar infraestrutura em nuvem são essenciais para todos os tipos de ambientes em nuvem.

> *O conjunto de habilidades fundamental para a nuvem e segurança em nuvem é o conjunto de habilidades do desenvolvedor — a capacidade de programar, elaborar os* scripts *e entender como o DevOps funciona. Ensinar os profissionais com essa perspectiva os princípios da segurança, em vez de ensinar os profissionais de segurança sobre como programar, é uma estratégia mais eficaz.*
>
> **Steve Barlock**
> Sócio-líder de Cyber Security Services da KPMG nos EUA

[2] AQUA SECURITY. *2021 Cloud Security Report: Cloud Configuration Risks Exposed.* 2021.

Qual é o seu plano?

Quando se trata de segurança, as transformações da nuvem devem priorizar uma ampla gama de fatores regulatórios e contratuais. Em termos de regulamentação, a verdadeira sopa de letrinhas de normas — o Regulamento Geral de Proteção de Dados (*General Data Protection Regulation* - GDPR), a Lei de Portabilidade e Responsabilidade de Seguro Saúde (*Health Insurance Portability and Accountability Act* - HIPAA), a Diretiva sobre Segurança de Rede e Sistemas de Informação (*Directive on Security of Network and Information Systems* - Diretiva NIS), as Normas de Segurança de Dados do Setor de Cartões de Pagamento (*Payment Card Industry Data Security Standards* - PCI DSS) etc. — continuam gerando complexidade para o cumprimento da segurança e devem ser prioridade.

Nesse ambiente, as equipes de segurança são incentivadas a adicionar o gerenciamento da postura de segurança na nuvem (CSPM) à sua caixa de ferramentas. Essa classe automatizada de dispositivos oferece verificações de políticas pré-configuradas, mapeadas para regimes regulatórios específicos, para ajudar a identificar problemas de configuração incorreta relacionados à nuvem e riscos de conformidade. Com o simples clique de um botão, possíveis configurações incorretas podem ser verificadas e identificadas.

No lado contratual, tanto os fornecedores de nuvem quanto as empresas que usam seus serviços estão firmando acordos de responsabilidade compartilhada que muitas vezes são mal interpretados, especialmente do lado do cliente. Consequentemente, a propriedade da segurança da nuvem *versus* a segurança *dentro* da nuvem pode ser um conceito obscuro. Essa questão torna-se ainda mais complexa ao se analisar a plataforma, infraestrutura e *software* como um serviço. As equipes de segurança organizacional devem promover a visão de que todos os dados armazenados na nuvem são de responsabilidade da organização. Com base nisso, os dados precisam ser criptografados (quando apropriado, é claro) e protegidos com os controles relevantes.

Os CISOs e suas equipes são incentivados a trabalhar com parceiros de negócios para ajudar a garantir que todos entendam os requisitos de segurança específicos da nuvem e colaborem com o provedor para evitar configurações incorretas. As organizações que adotam essa abordagem e buscam se manter informadas sobre os clientes da nuvem podem alcançar resultados positivos.

É possível pensar nisso também como um modelo subtrativo. Isso significa que, conforme há a transição da infraestrutura como serviço (*Infrastructure as a Service* - IaaS) para o *software* como serviço (*Software as a Service* - SaaS), a equipe de segurança é cada vez menos pela propriedade da segurança. De qualquer maneira, com o ritmo acelerado de migração para a nuvem, as empresas devem estar prontas para proteger seus próprios dados baseados em nuvem, especialmente por meio de ferramentas e protocolos de automação, em todos os tipos de relações contratuais.

Para ajudar a assegurar que as implementações em nuvem apresentem o nível correto de segurança e se adequem à sua organização e ao seu perfil de risco, com muitos recursos e funcionalidades, uma forte recomendação é montar uma equipe de segurança em nuvem dedicada, que seja centralizada sob uma perspectiva de governança e distribuída em toda a organização, conforme apropriado. Uma vez que a estrutura e as habilidades estão estabelecidas com segurança, essa equipe pode ser distribuída ou alinhada com unidades de negócios específicas. Continue automatizando tudo o que puder, conforme apropriado, especialmente nas áreas de implementação, monitoramento e remediação.

> *"O conjunto de habilidades fundamental para a nuvem e segurança em nuvem é o conjunto de habilidades do desenvolvedor — a capacidade de programar, elaborar os* scripts *e entender como o DevOps funciona. Ensinar os profissionais com essa perspectiva os princípios da segurança, em vez de ensinar os profissionais de segurança sobre como programar, é uma estratégia mais eficaz."*
>
> **Andreas Tomek**
> Sócio-líder global de Cloud Security da KPMG na Áustria

Algumas ações fundamentais a serem consideradas para 2022

1. Automatizar a segurança em nuvem, especialmente em relação à implementação, monitoramento e recuperação, eliminando processos manuais.
2. Montar uma equipe de segurança em nuvem centralizada, proveniente das áreas de desenvolvimento, em vez de liderar com as habilidades de segurança tradicionais.
3. Estabelecer as responsabilidades operacionais em um modelo compartilhado, definindo qual entidade é responsável pela segurança em nuvem e qual é responsável pela segurança da nuvem.
4. Procurar ferramentas de gerenciamento de segurança que tenham verificações de políticas pré-configuradas e mapeadas para diferentes regimes regulatórios.
5. Construir um processo de resposta a incidentes que esteja em sintonia com a estratégia em nuvem mais ampla.

Saiba mais

Proteger a nuvem — o próximo capítulo
Como as soluções atuais baseadas em nuvem estão revelando benefícios e ameaças potenciais para os negócios.

Você é pragmático do ponto de vista cibernético?
Adotando uma nova abordagem para a proteção dos negócios no mundo pós-pandemia.

Proteção de dados na nuvem
Habilitando recursos de proteção de dados escaláveis.

Fator-chave 4

Colocar a identidade no centro do modelo *Zero Trust* (confiança zero)

Coloque a gestão de identidade e acesso (*Identity and Access Management* - IAM) e o modelo *Zero Trust* para funcionar no local de trabalho hiperconectado de hoje.

Com dezenas de milhões de funcionários trabalhando nas suas mesas de cozinha e nos seus *home offices*, e bilhões de consumidores comprando produtos nos seus celulares de qualquer lugar, proteger dados essenciais e outras informações confidenciais em um ecossistema complexo de fornecedores e aliados nunca foi tão essencial. Em um ambiente em que os criminosos cibernéticos geralmente estão a apenas um clique de distância, as organizações devem adotar uma arquitetura e uma mentalidade de *Zero Trust*, com o gerenciamento de identidades e de acessos no centro de tudo.

A demanda por experiências sem atritos

O ritmo explosivo da transformação digital entre empresas de capital aberto e fechado — especialmente durante a pandemia — além de uma estrutura de trabalho remoto que se normaliza rapidamente, oferece uma janela de oportunidades aos invasores. Consequentemente, houve um número sem precedentes de ataques cibernéticos nos últimos meses, especialmente eventos de *ransomware* e ataques à cadeia de suprimentos. Os modelos atuais de gestão de identidade e acesso (*Identity and Access Management* - IAM), originalmente desenvolvidos para gerenciar identidades digitais e o acesso do usuário para organizações individuais, atualmente estão sendo reconfigurados para oferecer o nível adequado de resiliência, além de fornecer recursos de autenticação essenciais para ambientes de computação governamentais, privados, públicos ou *multi-cloud*.

Cada vez mais, clientes, fornecedores e usuários corporativos esperam experiências transparentes, livres de senhas em constante mudança e várias camadas de identificação digital. Ecossistemas ampliados de terceirizados, subcontratados e trabalhadores da *gig economy* — todos eles extensões da força de trabalho de uma empresa — exigem acesso em momentos diferentes em níveis distintos de dados corporativos confidenciais. Infelizmente, a falta de processos específicos para esses participantes mutas vezes resulta em violações significativas na cadeia de segurança.

A linha entre a segurança *business-to-consumer* (B2C) e *business-to-business* (B2B) continua tênue, com as empresas se afastando de políticas distintas de segurança. Em vez disso, as organizações estão, em muitos casos, mesclando os dois em suas abordagens de gerenciamento de autenticação. Conforme a tecnologia de segurança amadurece, pode haver uma ampla mudança para a prova de identidade e autenticação sem senha, não apenas para consumidores, mas também para empresas. É provável que a escalabilidade seja um problema, considerando o número absoluto de clientes B2C e B2B em relação aos profissionais de segurança cibernética corporativos.

Como uma abordagem automatizada que pode ajudar a eliminar processos manuais onerosos e complicados, reduzir os ataques de um ambiente e estabelecer políticas e princípios cibernéticos adequados à finalidade da empresa, o modelo de segurança de *Zero Trust* está cada vez mais sendo visto como uma perspectiva de segurança viável no mundo pós-pandemia. Com a identidade na sua base, o modelo de *Zero Trust* permite que as organizações avaliem se um usuário está devidamente autenticado, isolem o recurso que o usuário está tentando acessar, determinem se a solicitação é proveniente de um dispositivo confiável, roubado ou de terceiros e decidam com segurança se o acesso deve ou não ser concedido.

> *A arquitetura e o modelo de* Zero Trust *não podem ter sucesso sem que a identidade esteja no centro. Desenvolva seu roteiro de* Zero Trust *em torno da identidade para facilitar a sua adoção e fortalecer o ROI* (Return Over Investment).

Deepak Mathur
Diretor de Cyber Security Services da KPMG nos EUA

O surgimento do modelo *Zero Trust* representa uma mudança de mentalidade, na qual a equipe cibernética assume o compromisso em relação ao acesso ao sistema e toma decisões com base na identidade, dispositivo, dados e contexto. Com os usuários exigindo acesso cada vez mais rápido e estruturas centradas em nuvem ampliando a abrangência das invasões, as soluções e recursos de segurança existentes podem não ser suficientes para proteger os dados de maneira adequada enquanto eles trafegam pela rede.

Qual é o seu plano?

Para enfrentar os riscos crescentes de acesso e identidade que continuam desestabilizando as organizações financeira e operacionalmente, além de responder a um ambiente regulatório ampliado, as empresas e instituições devem considerar novos padrões, ferramentas e estratégias para proteger melhor seus sistemas, dados e infraestrutura.

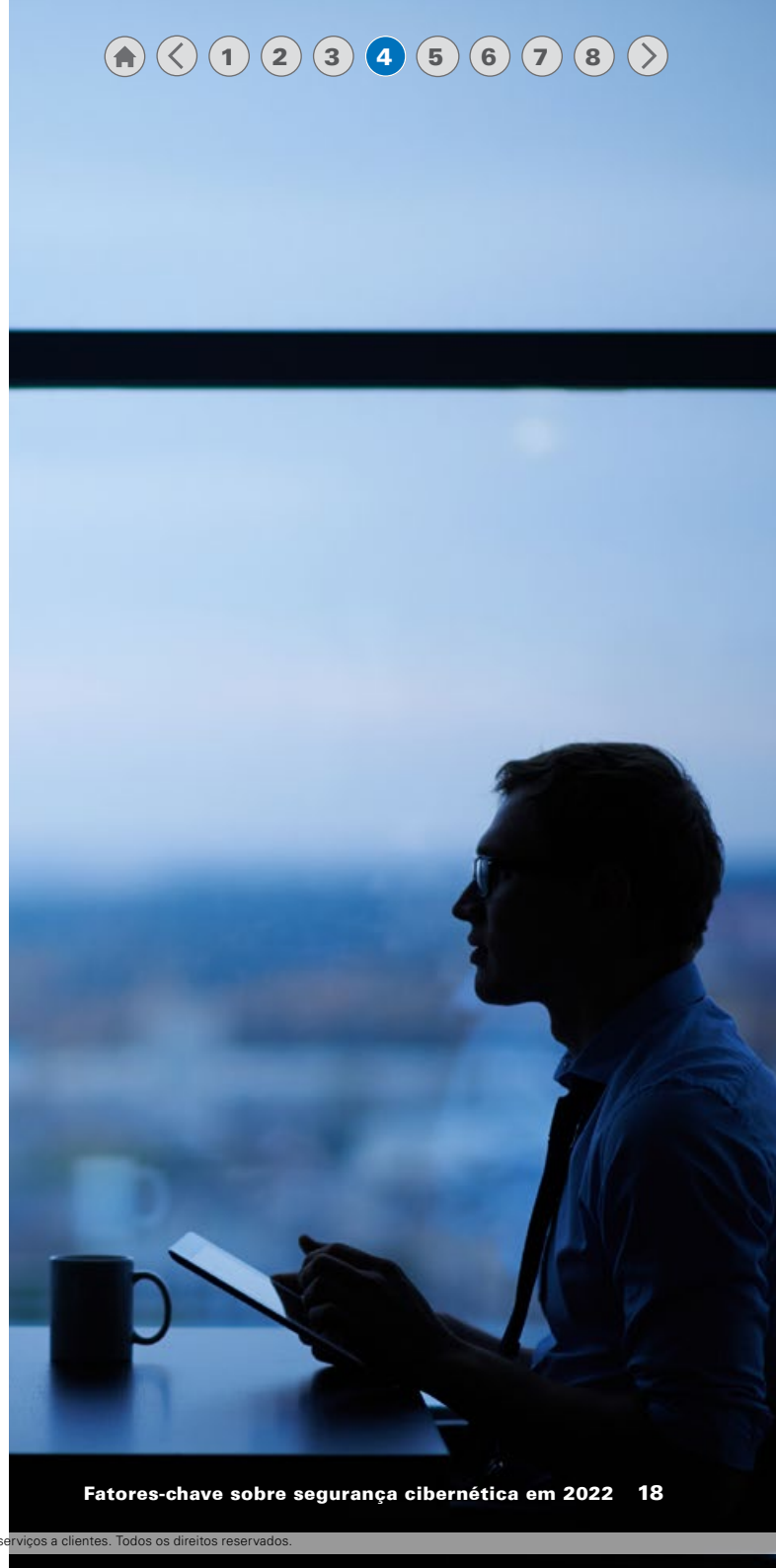
Em um ambiente de negócios pós-pandemia em que muitos, senão a maioria, dos trabalhadores trabalham de forma remota, soluções provisórias e correções temporárias provavelmente não conseguirão acompanhar o ritmo e a virulência dos ataques cibernéticos e das ameaças que já bombardeiam empresas e agências governamentais. Em breve, os usuários provavelmente não precisarão mais estar na rede (ou seja, em uma conexão de rede virtual privada [VPN] persistente). Espera-se que o acesso condicional venha da confiança e garantia geradas pelos dispositivos que as pessoas utilizam e pelos processos de autenticação e decisão implementados pelas organizações.

O conceito de *Zero Trust* é um ponto de interesse crescente, mas muitos CISOs — e, mais ainda, os CIOs e diretores de infraestrutura — devem continuar trabalhando em direção aos meios mais eficazes para implementar uma arquitetura de *Zero Trust* em toda a organização e um conjunto de princípios que se alinham com as prioridades de negócios e operacionais. Além disso, certamente, tudo isso deve ser considerado dentro do contexto da segurança cibernética global, gerenciamento de riscos e programas de tecnologia da organização.

O princípio do menor privilégio é talvez uma das ideias mais simples relacionadas à forma como os dados são protegidos; no entanto, ela também é uma das mais importantes. A ideia geral é que os usuários, processos, cargas de trabalho e aplicativos devem receber apenas o menor nível de direitos de acesso aos recursos do sistema necessários para cumprir sua função. Por exemplo, os *web designers* não precisam de acesso a registros financeiros, e os indivíduos responsáveis por atualizar as listas de produtos não precisam de direitos de administrador. As organizações devem continuar enxergando o princípio de acesso de menor privilégio como um elemento central do modelo de *Zero Trust*.

> *O modelo* Zero Trust *não é um recurso, não é uma tecnologia, não é uma norma. É uma abordagem e uma estrutura de segurança, com a identidade como um componente fundamental.*

Jim Wilhelm
Sócio-líder global de IAM da KPMG nos EUA



Algumas ações fundamentais a serem consideradas para 2022

1. Testar ou começar a ter uma estratégia em torno da autenticação sem senha para casos de uso selecionados.
2. Certificar-se de que o seu programa de identidades tenha uma base sólida de dados e análises.
3. Incorporar uma mentalidade de *Zero Trust* na sua estratégia de segurança cibernética global.
4. Comprometer-se a criar uma experiência sem atritos para melhorar a experiência do usuário e do cliente, simplificando a autenticação e o gerenciamento de identidades.
5. Automatizar a funcionalidade de segurança para possibilitar que profissionais altamente qualificados se concentrem nas atividades mais estratégicas.
6. Aceitar que a adoção de uma abordagem de *Zero Trust* é uma jornada de longo prazo para implementação.

Saiba mais

A autenticação é um facilitador futuro?
Porque precisamos da autenticação contínua para a infraestrutura digital.

Todos podem adotar o modelo *Zero Trust*
O modelo de segurança cibernética sem limites é um projeto promissor para o ambiente de ameaças em evolução.

Atingindo a eficiência de custos no gerenciamento de identidades e de acesso
Uma perspectiva estratégica para abordar a IAM, com automação e dimensionamento corretos da sua organização, pode ajudar a reduzir os custos operacionais.

Fator-chave 5

Explorar a automação da segurança

Obtenha vantagem competitiva por meio da implementação inteligente de automação da segurança.

Embora muitos considerem a automação uma panaceia universal, a experiência mostra que os melhores resultados são decorrentes de uma abordagem de aplicação pragmática. Alguns dos maiores benefícios potenciais da automação surgem quando há um foco em implementações projetadas para ajudar a resolver problemas de negócios: aumentar a disponibilidade dos profissionais ao gerir tarefas do cotidiano de maneira mais eficiente; conquistar vantagem competitiva em áreas em que a velocidade é importante; e analisar grandes conjuntos de dados, muitas vezes não estruturados. Em um mundo hiperconectado com uma infinidade de ferramentas disponíveis, as organizações devem estar prontas para o futuro, pois o cenário de ameaças e a complexidade continuam aumentando.

Entenda o valor do negócio

As empresas estão automatizando a função de segurança com sucesso e liberando profisionais para outras atividades ao aplicar a automação a tarefas rotineiras e repetitivas. Trabalhos que antes eram realizados por profissionais altamente treinados, como a varredura de vulnerabilidades, análise de registros (*logs*) e *compliance*, estão agora sendo padronizados e realizados automaticamente. Isso pode aumentar a produtividade do analista, acelerar a detecção de incidentes e os tempos de reação, além de oferecer uma oportunidade de escalabilidade. Automatizar as ameaças de nível inferior e transações de rotina melhora o centro de operações de segurança, permitindo a priorização de tarefas de maneira mais eficaz e uma resposta mais rápida a ameaças que exigem intervenção humana.

Em situações em que os conjuntos de dados são muito grandes ou complexos para análise direta, a automação foi testada como sendo extremamente valiosa, e já está sendo aplicada em muitos setores para revelar elos e padrões difíceis de identificar. A automação também está sendo utilizada com eficácia para tarefas que se beneficiam do aumento da velocidade, como a identificação de incidentes de segurança em dados de registros volumosos e a realização de descobertas de dados muito numerosos, em que a análise de arquivos individuais costuma ser ineficiente.

De uma perspectiva de DevOps, a automação de segurança deverá ser construída em cada ponto crítico de interseção no SDLC, de histórias de usuários e análises de código seguro à modelagem de ameaças e análises de *design* seguro com a ajuda de produtos de testes de segurança de aplicativos estáticos e dinâmicos (SAST e DAST). Com isso em mente, o DevSecOps está ganhando impulso em resposta à necessidade de segurança rigorosa que se move na velocidade da entrega em nuvem.

Com a migração para a nuvem, as organizações não têm controle consistente sobre as versões de *software* e os recursos gerais disponíveis no ambiente de nuvem. A automação tem sido uma parte integrante da avaliação segura do risco e da adoção de novos recursos de linha de base, conforme necessário. Em ambientes com várias nuvens, a exposição não intencional de dados, permissões de contas mal gerenciadas, conexões de rede inseguras, ataques de *ransomware* e outros riscos são as principais preocupações das organizações. As estruturas de segurança automatizadas podem fornecer melhor visibilidade e controle.

> *A maturidade crescente dos recursos de automação cibernética torna-os um componente fundamental da estratégia de segurança cibernética. As organizações devem buscar oportunidades de aproveitar a automação para deslocar tarefas manuais repetidas, aumentar a inteligência para os analistas, reduzir a latência de processos complexos e ajudar a obter a escala e velocidade necessárias para proteger ativos críticos.”*

Matthew Miller
Sócio-líder de Cyber Security Services da KPMG nos EUA

Qual é o seu plano?

Comece com o básico e identifique os casos de uso de automação de que a sua organização realmente precisa e com os quais conseguirá gerar valor para os negócios. Embora seja prudente implementar a arquitetura de segurança corporativa integrada, mantenha-a simples e não realize uma engenharia complexa nas soluções. Temendo perder a última tendência, as empresas podem entrar em uma onda de compras, adquirindo várias ferramentas que muitas vezes não são utilizadas por falta de funcionários experientes.
Resista a esse impulso.

Observe primeiro o seu cenário tecnológico atual. Há uma enorme quantidade de recursos avançados de automação nas ferramentas atuais e, muitas vezes, não é necessário olhar para fora da sua organização. Da mesma forma, procure colegas com experiência em automação e considere torná-los parte da equipe cibernética. É mais fácil recrutar alguém que tem experiência anterior com automação de processamento robótico (*Robotic Processing Automation* - RPA) de outras áreas da empresa ou de um empregador anterior, e ensiná-lo a aplicá-la dentro do cenário cibernético, do que contratar alguém que tenha credenciais cibernéticas básicas e ensinar a RPA a ele.

As equipes de segurança cibernética estão cada vez mais sobrecarregadas com cargas de trabalho maiores. É uma jogada inteligente usar ferramentas de maneira sensata em termos de automação de parte do gerenciamento de incidentes de nível 1 ou de baixo nível, para que haja tempo suficiente para dedicação a problemas que exigem uma mentalidade mais diferenciada ou criativa.

Em vez de ter uma equipe de segurança separada para identificar vulnerabilidades e violações, a automação da segurança deve mudar e estar presente em todos os pontos de interseção críticos no SDLC, de histórias de usuários e revisões de código seguro à modelagem de ameaças e revisões de projeto seguras. Use produtos como testes de segurança de aplicativos estáticos e dinâmicos que se integram de maneira transparente ao fluxo de integração/entrega contínua (*Continuous Integration/Continuous Delivery* - CICD), tornando menos desafiador incorporar segurança em todo o SDLC.

> Algumas tecnologias, como a resposta de automação de orquestração de segurança *(Security Orchestration Automation Response* - SOAR), são inerentemente complementares, destinadas não a substituir os analistas humanos, mas a aumentar suas habilidades e fluxos de trabalho para uma melhor experiência do funcionário.

Shreyashi Sengupta
Sócio de Confiança Digital da KPMG na Índia

Algumas ações fundamentais a serem consideradas para 2022

1. Adotar uma abordagem proativa para a automação da segurança, concentrando-se nas ameaças ao invés dos incidentes.
2. Automatizar as tarefas cotidianas para liberar os profissionais e capacidade cognitiva para as atividades mais importantes.
3. Aproveitar a tecnologia existente e os especialistas em automação na sua organização.
4. Construir a automação de segurança em cada ponto crítico de interseção dentro do SDLC.
5. Ampliar os limites do que já é possível — estar disposto a falhar, mas aprender rapidamente e implementar esse *insight*.
6. Manter a simplicidade e não realizar uma engenharia complexa de soluções ou adquirir ferramentas de automação que não atendam ao problema ou gerem valor para a empresa.

Saiba mais

Adotar a automação como a estrela em ascensão
Trazendo diversos benefícios esperados de eficiência e força de trabalho.

Segurança ágil em DevOps na nuvem
Uma abordagem futura para a segurança e desenvolvimento de *softwares*.

Monitoramento da segurança para fluxos de desenvolvimento de *software*
Primeiros passos para aumentar a confiança na integridade do seu ambiente de desenvolvimento.

Fator-chave 6

Proteger a fronteira da privacidade

Migrar para uma abordagem multidisciplinar de gerenciamento de risco de privacidade que incorpore os conceitos de *privacy by design* e *security by design*.

Em muitas empresas, a segurança cibernética e a privacidade de dados são vistas como disciplinas diferentes que costumam funcionar em áreas separadas. Em um ambiente em que tantos dados confidenciais são capturados e utilizados, a revisão de terceiros, novos sistemas e novos aplicativos exige uma abordagem multidisciplinar para o gerenciamento de risco de privacidade — que inclui a privacidade e segurança desde a fase de *design* até a gestão da mudança organizacional.

Mantenha os direitos individuais em mente

Atualmente, há conscientização e reconhecimento mais globais dos direitos individuais em relação às informações pessoais. Com a profusão de regulamentações ao redor do mundo, do GDPR na Europa a vários regimes individuais na Ásia, América do Norte e do Sul — notadamente a Lei Geral de Proteção de Dados do Brasil (LGPD), a Lei de Privacidade do Consumidor da Califórnia (*California Consumer Privacy Act* - CCPA) e outras leis estaduais emergentes dos EUA, além das leis federais e municipais em vigor no Canadá — o foco nos direitos de dados, privacidade e segurança está mais claro do que nunca.

A evolução do ambiente regulatório pode ser vista em relação à privacidade de dados praticamente em tempo real. Governos e órgãos reguladores estão reconhecendo que os incidentes de privacidade resultantes de invasões são apenas uma parte do universo mais amplo de incidentes cibernéticos. Além disso, eles estão exigindo que as organizações divulguem as violações muito mais cedo e de maneira muito mais transparente, independentemente de terem afetado a privacidade dos cidadãos ou não.

A maioria das jurisdições em todo o mundo atualmente tem obrigação de reportar violações, de maneira que não há como atuar sem cumprir as exigências legais, com órgãos reguladores da indústria e outros não específicos de privacidade agora tendo um interesse real no tema e implementando obrigações similares. Essa é uma grande mudança em relação a apenas alguns anos atrás, antes do GDPR, quando havia pouco mais do que uma colcha de retalhos de regras e regulamentos em todo o mundo.

Há uma harmonia praticamente universal no sentido de que tantos países e territórios implementaram regras e regulamentações de privacidade baseadas em direitos que visam capacitar o indivíduo e devolver-lhe o controle que ele abdicou ao compartilhar suas informações pessoais. No entanto, com tantas regulamentações diferentes, o cenário regulamentar está se tornando cada vez mais difícil de ser cumprido, especialmente para empresas globais que atuam em várias jurisdições.

A automação é fundamental, especialmente para organizações que não têm a capacidade e os recursos para gerenciar áreas como identificação e relatórios de riscos à privacidade. As empresas ficam em desvantagem se não tiverem, por exemplo, processos de IAM automatizados e apoiados por um gerenciamento de metadados eficaz. Em um mundo virtual, sem controles automatizados incorporados nos processos cotidianos — incluindo a automação de solicitações de acesso por assunto — a maioria das organizações simplesmente não terá pessoal suficiente para supervisionar novos servidores, armazenamento de dados e aplicativos manualmente de uma maneira eficiente e eficaz.

> *Os programas de privacidade do futuro devem incorporar a mentalidade de* privacy-by-design, *que não é apenas uma filosofia, é uma mentalidade cultural e uma mudança organizacional, uma vez que a privacidade não é uma disciplina jurídica independente, mas sim uma abordagem multifacetada à proteção de dados, que inclui engenharia de privacidade, segurança cibernética, tecnologia e gerenciamento de risco.*
>
> **Sylvia Klasovec Kingsmill**
> Sócia-líder global de Privacidade da KPMG na Austrália

É fundamental assegurar o consentimento explícito de qualquer indivíduo ou entidade durante ou antes da coleta de dados. Por sua vez, os clientes precisam sinalizar que entendem a finalidade da coleta e o que será feito com suas informações. Ser sempre totalmente transparente promoverá a confiança e ajudará a evitar quaisquer problemas éticos de tratamento de dados.”

Matthew Quick
Diretor de Technology Risk
e Cyber Security da KPMG
na Austrália

Qual é o seu plano?

Manter os dados individuais seguros e levar a privacidade a sério é mais do que apenas implementar novos processos para atender aos requisitos regulamentares — é uma mudança cultural. Assim como a segurança, as organizações devem adotar uma mentalidade de *privacy-first* ou *privacy-by-design*. Incorporar a privacidade e segurança na mudança organizacional, cultura, processos, tecnologia e produtos é um bom ponto de partida e provavelmente ajudará as empresas a evitar reformulações e investigações regulatórias caras, além de promover a confiança dentro e fora da organização.

Essa mudança cultural deve começar no topo, com os altos executivos reconhecendo que os dados pertencem a seus clientes e aliados, e eles têm a responsabilidade de coletá-los e utilizá-los de maneira legal e ética. Com esse objetivo em mente, as empresas são incentivadas a desenvolver relacionamentos complementares entre as linhas de negócios, o escritório de privacidade e a equipe de segurança. Da mesma forma, deve haver clareza quanto à responsabilidade de identificar e reportar os riscos à privacidade e de assumir e demonstrar uma posição de responsabilidade que pode ser defendida perante um órgão regulatório.

A automação é fundamental para o gerenciamento eficaz e a maior eficiência dos processos de privacidade, particularmente as avaliações de impacto sobre a privacidade e solicitações de acesso de titulares de dados. Isso pode permitir que a organização aproveite as tecnologias de governança, risco e *compliance* nas quais investiram — gerenciamento de conteúdo e fluxo de trabalho e análise de riscos, por exemplo — o que, por sua vez, podem operacionalizar módulos de privacidade que poderão ter um impacto tangível no mapeamento de dados e de acesso.

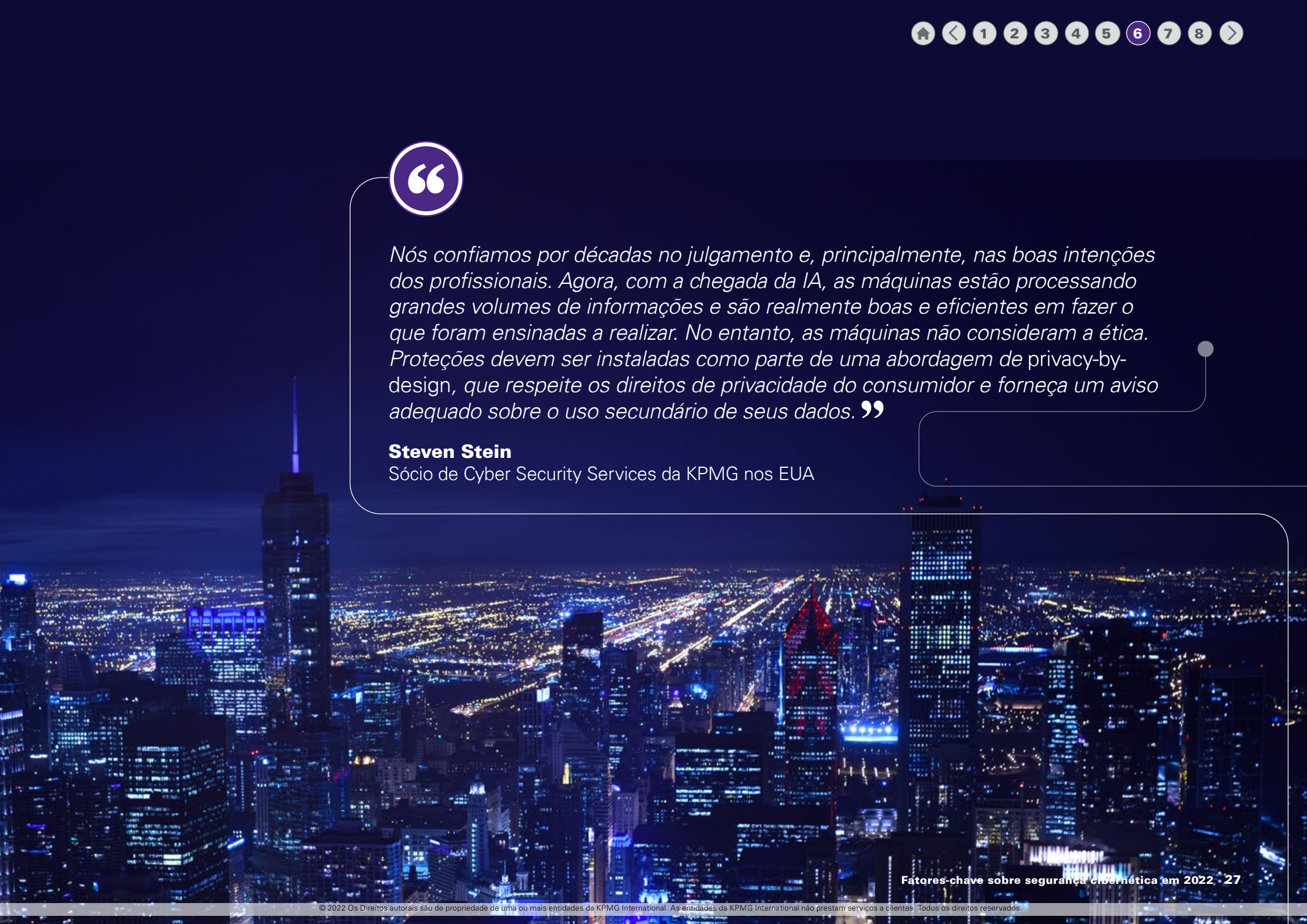
A automação também pode ajudar a quebrar as barreiras entre as funções de segurança cibernética e de privacidade. Essas são disciplinas muito complementares, e as organizações podem alinhá-las operacionalmente e compartilhar orçamentos maiores, o que, de forma geral, a equipe cibernética gosta, mas a equipe de privacidade, não.

Por exemplo, com metadados e mapeamento de dados, as equipes de segurança cibernética e de privacidade contam com os mesmos ativos. As duas equipes devem entender os dados aos quais a organização tem acesso e seus direitos de usar e processar essas informações. Elas podem então trabalhar juntas para implementar controles apropriados de segurança e privacidade, mantendo a filosofia de *Zero Trust* em mente. A automação pode permitir que elas entendam melhor onde seus principais ativos de dados estão localizados e como usá-los de forma mais eficaz. Em seguida, elas começam a aproveitar os mesmos recursos financeiros utilizados para atingir o mesmo resultado: proteger as joias da coroa.

Familiarizar-se com as tecnologias emergentes, como automação e IA, é algo importante e recomendado, mas os princípios básicos das perspectivas de segurança e privacidade devem ser constantes. Em outras palavras, obter o consentimento dos indivíduos cujos dados são coletados, reunir apenas os dados relevantes, retê-los apenas enquanto for necessário, descartá-los quando não forem mais necessários e protegê-los adequadamente.

Nós confiamos por décadas no julgamento e, principalmente, nas boas intenções dos profissionais. Agora, com a chegada da IA, as máquinas estão processando grandes volumes de informações e são realmente boas e eficientes em fazer o que foram ensinadas a realizar. No entanto, as máquinas não consideram a ética. Proteções devem ser instaladas como parte de uma abordagem de privacy-by-design*, que respeite os direitos de privacidade do consumidor e forneça um aviso adequado sobre o uso secundário de seus dados.*

Steven Stein
Sócio de Cyber Security Services da KPMG nos EUA



Algumas ações fundamentais a serem consideradas para 2022

1. Educar a alta administração e a gerência de negócios sobre a importância de garantir o consentimento da coleta de dados dos indivíduos e como o descumprimento dos direitos do consumidor pode afetar a empresa negativamente.
2. Alinhar seu programa de privacidade de dados com as prioridades e visão de liderança dos altos executivos e da linha de negócios, para ajudar a garantir que todos estejam em sintonia no que tange às perspectivas de coleta, consentimento e uso.
3. Adotar um padrão de *privacy-by-design* para complementar as regras, regulamentos e expectativas regulatórias em torno da privacidade.
4. Tornar as políticas baseadas em papel em práticas de negócio verificáveis para convencer consumidores e órgãos regulatórios do seu compromisso em respeitar os direitos do cliente e proteger seus dados.
5. Explorar oportunidades para implementar uma ferramenta de tecnologia de gerenciamento de privacidade de dados para automatizar processos, cumprir regulamentos, ajudar a aumentar a velocidade de resposta e auxiliar na redução de erros humanos.

Saiba mais

Tecnologia de privacidade: quais são as próximas etapas?
A evolução da tecnologia de privacidade de dados na era da automação.

Um ato de equilíbrio: privacidade, segurança e ética
Como a elaboração do conjunto de dados adequado pode ajudar a impulsionar o crescimento.

Responsabilidade de dados corporativos: preenchendo a lacuna de confiança do consumidor
Conforme as empresas coletam mais dados pessoais, as preocupações dos consumidores aumentam. Aprenda como as empresas podem agir para recuperar a confiança do consumidor.

Fator-chave 7

Proteger além das fronteiras

Incentivar uma ampla cadeia de suprimentos a ter segurança cibernética, enquanto ela protege a organização.

A corrida para a transformação digital continua sendo uma alta prioridade para as grandes e pequenas empresas. Tornar-se uma organização que prioriza o digital implica em uma abordagem centrada nos dados, na qual as informações são compartilhadas de maneira praticamente constante em um ecossistema complexo e conectado de aliados e fornecedores. Essa fluidez de dados entre terceirizados gera inúmeras oportunidades para os ataques cibernéticos comprometerem os sistemas e os dados. Como os CISOs podem ajudar a proteger suas próprias organizações e, ao mesmo tempo, estimular seu ecossistema mais amplo a ser seguro do ponto de vista cibernético?

Segurança do ecossistema: a situação atual das soluções e os obstáculos

A maioria das organizações não é mais a entidade única e monolítica há muito tempo. Elas são profundamente dependentes operacionalmente de uma cadeia de suprimentos robusta e de uma grande quantidade de fornecedores tradicionais e não tradicionais, que geralmente têm acesso direto a sistemas e dados de negócios. Embora as normas regulatórias e estruturas de segurança mutuamente acordadas possam ajudar a minimizar o impacto de ameaças cibernéticas de terceiros, há situações em que os participantes dessas estruturas complexas de ecossistemas — fornecedores de nuvem, empresas de SaaS, fabricantes de dispositivos de Internet das Coisas (IoT) etc. — podem não ter obrigações claras sobre como estabelecer controles adequados para proteger os dados de seus aliados, deixando toda a rede vulnerável a ataques cibernéticos.

Do ponto de vista da negociação de contratos, deve haver uma avaliação adequada de todas as políticas de segurança organizacional dos fornecedores potenciais e da segurança incorporada nos produtos e serviços que serão acessados. Atualmente, isso exige uma due *diligence* complexa e talvez inviável de cada parte do ecossistema. Na maioria dos casos, avaliações pontuais e periódicas são realizadas manualmente por programas de segurança de terceiros, gerenciados internamente ou terceirizados.

Algumas organizações, especialmente em setores regulamentados, também estão usando melhor as empresas de classificação de segurança, cujos serviços complementam as avaliações pontuais ao fornecer pontuações de risco de segurança em relação a um conjunto de parâmetros pré-definidos. Isso ajuda a determinar se a segurança de um aliado do ecossistema é minimamente suficiente, oferecendo uma análise qualitativa e quantitativa detalhada.

Infelizmente, essa abordagem não é mais adequada para o propósito no ambiente digital em constante evolução atual. Embora essa forma de estrutura de confiança — ou de falta de confiança — possa fornecer visibilidade de risco praticamente em tempo real, ela é simplesmente muito demorada e cara para a maioria das organizações. Consequentemente, muitas empresas, fornecedores terceirizados e até mesmo órgãos regulatórios estão sob pressão crescente para fornecer uma garantia contínua sobre a segurança dos seus ecossistemas. Esse cenário só vai se tornar mais desafiador conforme a complexidade do ecossistema de fornecedores aumenta, e outros fornecedores, *shadow-IT* e uma falta de supervisão de provedores de SaaS exigem cada vez mais atenção. Como resultado, os CISOs enfrentam a difícil tarefa de fazer a transição da estratégia baseada em conformidade para uma abordagem muito mais proativa, que coloca o monitoramento contínuo, o uso de soluções baseadas em IA/ML, inteligência de ameaças e *Zero Trust* no centro do seu modelo de segurança do ecossistema.

> *Com a nuvem e as tecnologias digitais criando ecossistemas hiperconectados e com vários fornecedores, há uma nova disposição para abordar o risco associado proativamente. A automação continuará desempenhando um papel importante na ativação de medidas corretivas adequadas nesses ambientes em terceiros.*

Atul Gupta
Sócio-líder global de Cyber Security para telecomunicações, mídia e tecnologia da KPMG na Índia

Qual é o seu plano?

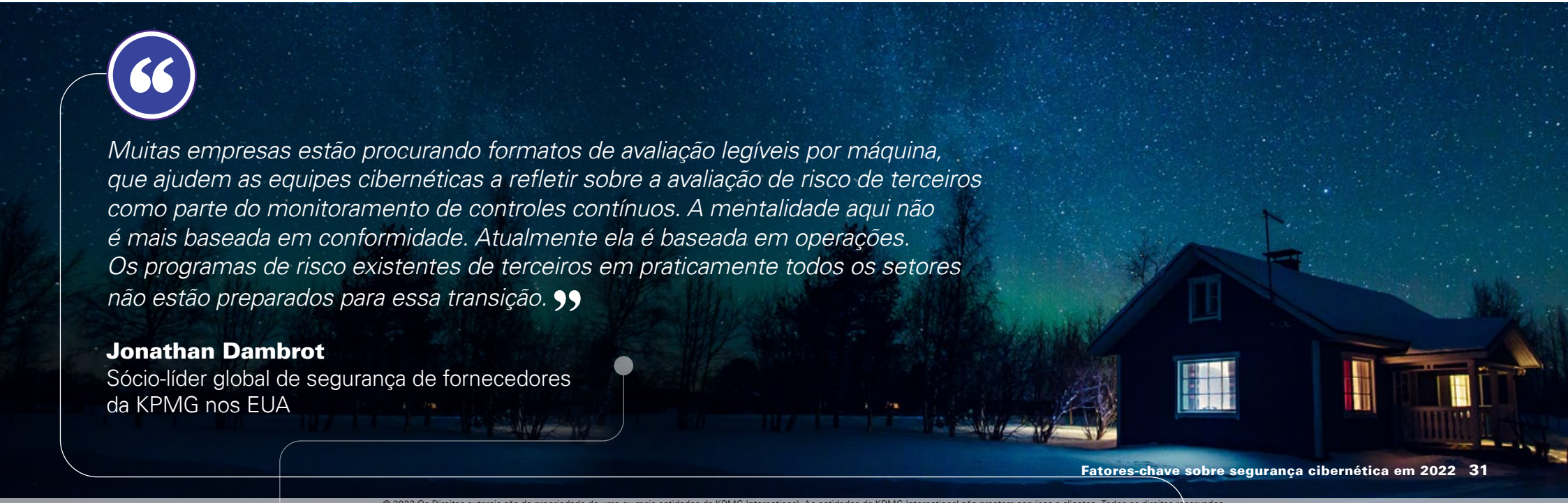
As regulamentações relacionadas à segurança cibernética provavelmente continuarão aumentando e se tornando mais rigorosas, conforme exemplificado por ordens executivas do governo norte-americano sobre a cadeia de suprimentos e a Diretiva de NIS em constante evolução da União Europeia, que traçou linhas claras sobre como os estados-membro, setores e organizações devem melhorar suas políticas internas e externas de segurança cibernética, especialmente em um mundo pós-pandemia.

Uma sólida estrutura de gerenciamento de risco que olhe para dentro e para fora é fundamental, especialmente para setores de alto risco, como serviços financeiros, energia e saúde. Uma metodologia à prova de limitação de sua vida útil também deve ser aplicada nos principais setores ao redor do mundo, em um esforço para garantir que todos os fornecedores do ecossistema sigam um caminho claro na proteção de suas próprias organizações e das cadeias amplas nas quais atuam.

Outra área importante deve ser a automação, incluindo o uso de IA/ML em todo o ecossistema. A IA/ML pode ser aplicada a políticas de segurança para solucionar problemas de *shadow IT,* fornecer melhor supervisão de produtos SaaS de terceiros, implementar chatbots de autoatendimento e automatizar muitos aspectos dos processos de gerenciamento de risco de terceiros da organização.

O monitoramento contínuo de controles (*Continuous Controls Monitoring - CCM)* leva esse cenário um passo adiante, afastando as avaliações de segurança de atividades pontuais que se tornam obsoletas rapidamente. O CCM pode agilizar os ciclos do fornecedor utilizando avaliações legíveis por máquina, o que, em última análise, aumenta o risco e a supervisão do controle. Para ser eficaz no contexto de um ecossistema de aliados, o CCM exige a participação do fornecedor e a aceitação desse tipo de avaliação. Esse modelo pode inspirar os fornecedores a migrar de uma atuação baseada em conformidade para um foco mais operacional, que possibilite medidas corretivas em tempo real com ou sem intervenção humana.

Com a mudança em direção à garantia contínua, os órgãos regulatórios e até mesmo as grandes organizações podem adotar uma abordagem mais ativa para construir a segurança do ecossistema. Em um mundo de negócios interconectado, as empresas estão percebendo que têm a responsabilidade de proteger sua cadeia de fornecedores, especialmente aqueles que não têm o mesmo nível de recursos. Isso pode significar fornecer um serviço de monitoramento/inteligência de ameaças em todo o seu ecossistema de suprimentos e colaborar com os fornecedores em sua defesa contra as ameaças identificadas. Embora ainda estejam nos passos iniciais, os reguladores e órgãos nacionais estão cada vez mais adotando essa perspectiva, e as organizações maiores e mais maduras podem seguir o exemplo.



> *“Muitas empresas estão procurando formatos de avaliação legíveis por máquina, que ajudem as equipes cibernéticas a refletir sobre a avaliação de risco de terceiros como parte do monitoramento de controles contínuos. A mentalidade aqui não é mais baseada em conformidade. Atualmente ela é baseada em operações. Os programas de risco existentes de terceiros em praticamente todos os setores não estão preparados para essa transição.”*

Jonathan Dambrot
Sócio-líder global de segurança de fornecedores da KPMG nos EUA

Algumas ações fundamentais a serem consideradas para 2022

1. Acompanhar os requisitos regulatórios conforme eles continuam evoluindo e se concentrando na segurança da cadeia de suprimentos.
2. Considerar o CCM como uma maneira de mudar os ecossistemas de uma visão de conformidade para uma de segurança mais operacional.
3. Explorar as oportunidades para automatizar, aproveitar a IA/ML em abordagens de segurança da cadeia de suprimentos para melhorar a segurança e permitir que profissionais qualificados se concentrem nas atividades mais estratégicas.
4. Não negligenciar a cadeia de suprimentos de tecnologia operacional *(Operational Technology - OT)*. À medida que os sistemas de TI e OT convergem, os invasores provavelmente tentarão explorar os sistemas de OT em um esforço para comprometer os dados da empresa.
5. As organizações maiores e com mais recursos devem buscar uma perspectiva de capacitação, aplicando medidas de segurança para proteger seu ecossistema mais amplo, além do seu próprio ambiente.

Saiba mais

A empresa ampliada — garantindo o futuro
Definindo o caminho para um ecossistema de terceiros mais seguro.

O ecossistema de terceiros em mudança
Adaptando a abordagem para ajudar a proteger o ecossistema em evolução.

Racionalizar o gerenciamento de risco de terceiros com IA
Apresentando um profissional digital de IA aos seus esforços de segurança de terceiros.

Fator-chave 8

Reformular a conversa sobre resiliência cibernética

Amplie a capacidade de manter as operações, recuperar-se rapidamente e administrar as consequências quando um ataque cibernético ocorrer.

No ambiente digital volátil de hoje, a resiliência deve considerar até que ponto as empresas entendem, antecipam-se e estão preparadas para se recuperar do impacto potencial de um grande incidente cibernético. Os CISOs e suas equipes são incentivados a iniciar um diálogo com os líderes seniores que questione a premissa de que a organização pode absorver um ataque cibernético ou, na pior das hipóteses, recuperar-se em alguns dias. Eles devem explorar a capacidade de manter as operações caso a interrupção dure várias semanas, enquanto gerenciam os meios de comunicação e as atenções regulatória e do público.

"Há um plano"

Quando os CEOs são questionados sobre como abordam a possibilidade de um ataque cibernético, a maioria afirma: *"Há um plano"* e *"Esta é uma prioridade na agenda do conselho."* A experiência dos últimos meses sugere que as perguntas mais pertinentes são: como você está preparado para enfrentar uma paralisação de quatro a seis semanas como resultado de um ataque cibernético? Como isso afetaria o atendimento ao cliente? O que isso significaria para os seus centros de atendimento e distribuição? Você conseguiria cobrir a próxima folha de pagamento? Você conseguiria pagar os fornecedores? Como uma interrupção pode afetar os requisitos legais e regulamentares da empresa?

A resiliência exige uma avaliação dos principais processos operacionais de negócios e uma estratégia para protegê-los.

Na realidade do mercado atual, um grande evento cibernético é praticamente inevitável para a maioria das empresas. Com isso em mente, pensando na evolução da mentalidade dos profissionais de segurança, o foco de muitos CISOs atualmente está na redução da probabilidade de uma invasão e no gerenciamento das consequências. Claramente, isso não é o suficiente para detectar uma violação bem-sucedida: é igualmente importante agir rápido o suficiente para limitar os danos. Na verdade, sabe-se que o código malicioso permanece inativo em um ambiente violado por meses antes de ativar e reinfectar o sistema de maneira repentina.

Nos últimos anos, os *hackers* aumentaram seu foco em dois tipos de ataques cibernéticos.

— **Ataques de *ransomware*:** houve uma série de incidentes em que um invasor viola uma organização e criptografa seus dados, tornando-os inacessíveis até que a vítima pague um resgate exorbitante para recuperar o acesso. Exceto nesse momento, os invasores estão usando táticas de dupla extorsão, lançando a ameaça adicional de vazar publicamente os dados criptografados caso um pagamento adicional de resgate não seja feito, ao mesmo tempo em que foca nos *backups on-line* da organização.

— **Ataques à cadeia de suprimentos:** cada vez mais, os invasores têm como alvo as empresas que produzem *softwares* importantes e que são elos logísticos vitais em redes muito maiores e mais amplas. Da perspectiva do *hacker*, infiltrar-se em um alvo menor requer muito menos esforço para causar danos maiores.

Embora esses ataques não sejam excessivamente sofisticados em termos de metodologia — eles ainda usam *phishing*, pulverização de senhas e rastreamento de vulnerabilidades — eles são incrivelmente eficazes. Espera-se que esses tipos de ataques aumentem no futuro. Especificamente para *ransomware*, enquanto as empresas estiverem dispostas a pagar o resgate, esse problema provavelmente persistirá.

> *"A empresa deve desempenhar um papel ativo na resiliência digital: simulações de cenários, conhecimento das dependências, planos que deixem claro o que pode e o que não pode ser feito. Assim, pode ser dada uma resposta coletiva."*
>
> **Dani Michaux**
> Sócio-líder de Cyber Security para a Europa, Oriente Médio e África da KPMG na Irlanda

Em um mundo digital cada vez mais interconectado e interdependente, esses eventos, como os ataques WannaCry há alguns anos e o ataque à Colonial Pipeline no início de 2021, podem ter implicações muito mais amplas e sistêmicas em uma economia, motivando os órgãos regulatórios em todo o mundo a emitir novas regras e diretrizes para uma ampla gama de setores. Talvez o exemplo mais pertinente seja a Diretiva de Rede e Sistemas de Informação *(Network and Information Systems - NIS)* da União Europeia de 2016, que visava criar um alto padrão de segurança de redes e informações, e sua substituição proposta, a NIS2, que visa abordar a gama crescente de infraestrutura digital da qual nossas sociedades atualmente dependem. Iniciativas regulatórias específicas do setor, como a Lei de Resiliência Operacional Digital na Europa, também colocarão obrigações crescentes no setor em relação à resposta a incidentes, divulgação de vulnerabilidades, testes de penetração, criptografia e outras áreas.

Qual é o seu plano?

O CISO e sua equipe não podem garantir a resiliência cibernética por conta própria. Esse deve ser um esforço de toda a organização, com adesão e apoio ativo da alta administração, da área financeira, de marketing e outras partes interessadas. Há um desenvolvimento dinâmico interessante, especialmente na Europa, onde diversos cargos — CISOs, diretores de risco (CROs) e diretores de dados (CDOs) — estão evoluindo em direção ao que pode ser chamado de um diretor de resiliência digital, o que envolve uma agenda mais ampla de prioridades compartilhadas de segurança, risco de tecnologia e continuidade de negócios.

Os CISOs devem educar a liderança sobre o risco e as consequências de uma violação e sobre os motivos da resiliência cibernética ser tão importante. No entanto, evite jargões técnicos excessivos — fale sobre o cenário de ameaças, o custo da falha, o tempo de recuperação e o impacto potencial.

Reserve algum tempo para analisar seus planos de resiliência cibernética organizacional e se esforce para garantir que eles sejam adequados ao propósito. Planos que foram desenvolvidos anteriormente para problemas de resiliência física provavelmente não são adequados para um evento cibernético. Há várias diferenças importantes entre o planejamento da resiliência física e cibernética: no espaço virtual, geralmente há um alto grau de incerteza quanto ao que realmente aconteceu, quando e como; o impacto costuma ocorrer em toda a organização, em vez de ser relegado a um local específico (e muitas vezes vai além da organização); e, muitas vezes, presume-se que a área de TI tem a capacidade de ajudar a gerenciar o incidente — o que pode ou não ser o caso. Não espere que um evento cibernético aconteça para testar seus planos. Simular ataques cibernéticos do mundo real regularmente com executivos é algo importante e ajuda a entender o impacto potencial de um ataque cibernético na organização e o que é necessário para responder e se recuperar. Você não pode replicar totalmente uma situação real, mas quanto mais bem preparada a organização estiver, melhores serão as chances de gerenciar incidentes com mais eficácia.

Obviamente, as equipes cibernéticas ainda precisam se concentrar nos fundamentos da segurança para fortalecer a resiliência em toda a organização. Na verdade, muitas violações são bem-sucedidas porque o alvo não realizou o trabalho fácil, como identificar ativos críticos, proteger as contas com senhas fortes e gerenciar os *patches*. No entanto, no mundo digital acelerado atual, isso por si só não é suficiente. As organizações devem complementar os fundamentos com recursos de detecção sólidos, uma capacidade avançada de responder e se recuperar rapidamente e um foco no gerenciamento das consequências de um ataque cibernético.

O que fazer agora mesmo, ou em breve? Identifique de cinco a dez processos de negócios e suas dependências dos principais fornecedores que representam o maior risco, conforme o impacto financeiro, a corrupção de dados ou gatilhos regulatórios. Isso pode lhe dar uma visão clara das prioridades, para que você possa implementar os controles e estratégias adequados.”

Wilhelm Dolle
Sócio-líder de Cyber Security da KPMG na Alemanha

Algumas ações fundamentais a serem consideradas para 2022

1. Considerar por quanto tempo você pode manter o negócio caso funções importantes fiquem inoperantes, e o que isso significaria do ponto de vista do impacto sobre o cliente.
2. Refletir sobre como um evento cibernético significativo afetaria a sua dependência dos fornecedores.
3. Escalar o tema de segurança cibernética e resiliência cibernética para o nível do Conselho.
4. Questionar se seus planos de resiliência atuais são adequados para um ataque cibernético e tomar as medidas corretivas adequadas.
5. Ter a humildade de reconhecer que suas premissas podem estar erradas e um plano alternativo talvez precise ser operacionalizado rapidamente.
6. Ajudar os altos executivos a desenvolver seus recursos de gerenciamento de crises e suas funções individuais no caso de um ataque cibernético, por meio de simulações regulares do mundo real.
7. Concentrar-se nos fundamentos, mas também investir em recursos de detecção, agilidade de resposta e capacidade de recuperação.
8. Colaborar com especialistas relevantes do setor, caso você não tenha a capacidade ou os recursos internos necessários.

Saiba mais

A mudança de formato de *ransomwares*
Como se defender e responder a ataques de *ransomwares*.

Proteger um mundo hiperconectado
Como se preparar e responder a ataques cibernéticos direcionados a infraestruturas críticas.

Como proteger sua OT durante a pandemia de *ransomware*
A nova cara do *ransomware*.

Conclusão

Em um futuro não tão distante

Daqui para frente, a sociedade inteligente hiperconectada provavelmente enfrentará riscos cibernéticos cada vez maiores em várias frentes globais, por meio de vetores diversos de ameaças em evolução. Claramente, os avanços tecnológicos que impulsionam os negócios, as comunicações e o entretenimento trazem novos perigos. Neste relatório, exploramos temas oportunos, como a equipe de segurança em evolução, a automatização da função de segurança, a privacidade de dados e a proteção do ecossistema. Agora vamos dar uma olhada em vários desafios emergentes de segurança cibernética. Embora nenhum desses temas seja novo, acreditamos que em breve eles se tornarão as principais áreas de foco para profissionais de segurança cibernética em praticamente todos os setores industriais.

IIoT

Conforme a Internet das Coisas Industrial (IIoT) continua crescendo, milhões, senão bilhões, de sensores baseados em nuvem, máquinas e outros dispositivos conectados podem se tornar pontos de entrada vulneráveis para ataques cibernéticos. A urgência de uma perspectiva cibernética é que, na pressa para inovar, o *software* usado nesses sistemas hiperconectados muitas vezes não inclui os controles de gerenciamento de risco apropriados.

É certo que a IIoT está criando um conjunto de ambientes propícios ao ataque. Embora as prioridades dos fabricantes estejam mudando, até agora, o projeto da arquitetura de sensores em conexão com a qualidade do ar, o tráfego, a gestão de resíduos e a rede de energia em geral, por exemplo, pode não ter abordado a segurança completamente.

Pode haver grandes restrições operacionais em dispositivos individuais em relação às limitações de energia e peso que poderão atrapalhar a incorporação de controles. Porém, a segurança da infraestrutura simplesmente não pode ser deixada de lado.

As organizações devem se concentrar no grau de segurança incorporada nos produtos que possibilitam a IIoT e na maneira como esses dispositivos são aproveitados no ecossistema mais amplo. Com relação à implementação estratégica desses produtos em um ambiente corporativo ou de cidade inteligente, você está falando sobre um conjunto muito mais amplo de pessoas, políticas, procedimentos e tecnologias, além de considerações como monitoramento de anomalias, gerenciamento de identidades e *Zero Trust*, entre outros fatores. No futuro, acreditamos que a IIoT deverá ser vista como um componente de um ecossistema mais amplo de soluções que, em última análise, constituem uma postura de segurança abrangente.

> *Este é um ciclo vicioso, em que cada nova tecnologia amplia o cenário de ameaças e gera inovação cibernética para ajudar a melhorar os recursos de defesa. Essa é a única maneira de funcionar? Acredito que incorporar a segurança em todos os aspectos de TI e OT, além de todos os processos e procedimentos no nível do DNA de uma empresa, é o futuro inevitável e a única saída.”*

Prasad Jayaraman
Sócio-líder de Cyber Security para as Américas da KPMG nos EUA

Atualmente, a sociedade vive e faz negócios em um mundo digital de dados, dispositivos e dependência. A confiança é depositada — consciente ou inconscientemente — na tecnologia de uma maneira que seria impensável há uma década, o que levanta questões sobre segurança, proteção, privacidade e até mesmo ética. Os profissionais de segurança devem navegar nessa nova realidade, ajudando os líderes a entender as implicações de confiar na tecnologia e na sua resiliência, ao mesmo tempo em que antecipam como essa tecnologia pode ser explorada por outras pessoas. Isso pode trazer uma perspectiva diferente e valiosa, mas também há o dever de oferecer conselhos pragmáticos e práticos.”

David Ferbrache
Sócio-líder global de Cyber Future da KPMG no Reino Unido

Redes 5G

Os recursos potenciais de conectividade, possibilitados por aplicativos emergentes instalados em redes 5G, são empolgantes. No entanto, esses ecossistemas conectados baseados em *software* devem priorizar não apenas a inovação técnica, mas também a segurança dos dispositivos que podem facilitar essas conexões.

Uma rede 5G é fundamentalmente diferente da 4G em termos de velocidade, largura de banda, latência e sofisticação geral. Obviamente, o 5G permitirá grandes avanços na conectividade, mas também traz um conjunto diferente de desafios de segurança e exige arquitetura, monitoramento e controles de segurança muito sofisticados. Algumas dessas preocupações influenciam as tensões geopolíticas das cadeias de suprimentos existentes hoje em relação ao fornecimento de componentes de tecnologia e infraestrutura essenciais.

Isso também levanta uma questão sobre a confiança. Com o 5G, os profissionais de segurança cibernética provavelmente estarão em uma posição em que milhões de dispositivos, cada um com a sua própria identidade digital, podem se conectar simultaneamente em ambientes não confiáveis caracterizados por arquiteturas de conexão muito difusas. Na nossa opinião, esse ar de imprevisibilidade sugere que as organizações devem assumir uma mentalidade de *Zero Trust* contínua e uma arquitetura de autenticação que seja flexível e adaptável a essas novas dependências e problemas de resiliência.

IA

Uma área já florescente, a IA — em especial o ML e o aprendizado profundo — provavelmente continuará sendo um tema cativante daqui para frente.

Proteger os aplicativos de IA de aprendizagem é um desafio muito diferente do que proteger sistemas convencionais. Há muitas perguntas: o software está operando dentro dos parâmetros treinados? Qual é o nível de vieses inconscientes? O aplicativo está sendo manipulado por um mau agente ou uma IA adversária em um esforço para comprometer informações confidenciais? Olhando para o futuro, os profissionais de segurança cibernética também podem ter que pensar sobre a integridade, previsibilidade e aceitabilidade do aplicativo de IA no contexto do ambiente operacional para o qual foi treinado e projetado. Nesta esfera, os CISOs e suas equipes devem esperar construir alianças sólidas com o diretor de tecnologia e sua equipe de ciência de dados. Por uma questão de segurança, esse é um novo território.

Em um futuro próximo, os ataques cibernéticos provavelmente também usarão automação de processos robóticos, ML e aprendizado profundo. Sondar e testar as vulnerabilidades e defesas de um ambiente profissional pode ser tão facilmente automatizado quanto construir campanhas de spam ou comprometer o *e-mail*. Os invasores estão usando IA, mas eles não têm limites. No curto prazo, é mais provável que os criminosos tenham uma vantagem no aproveitamento da IA para industrializar os ataques. Isso já está acontecendo e provavelmente continuará a acontecer.

Há inúmeras questões de responsabilidade em torno da IA. As estruturas jurídicas são bastante imaturas e há muitas iniciativas regulatórias. Pode levar ainda algum tempo para que os profissionais de segurança cibernética avaliem as implicações, enquanto os criminosos virtuais provavelmente serão mais audaciosos.

Agradecimentos

Este relatório não seria possível sem a colaboração de colegas de todo o mundo, que contribuíram com seu apoio, conhecimentos e ideias para o planejamento, análise, redação e produção.

Nossos agradecimentos:

À nossa equipe global de fatores-chave cibernéticos

Alissa Bernhardt
Jessica Booth
David Ferbrache
John Hodson
Billy Lawrence
Paula Reis
Michael Thayer

Aos nossos profissionais globais que contribuíram com seus *insights*

KPMG na Alemanha
Wilhelm Dolle

KPMG na Austrália
Matt O'Keefe
Matthew Quick

KPMG na Áustria
Andreas Tomek

KPMG no Canadá
Sylvia Klasovec Kingsmill

KPMG nos EUA
Deepak Mathur
Fred Rica
Jim Wilhelm
Jonathan Dambrot
Matthew Miller
Prasad Jayaraman
Rik Parker
Steve Barlock
Steven Stein

KPMG na Índia
Akhilesh Tuteja
Atul Gupta
Shreyashi Sengupta

KPMG na Irlanda
Dani Michaux

KPMG no Reino Unido
David Ferbrache

Contatos

KPMG na Alemanha
Wilhelm Dolle
Sócio-líder de Cyber Security
da KPMG na Alemanha
wdolle@kpmg.com

KPMG na Austrália
Gordon Archibald
Sócio da KPMG na Austrália
garchibald@kpmg.com.au

Matt O'Keefe
Sócio-líder de Cyber Security
da região Ásia-Pacífico da KPMG
na Austrália
mokeefe@kpmg.com.au

KPMG no Brasil
Leandro Augusto
Sócio-líder de Cyber Security
da KPMG no Brasil
lantonio@kpmg.com.br

KPMG no Canadá
Hartaj Nijjar
Sócio de Cyber Security
da KPMG no Canadá
hnijjar@kpmg.ca

KPMG na China
Henry Shek
Sócio da KPMG na China
henry.shek@kpmg.com
hnijjar@kpmg.ca

KPMG na Coreia do Sul
Min Soo Kim
Sócio da KPMG na Coreia do Sul
mkim9@kr.kpmg.com

KPMG na Espanha
Marc Martinez Marce
Sócio da KPMG na Espanha
marcmartinez@kpmg.es

KPMG nos EUA
Prasad Jayaraman
Sócio-líder de Cyber Security para
as Américas da KPMG nos EUA
prasadjayaraman@kpmg.com

Kyle Kappel
Sócio-líder de Cyber Security
Services da KPMG nos EUA
kylekappel@kpmg.com

KPMG na França
Vincent Maret
Sócio da KPMG na França
vmaret@kpmg.fr

KPMG na Holanda
Koos Wolters
Sócio de Data Privacy da KPMG
na Holanda
wolters.koos@kpmg.nl

KPMG na Índia
Akhilesh Tuteja
Sócio-líder global de Cyber Security
da KPMG na Índia
atuteja@kpmg.com

Atul Gupta
Sócio-líder global de Cyber Security
para telecomunicações, mídia
e tecnologia da KPMG na Índia
atulgupta@kpmg.com

KPMG na Irlanda
Dani Michaux
Sócio-líder de Cyber Security para
a Europa, Oriente Médio e África
da KPMG na Irlanda
dani.michaux@kpmg.ie

KPMG na Itália
Luca Boselli
Sócio da KPMG na Itália
lboselli@kpmg.it

KPMG no Japão
Atsushi Taguchi
Sócio de Technology Risk Services
da KPMG no Japão
atsushi.taguchi@jp.kpmg.com

KPMG no México
Rommel Garcia
Sócio de Advisory da KPMG
no México
rommelgarcia@kpmg.com.mx

KPMG em Singapura
Daryl Pereira
Sócio de Cyber Security da KPMG
em Singapura
darylpereira@kpmg.com.sg

Ser inovador
transforma negócios.

#KPMGTransforma

Baixe o
nosso APP

kpmg.com.br

/kpmgbrasil

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.