Considerações de Segurança Cibernética para 2023

O fio condutor

Junho de 2023

kpmg.com.br

Prefácio

Nosso futuro é dependente de dados e infraestrutura digital. A pandemia de covid-19 acelerou nossa mudança para os canais digitais e colocou essas questões em foco. Conforme as economias globais e as cadeias de suprimentos foram interrompidas, as organizações tiveram que repensar suas dependências de bens, serviços e da infraestrutura digital que as sustenta.

Tecnologias inovadoras devem moldar esse futuro, alguns exemplos são: inteligência artificial, *blockchain*, biometria, sistemas hiperconectados e realidade virtual. E todos podem representar novos desafios de segurança, privacidade, ética e levantar questões fundamentais sobre nossa confiança em sistemas digitais. Pode ser difícil chegar a um consenso sobre essas questões com diversas visões nacionais e culturais, no entanto, este é o ambiente em que o comércio global precisa prosperar. Precisamos abordar as preocupações agora à medida que inovamos, não retrospectivamente, quando for tarde demais.

A lista de indústrias que consideramos sistemicamente importantes também está mudando. No passado, o foco era em serviços de utilidade pública, telecomunicações e serviços financeiros. Agora temos um grande leque de parcerias público-privadas, ecossistemas conectados e infraestruturas de informação. Um olhar sobre os mercados financeiros mostra um mundo hiperconectado de instituições, provedores de dados e serviços gerenciados, e todos eles agora são sistemicamente importantes. E à medida que o grau de conectividade e dependência entre estes serviços aumenta, cresce também o interesse daqueles que procuram atacar e explorar essas infraestruturas.

Com essas mudanças, vem um impulso global em direção a uma maior regulamentação de segurança cibernética. Isso aumenta a preocupação entre as organizações sobre a crescente carga de regras e a diversidade dos requisitos regulatórios. Como resultado, as empresas estão colocando cada vez mais esforços ao incorporar privacidade e segurança na forma como operam, tanto em resposta às novas ameaças quanto à necessidade de cumprir os requisitos regulatórios entre países.

A segurança cibernética deve ser parte integrante de cada linha de negócios, função, produto e serviço. As organizações devem ter como objetivo garantir que a segurança cibernética seja onipresente em toda a empresa digital e entrelaçada junto à estratégia, desenvolvimento e operações. Lisa Heneghan, Chief Global Digital Officer da KPMG International, diz que:

"*As organizações precisam começar a pensar na segurança cibernética como o fio condutor de seus negócios, devendo ser colocado no centro dos negócios e usado como base para construir confiança digital. No entanto, o Chief Security Officer (CISO) e suas equipes não podem fazer isso sozinhos, deve ser responsabilidade de todos e isso não é fácil. Primeiro, as pessoas devem entender como isso se relaciona com elas e depois pensar em como pode-se integrar a segurança aos processos existentes. Tratar cada função do negócio como um cliente e projetar controles de segurança de forma contínua pode incentivar comportamentos responsáveis e seguros e beneficiando imensamente o negócio.*"

Os CISOs também desempenharão um papel importante em iniciar e moldar um diálogo mais amplo em torno da resiliência dos negócios à disrupção digital, ajudar as empresas a entender melhor a natureza evolutiva dos ativos e serviços digitais que as empresas precisam proteger, e fornecer a base para a confiança nesses sistemas.

O relatório explora as ações que os CISOs, e o mercado em geral, podem tomar no próximo ano para demonstrar aos executivos e à alta administração que a confiança digital pode e deve ser uma vantagem competitiva. Consulte a página 22 para recomendações específicas em gestão de pessoas, processos, dados/tecnologia e regulatório.

Akhilesh Tuteja

Líder Global de Cyber Security
KPMG International

Oito considerações-chave de segurança cibernética para 2023

Clique em cada consideração para ver mais detalhes

01

Confiança digital: uma responsabilidade compartilhada

As organizações estão pensando amplamente sobre como proteger os interesses de funcionários, clientes, fornecedores e parceiros?

02

Segurança discreta leva a comportamentos seguros

Como as equipes de segurança integram efetivamente a segurança em processos de negócios, programas de desenvolvimento ágil e modelos operacionais diferentes?

03

Protegendo um futuro sem perímetro e centrado em dados

Com o perímetro de segurança praticamente extinto, como as organizações podem fazer uma transição pragmática e realista para uma abordagem de *Zero Trust* que proteja todos os aspectos de seu ecossistema?

04

Novas parcerias, novos modelos

Como as organizações mantém a segurança, privacidade e resiliência na linha de frente de um ambiente onde terceirizações e serviços gerenciados são uma prioridade crescente?

05

Confiança na automatização

O que as organizações podem fazer para ajudar a garantir que a automação de processos robóticos (RPA), *machine learning* (ML) e outras formas de inteligência artificial (IA) sejam implementadas e gerenciadas de forma eficaz, sensata e segura?

06

Protegendo um mundo inteligente

Quais são as implicações para as equipes de segurança e privacidade à medida que as empresas mudam para uma mentalidade de produto inteligente e hiperconectado?

07

Combatendo adversários ágeis

Como as equipes de segurança podem acompanhar as rápidas mudanças no cenário de ameaças e as táticas cada vez mais agressivas dos atacantes?

08

Seja resiliente quando - e onde - importa

Por que é importante pensar além da resposta e planejar proativamente a recuperação?

Consideração 1

Confiança Digital: uma responsabilidade compartilhada

A confiança digital está entrando na pauta dos Conselhos de Administração, à medida que os debates sobre privacidade, segurança e ética ganham força, impulsionados tanto pela regulamentação quanto pela opinião pública. O futuro sucesso de qualquer negócio ativado digitalmente é construído sobre a confiança digital, sendo segurança cibernética e privacidade de dados bases vitais para essa confiança. Os CISOs devem estar preparados para ajudar o conselho e o *C-level* a gerar e manter a confiança de seus *stakeholders*, criando assim uma vantagem competitiva. Realizar esse potencial requer um compromisso coletivo de todos os *stakeholders*.

A globalização tornou o mundo sem fronteiras e interconectado, uma realidade que ficou evidente pela interrupção das cadeias de suprimentos globais provocada pela pandemia. Para criar relacionamentos duradouros com os clientes (seja B2B ou B2C), as organizações devem estabelecer e manter a confiança digital.

A confiança digital abrange tópicos que afetam todos os aspectos de uma organização e está inerentemente ligada à estratégia corporativa. Não apenas por criar uma vantagem competitiva, mas porque é simplesmente a coisa certa a se fazer para a indústria e a sociedade em geral.

John Anyanwu
Sócio de Cyber Security Services
da KPMG na Nigéria

Valor e confiança

A confiança é a chave para o sucesso e não se trata apenas de reputação. Aumentar a confiança digital pode criar vantagem competitiva e aumentar os resultados.

Mais de 1/3 das organizações reconhecem que o aumento da confiança leva a uma maior rentabilidade.

Contudo, 65% reportam que os requerimentos de segurança da informação são moldados por requisitos de conformidade e não por ambições estratégicas de longo prazo.

65% dos executivos continuam vendo a segurança da informação como uma atividade de redução de risco, em vez de um facilitador de negócios.

49% acreditam que o Conselho de Administração vê a segurança como custo necessário em vez de uma maneira de ganhar vantagem competitiva.

Fonte: *KPMG Cyber Trust Insights 2022.*

O mercado está começando a se importar

Um número crescente de líderes seniores reconhecem os benefícios da confiança digital, com 37% vendo a melhoria da lucratividade como a principal vantagem comercial do aumento desta confiança[1]. A confiança digital abrange uma ampla gama de disciplinas, sendo a segurança cibernética uma parte importante desse amplo espectro de questões intimamente ligadas, relacionadas à confiança digital, como confiabilidade, segurança, privacidade e transparência. Essas áreas afetam a forma como as empresas conduzem os negócios e buscam valores; os produtos e serviços fornecidos; a tecnologia usada; como coletar e usar dados; e como proteger os interesses dos clientes, funcionários, fornecedores e todos as empresas colaboradoras e *stakeholders*.

Por outro lado, 65% continuam a ver a segurança da informação como uma atividade de redução de risco em vez de um facilitador de negócios[2]. Muitas organizações ainda enxergam a segurança cibernética principalmente como um custo e não necessariamente como um investimento no futuro, o que é um equívoco. Os executivos devem adotar o conceito de confiança digital e demonstrar como a segurança, como um facilitador para os negócios, certamente apoiará a expectativa de crescimento digital de uma organização.

Os CISOs têm um papel significativo em ajudar suas organizações a construir confiança digital, mas não podem fazê-lo sozinhos. Eles devem investir tempo suficiente para incentivar outros *stakeholders* críticos, internas e externas, em relação às suas respectivas funções na jornada de confiança digital. De fato, os CISOs devem demonstrar ao Conselho e ao C-level o por que de ser um assunto tão importante, e como a confiança digital depende de estratégias claramente articuladas e focadas nos negócios.

Como o Fórum Econômico Mundial (FEC) sugere, as empresas estão começando a reconhecer que a segurança cibernética é tanto um elemento estratégico de negócios como um risco empresarial, de desenvolvimento de produtos e de gerenciamento de dados. Em seu relatório *Earning Digital Trust: Decision-Making for Trustworthy Technologies*, o FEC afirma que "*a confiança digital requer uma abordagem holística, onde a segurança cibernética é uma dimensão de confiança, entre muitos*[3]."

Confiança digital para os clientes

Embora os típicos consumidores do varejo não se importem com detalhes do programa de proteção de dados da empresa, no momento em que os clientes descobrirem um vazamento de dados, eles querem saber quais ações estão sendo tomadas e se seus interesses estão sendo atendidos. A organização pode restabelecer a confiança ao longo do tempo ao responder os incidentes de forma rápida e transparente.

Os consumidores de hoje entendem que as violações acontecem e, gradualmente, a maioria dos consumidores irão voltar a consumir seus produtos caso a empresa ofereça produtos e serviços a um preço competitivo, se há uma experiência consistentemente positiva do cliente, e se os detalhes em torno da resposta e recuperação de um incidente cibernético são comunicados com transparência.

> ***Transparência significa coisas diferentes para diferentes públicos. Enquanto os consumidores de varejo exigem transparência quando ocorrem incidentes, as organizações devem saber com antecedência como os fornecedores e parceiros protegem suas informações. Isso ocorre porque as organizações têm uma obrigação muito maior com os clientes e precisam ter certeza de que podem entregar confiança em termos de proteção de dados.***
>
> **Henry Shek**
> Sócio de Cyber Security Services da KPMG na China

[1] KPMG. *KPMG Cyber trust insights survey 2022.*
[2] Ibid.
[3] WORLD ECONOMIC FORUM. *Earning Digital Trust: Decision - Making for Trustworthy Technologies. 2022.*

Estratégias que funcionam

É vital incorporar o conceito de confiança digital na estratégia corporativa, no desenvolvimento de produtos, na participação no mercado e no relacionamento com clientes corporativos e de varejo. Pensar amplamente sobre o que significa confiança digital em diferentes grupos de *stakeholders* pode ajudar a sublinhar a importância da segurança cibernética e das outras disciplinas que contribuem para estabelecer e manter a confiança digital, bem como incentivar uma abordagem holística em todas as disciplinas.

A confiança contempla uma função de tecnologias específicas desenvolvidas ou implantadas, juntamente com as decisões tomadas pela liderança. Os CISOs devem apoiar continuamente uma narrativa para o Conselho de Administração e o *C-level* esclarecendo o porque e como a segurança cibernética é essencial para a confiança digital.

> ***Resumindo, as empresas que são capazes de estabelecer confiança em seus produtos e serviços, como operam e protegem o negócio, por todos os stakeholders, tem maior probabilidade de verem impactos comerciais e reputacionais positivos.***

Annemarie Zielstra
Sócia de Cyber Security Services
da KPMG na Holanda

CISOs devem apoiar no direcionamento das decisões em torno dos parceiros e fornecedores adequados. Devem também ser estabelecidos critérios de qualificação que abranjam a transparência em relação às práticas de proteção de informações e a capacidade da organização de demonstrar resiliência adequada à recuperação e à resposta.

As obrigações regulatórias devem crescer em relação aos componentes da confiança digital, aumentando também as expectativas sobre os níveis de transparência e responsabilidade que os reguladores esperam das empresas a esse respeito. Uma abordagem holística e baseada em princípios para atender ao cenário regulatório diversificado e cada vez mais complexo traz vários benefícios e evita a criação de silos dispendiosos orientados à conformidade.

E isso começa no topo e vai descendo na organização, pois se a liderança aceita e vive essa narrativa, o resto da organização também deveria. Isso significa inserir um item concreto no relatório anual da empresa, no qual a filosofia, *design* e estratégia em torno da confiança digital são descritas em detalhes. Entre os líderes corporativos, 34% estão preocupados com a capacidade de seus negócios em satisfazer os requisitos regulatórios para maior transparência sobre segurança cibernética e privacidade. A KPMG defende uma abordagem proativa[4].

Saiba mais

Cyber Trust Insights 2022

Construindo a confiança através de segurança cibernética e privacidade.

Earning digital trust together

Por que a confiança importa mais do que nunca neste mundo hiperconectado.

Reversing the digital trust deficit

A necessidade crítica de reconstruir a confiança digital à medida que a tecnologia prolifera.

[4] *KPMG Cyber Trust Insights 2022. Op cit.*

Consideração 2

Segurança discreta leva a comportamentos seguros

Incorporar a segurança no negócio de uma maneira que ajude as pessoas a trabalhar com confiança, fazer escolhas produtivas e desempenhar seu papel na proteção da organização deve ser um objetivo-chave do CISO, embora muitas vezes vago. É muito comum as pessoas verem a segurança como um obstáculo, mas somente considerando a segurança sob ambas as perspectivas humana e de negócio, os CISOs podem ter a expectativa de mudar essa mentalidade.

Talvez o ponto mais essencial é estar atento a onde e quando a segurança é mais importante e onde as medidas de segurança adicionais provavelmente impactarão o negócio de forma justificada. Não há segurança absoluta e, se os CISOs tentarem proteger tudo a todo momento, correm o risco de não proteger nada, uma vez que os usuários encontram maneiras de contornar medidas de segurança intrusivas. Os CISOs precisam ser pragmáticos em relação à extensão dos controles de segurança que são implementados e que estejam alinhados à criticidade do processo de negócios e ao perfil de risco relacionado.

Em última análise, controles de segurança discretos e intuitivos são positivos para os usuários, seu melhor firewall.

Julia Spain
Sócia de Cyber Security Services
da KPMG no Reino Unido

Confiança no CISO

As organizações demonstram altos níveis de confiança e forte crença na capacidade do CISO de realizar tarefas cruciais.

79% das organizações estão confiantes que os CISOs podem mapear com precisão onde os dados críticos da empresa estão localizados.

3/4 estão confiantes de que os CISOs podem identificar quais são os dados mais importantes, as "jóias da coroa".

78% estão confiantes de que os CISOs sabem quanto dos seus dados confidenciais estão com terceiros e devidamente protegidos.

Fonte: *KPMG Cyber Trust Insights 2022.*

As empresas devem deixar de pensar em segurança corporativa em termos binários. No ambiente de hoje, que é bastante dinâmico, o conceito de "seguro" e "não seguro" é volátil. Em vez disso, os CISOs devem trabalhar para aumentar a inteligência organizacional em torno da segurança cibernética por meio da conscientização; processos simples, intuitivos e focados nos usuários; e manter uma base de funcionários e equipe executiva bem informados.

A experiência do cliente também se aplica à segurança

É crucial focar na construção de processos realistas para usuários responsáveis enquanto mantém meios para detectar e combater rapidamente atividades maliciosas. Tudo se resume à facilidade de uso, experiência do cliente e planejamento em torno da segurança cibernética dentro do contexto das prioridades de toda a empresa - as necessidades do negócio – em vez de pensar nisso apenas como um imperativo regulatório.

Avanços na tecnologia podem ajudar. De IA defensiva, *machine learning* e *chatbots* a criptografia em nuvem, *blockchain*, e aplicações de detecção e resposta estendida (XDR), são partes vitais deste quebra-cabeça. Da mesma forma é importante criar uma força de trabalho mais consciente em segurança, guiada por uma governança de TI consistente, para inspirar as pessoas a abordar as comunicações digitais com a devida cautela.

> ***A tecnologia sozinha não pode resolver o problema. Bilhões em fluxo de capital são direcionados para a segurança cibernética e milhares de empresas oferecem inúmeras ferramentas, mas as empresas ainda estão vulneráveis. Por que? Porque os agentes maliciosos possuem acesso às mesmas ferramentas.***

Prasad Jayaraman
Diretor de Cyber Security Services
da KPMG nos EUA

Os CISOs devem pensar em como podem ajudar os funcionários a fazer a coisa certa de forma instintiva e projetar controles de segurança que os ajudem a fazer isso.

Como um esforço contínuo e em constante evolução, a segurança cibernética apresenta muitas oportunidades para estabelecer novas ferramentas e controles. Ainda assim, incentivamos as organizações a considerá-la desde o início, juntamente com o elemento humano. As principais iniciativas transformadoras têm muitos componentes, e um deles deve ser a segurança. Integrar a segurança em iniciativas orientadas a processos, como DevSecOps, tecnologia operacional e suprimentos, pode ser uma maneira eficaz e discreta de motivar as pessoas a se comportarem de forma segura e funcionarem como *firewalls* humanos sem se sentirem sobrecarregados.

> ***Além da tecnologia, os CISOs devem olhar para o aspecto humano. Da educação e treinamento à conscientização geral, é importante construir uma cultura sólida de segurança em toda a organização.***

Eddie Toh
Sócio de Cyber Security Services
da KPMG em Singapura

As equipes de segurança podem aprender muito com a maneira como as organizações melhoram a experiência do cliente. Os controles de segurança internos devem ser fáceis de usar, ou os funcionários podem se sentir motivados a ignorar esses processos. Considere incluir especialistas em experiência do cliente no design de controles.

Os processos de segurança também devem ser humanos, direcionados e pensados para usuários internos. Fazer com que o indivíduo faça julgamentos, explique o contexto, e trace um paralelo entre comportamento seguro em suas vidas pessoais e profissionais, tornando as ações em educativas. Assim as pessoas podem desempenhar o seu papel na segurança e não ser vistas como o elo mais fraco.

Saiba mais

Firewall Humano

Superando o fator humano nos riscos de segurança cibernética.

Synthetic identity fraud

Um problema de US$ 6 bilhões.

Want better cyber security? Don't check that box.

A maior ameaça à segurança da sua organização pode não ser ataques de *ransomware* ou *phishing*. Pode ser a tendência de achar que as coisas estão concluídas.

Consideração 3

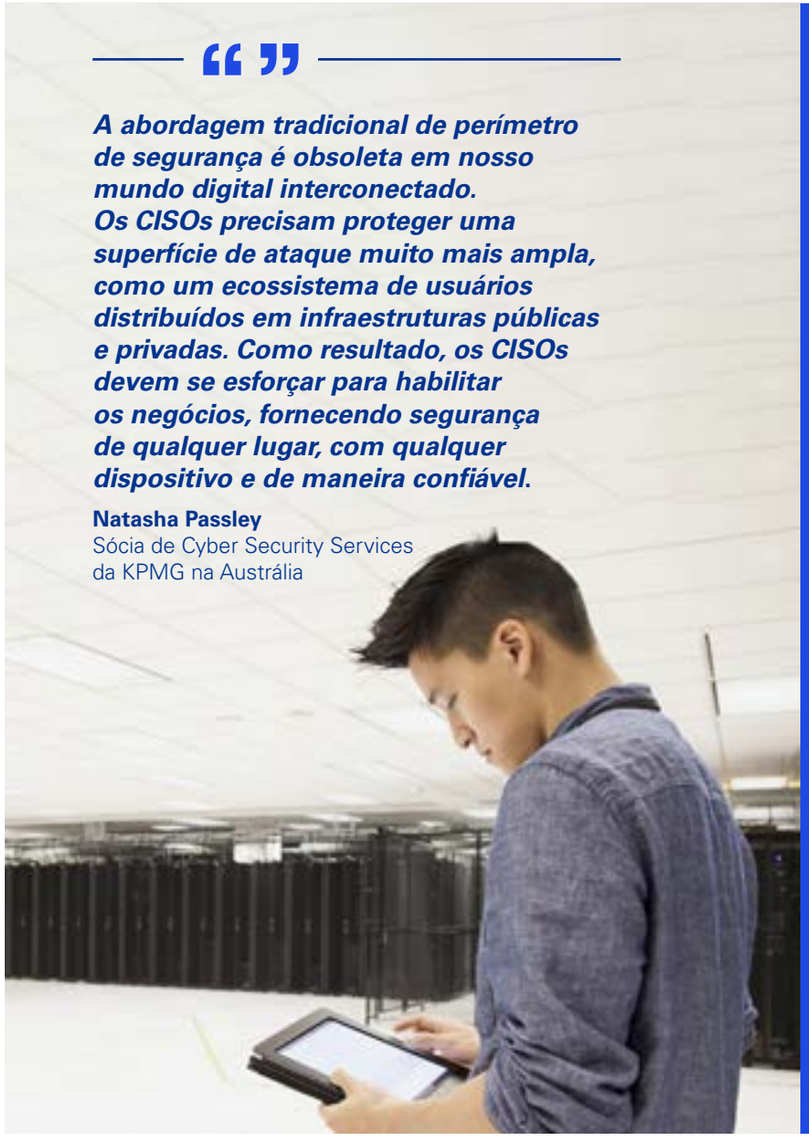
Protegendo um futuro sem perímetro e centrado em dados

Não é surpresa que os modelos operacionais de negócios tenham mudado fundamentalmente na última década, tornando-se mais fluidos, centrados em dados, com ecossistemas conectados de parceiros internos e externos e provedores de serviços. Neste mundo de computação distribuída, para reduzir a dimensão de possíveis falhas ou violações, os CISOs e as equipes de segurança devem adotar abordagens muito diferentes, como *Zero Trust*, serviço de acesso seguro de borda (*Secure Access Service Edge - SASE*) e arquitetura *mesh* de segurança cibernética (CSMA).

Hoje, o imperativo claro do negócio é permitir que os funcionários, clientes, fornecedores e outros terceiros se conectem perfeitamente de forma remota e segura. O desafio de segurança associado é que, em um ambiente sem perímetro definido, as organizações não podem mais confiar em todos os usuários e dispositivos.

Zero Trust para negócios sem perímetro

Abordagens de *Zero Trust* podem diminuir a amplitude de uma interrupção ou violação dos serviços e limitar o impacto para que o incidente possa ser melhor gerenciado e contido.



> ***A abordagem tradicional de perímetro de segurança é obsoleta em nosso mundo digital interconectado. Os CISOs precisam proteger uma superfície de ataque muito mais ampla, como um ecossistema de usuários distribuídos em infraestruturas públicas e privadas. Como resultado, os CISOs devem se esforçar para habilitar os negócios, fornecendo segurança de qualquer lugar, com qualquer dispositivo e de maneira confiável.***
>
> **Natasha Passley**
> Sócia de Cyber Security Services da KPMG na Austrália

Segurança de dados é uma questão fundamental para *stakeholders*

Em ambientes sem perímetro definidos, as preocupações sobre como os dados são protegidos, usados e compartilhados são os principais fatores que minam a confiança dos *stakeholders* na capacidade da organização usar e gerenciar seus dados.

28% dos executivos identificam "a falta de confiança nos mecanismos de governança atuais" como um dos principais fatores que minam a confiança dos *stakeholders* em usar e gerenciar seus dados.

32% também identificam "falta de clareza sobre por que os dados são necessários para um determinado serviço, e os benefícios de compartilhar ou fornecer dados" como outro fator.

36% estão preocupados com a forma que seus dados são protegidos.

35% estão preocupados com a forma que seus dados são usados ou compartilhados.

Fonte: *KPMG Cyber Trust Insights 2022.*

Os serviço de acesso seguro de borda (SASE), arquitetura *mesh* de segurança cibernética (CSMA), baseadas no conceito *Zero Trust*, têm princípios comuns em como a segurança é organizada, distribuída e alinhada em toda a rede. Talvez o mais importante, no entanto, é que à medida em que mais empresas adotam uma mentalidade centrada na nuvem, tornou-se fundamental mover os mecanismos de segurança para perto dos dados.

Como um guarda-chuva sobre o atual ambiente sem perímetros de negócios, *Zero Trust* é um *framework*, uma maneira de pensar sobre como o *design*, capacitação da segurança e gestão de acesso precisam mudar ao longo do tempo. O modelo de *Zero Trust* complementa a convergência de serviços sob um modelo SASE e a holística e analítica arquitetura *mesh* de segurança cibernética.

Novos modelos de identidade

O gerenciamento descentralizado de identidade de acesso é uma responsabilidade essencial dos CISOs e uma função do tráfego de rede. O conceito de tráfego norte-sul, que é do usuário para o recurso, é focado em identidade, enquanto o tráfego leste-oeste, de movimento lateral dentro do ambiente, é relacionado com segmentação e outros controles.

A ligação entre dados e identidade é inconfundível. Em um ambiente sem perímetro definido, não há *Zero Trust*, SASE, ou arquitetura *mesh* de segurança cibernética sem um foco claro em identidade e governança de dados.

Para os CISOs, o desafio com a metodologia *Zero Trust* é verificar se os dispositivos e os usuários são quem dizem ser e se são confiáveis. Isso exige que os CISOs pensem em segurança a partir de uma perspectiva de verificação de identidade, concentrando-se no mínimo privilégio de acesso para os usuários dentro de sua empresa e os muitos terceiros com quem interagem.

Zero Trust na prática

Os princípios do *Zero Trust* devem ser definidos em relação a todos os cenários, usuários e *endpoints*, representando um pilar-chave dos princípios fundamentais e do programa de segurança. Os CISOs devem desempenhar um papel fundamental não apenas na instituição do modelo e da abordagem do *Zero Trust*, mas no estabelecimento de políticas, na definição de padrões, na concepção de soluções de *software* e na montagem de um conselho de segurança amplo, abrangendo vários líderes de tecnologia e negócios.

Outro desafio é em torno de financiamento e orçamento. Os CISOs devem ser capazes de explicar a estrutura em torno da abordagem *Zero Trust*, para que os executivos e outros líderes corporativos entendam que o investimento não é apenas mais uma nova tecnologia, mas uma nova maneira de projetar um futuro para os negócios.

Encontrar um meio termo entre estruturas *on* e *off-premises* é um grande desafio, particularmente com tecnologias nativas em nuvem. Muitas empresas estão pensando em mover seus processos para a nuvem, mas muitas vezes a infraestrutura legada não pode ser totalmente adaptada aos requisitos tecnológicos atuais.

Os CISOs de grandes organizações têm o desafio de gerenciar uma postura de segurança que abrange um ecossistema *on-premises* e *off-premises*, e que pode resultar em altos custos operacionais no curto prazo. Os clientes que buscam a adoção completa em ambientes em nuvem devem considerar os mesmos princípios do *Zero Trust on-premises* para novos sistemas implementados na nuvem. Eles também devem levar em consideração o impacto da mudança no modelo operacional, tal como, um modelo de responsabilidade compartilhada bem gerenciado com um provedor de nuvem pode ser fundamental para ajudar a garantir uma arquitetura de nuvem segura.

> ***"O ecossistema de identidade explodiu no mundo econômico em que operamos hoje. Desta forma, as organizações só conseguem monitorar com precisão seres humanos e máquinas através da gestão de suas identidades."***

Deepak Mathur
Diretor de Cyber Security Services da KPMG nos EUA

Saiba mais

The convergent future of identity

O que está por vir sobre o gerenciamento de identidades e acessos.

Verifique tudo. Não confie em nada

Porque o *Zero Trust* é o caminho a seguir.

Safeguard your digital environments from all angles

As cinco etapas para começar a jornada de *Zero Trust*.

Consideração 4

Novas parcerias, novos modelos

Foram-se os dias em que as equipes de segurança se concentravam exclusivamente nos sistemas de TI da organização. Os CISOs precisam entender o momento de frear ou acelerar quanto a terceirização de esforços de segurança cibernética e determinar quais habilidades manter internamente hoje e no futuro. A segurança tornou-se uma prioridade de negócio, entregue através de um modelo de responsabilidade compartilhada entre a organização e os provedores de serviços.

Atualmente, os CISOs estão suportando a estratégia de negócios em toda a organização, desde a tecnologia operacional e segurança de produtos, até ecossistemas complexos da cadeia de suprimentos. Cada vez mais, as organizações reconhecem que a inovação se beneficia da colaboração entre várias fontes alinhadas, desde a cadeia de suprimentos e atendimento ao cliente até o *design* organizacional e a segurança da informação.

Essa combinação de inovação entregue a um preço competitivo para os clientes, onde quer que eles estejam, é como as empresas ganham vantagem competitiva.

No entanto, algumas organizações sofrem para implementar uma segurança robusta em larga escala, principalmente por causa da falta de talentos e habilidades, e é por isso que eles estão procurando por terceirizações, serviços gerenciados e transição para a nuvem.

> ***Embora muitas organizações terceirizem certos processos de negócios com fornecedores externos, a segurança de dados, gerenciamento de identidade e acesso, e seus controles relacionados, permanecem responsabilidades internas.***

Markus Limbach
Sócio de Cyber Security Services
da KPMG na Alemanha

Parceirias confiáveis

Espera-se que as colaborações externas também sejam vitais para o sucesso de ecossistemas hiperconectados, mas há barreiras práticas que impedem a colaboração.

79% dizem que a colaboração construtiva com fornecedores e clientes é vital, mas apenas **42%** reportaram fazer isso.

60% admitem que suas cadeias de suprimentos estão deixando-os vulneráveis aos ataques.

78% dos executivos estão confiantes de que o CISO pode proteger seus dados em toda sua cadeia de suprimentos.

Fonte: *KPMG Cyber Trust Insights 2022.*

Saber o que manter

Assim como as empresas não podem simplesmente terceirizar a segurança, elas também precisam dos talentos e das habilidades certas internamente. É preciso conhecimento especializado para estabelecer uma estrutura de controle e monitoramento reproduzível, sob a qual a equipe interna e os fornecedores terceirizados possam operar de forma eficaz. Uma das chaves é entender o que reter internamente em termos de responsabilidades de segurança e, em seguida, identificar a estratégia de aquisição mais eficaz para talentos nessas áreas.

Usando a nuvem como exemplo, estrategicamente, os CISOs têm que incorporar vários papéis (operador, orquestrador e integrador) para alinhar a as capacidades necessárias da equipe e terceiros, gerenciar riscos, governança e reportes. Isso não pode ser totalmente terceirizado. As organizações podem terceirizar a preparação e o planejamento, mas idealmente, alguém interno que entenda os ambientes de negócios e segurança, e o potencial impacto de um incidente cibernético, deve gerenciar o envolvimento organizacional e controle de qualidade.

> ***A arquitetura de controles cibernéticos em um ecossistema de nuvem demanda um conjunto de habilidades diferentes em relação ao da engenharia de segurança tradicional. A capacidade de gerenciar segurança entre organizações, APIs e tecnologias diferentes na velocidade dos negócios requer um nível de sofisticação que muitas organizações não possuem. É uma capacidade que os CISOs devem aspirar.***
>
> **Matt O'Keefe**
> Sócio de Cyber Security Services
> da KPMG na Austrália

Encontrar a combinação certa de habilidades

É crucial, e mais fácil falar do que fazer, que os CISOs entendam suas responsabilidades internas e externas, explorem diferentes modelos e disciplinas, e gerenciem essas complexidades para estabelecer os controles apropriados.

Trabalhar com provedores de segurança externos requer um conjunto único de habilidades, com foco em gerenciamento e governança, em vez de habilidades técnicas. Independentemente da quantidade de trabalho terceirizado, as organizações precisam de conhecimentos e capacidades de segurança dentro de casa. Também é essencial que o diálogo entre as partes seja claro e constante para garantir que os controles implementados e os reportes de KPIs sejam adequadamente gerenciados. Além disso, é crucial chegar a um acordo sobre processos claros de resposta a incidentes e executar simulações.

Os CISOs precisam avaliar sua base de habilidades regularmente e garantir que a organização esteja preparada para ser um consumidor inteligente e colaborativo dos serviços gerenciados de segurança e de nuvem. Fazer isso requer o entendimento das futuras necessidades de infraestrutura do negócio e determinar qual deve ser o papel da segurança para fornecer o melhor suporte. A palavra-chave é "futuro", olhe para três a cinco anos e trabalhe agora, em vez de apenas olhar para as necessidades atuais de segurança da empresa.

Saiba mais

Third-party risk management outlook 2022

Tempo de agir.

Evolving vendor, operational and strategic risks

Gestão de riscos de terceiros.

Third party and cloud: Regulatory challenges

As empresas estão formando relacionamentos mais frequentes e complexos com terceiros, introduzindo novos e elevados riscos.

Consideração 5

Confiança na automatização

Na corrida para inovar e aproveitar as tecnologias emergentes, preocupações com segurança, privacidade, proteção de dados e ética, embora ganhem mais atenção, são muitas vezes ignoradas ou esquecidas. Essa negligência pode levar as empresas a sabotar seu potencial, especialmente com novas regulamentações de privacidade para Inteligência Artificial (IA) no horizonte.

Historicamente, a IA tem recebido uma série de experimentos de ciência de dados, com uma porcentagem relativamente pequena de projetos em produção. Agora, a era do *machine learning* (ML) aplicado no mundo real começou e nos próximos 18 a 24 meses devemos esperar ver mais desses projetos serem lançados.

Houve muitas tentativas e erros, mas os aprendizados podem levar a um enorme sucesso em forma de mecanismos de recomendação, ferramentas de apoio à decisão, simulações sofisticadas e redes neurais que podem gerar centenas de milhões de dólares para muitas organizações.

Automatizar tarefas simples e repetitivas libera tempo e cria eficiências para que os profissionais possam se concentrar em iniciativas que exigem pensamento complexo, deliberativo e criativo. A IA está sendo usada em muitos setores. No setor bancário, os *bots* estão ajudando a decidir os produtos e serviços mais adequados para os clientes e, no setor de seguros, o uso da tomada de decisões automatizada na avaliação de crédito dos candidatos está sendo explorado.

> ***Saber como a empresa está pensando em usar o machine learning é realmente importante para toda a equipe de segurança poder agregar valor. Uma vez tendo esse entendimento, a equipe de segurança pode examinar os sistemas que usarão, identificar os dados de entrada corretos e então, trabalhar para lidar com os riscos adversariais ao usar seus sistemas de IA.***
>
> **Michael Gomez**
> Diretor de Cyber Security Services
> da KPMG dos EUA

Desafios da IA e ML

Há crescentes preocupações sociais e comerciais sobre as implicações éticas, de segurança e de privacidade sobre a adoção de soluções de IA e ML para análises de *big data*.

78% concordam que IA e ML trazem desafios únicos de segurança cibernética.

3 em 4 dizem que IA e ML levantam questões éticas fundamentais.

76% dos executivos concordam que a adoção de IA/ML requer salvaguardas adicionais sobre como estes sistemas de IA/ML são treinados e monitorados.

76% concordam que a adoção de IA/ML requer transparência na forma como as usamos.

Fonte: *KPMG Cyber Trust Insights 2022*.

Construindo modelos de IA confiáveis

As empresas estão utilizando a IA adequadamente e obtendo o resultado mais produtivo? No caso de uso de seguradoras há situações em que o algoritmo toma decisões a respeito do proponente que residem em regiões específicas. Aqueles que vivem em bairros mais carentes foram classificados de forma diferente daqueles que vivem em bairros de classe mais alta. Como resultado, os prêmios diferem com base no endereço do proponente. O viés da IA pode ser visto como discriminatório e precisa ser controlado.

Historicamente as aplicações foram desenvolvidas para funcionar uniformemente, e a relação entre as entradas e saídas correspondentes não deveria mudar. Essa era a base de testes dos desenvolvedores. O usuário final decidia se gostava de usar o aplicativo e se queria ou não continuar fazendo negócios com o desenvolvedor.

As ferramentas de ML e IA são projetadas para aprender e evoluir. E essa evolução representa uma enorme transformação na forma como as empresas devem pensar sobre esses sistemas, como elas podem se adequar ao seu propósito.

As pessoas têm sentimentos e entendimentos confusos relacionados à IA. E muitas empresas simplesmente não têm profissionais suficientes que entendam de IA, e muito menos como protegê-la.

As máquinas, assim como DevOps, estão começando a assumir um papel na redução do ciclo de desenvolvimento e na garantia da entrega contínua.

> ***A IA é poderosa, mas pode ser prejudicial para os indivíduos se a tomada de decisão automatizada for inadvertidamente tendenciosa ou discriminatória.***

Sylvia Klasovec Kingsmill
Sócia de Privacy
da KPMG no Canadá

E se as empresas não trouxerem segurança para esse ambiente movido pelas máquinas, ela pode nunca atingir escala porque as pessoas podem simplesmente não confiar na solução. Por isso, 76% dos executivos concordam que a adoção de IA e ML requer salvaguardas adicionais sobre como os sistemas são treinados e monitorados.[5]

IA e privacidade de dados

A IA alavanca muitos princípios fundamentais de privacidade, capacitando as equipes de segurança para, por exemplo, analisar os dados dos clientes mais profundamente, por exemplo, mas as organizações precisam pensar na proporcionalidade entre a quantidade de dados coletados em relação aos requisitos de minimização de dados de algumas regulamentações. Da mesma forma, considerando que a IA tem o potencial de incorporar vieses existentes, deve haver transparência em torno de seus resultados.

Reguladores, governo e indústria devem trabalhar juntos. A regulamentação da IA não é apenas uma questão de privacidade. Isso exige que os cientistas de dados trabalhem com especialistas em privacidade para determinar quais requisitos devem ser incorporados à tecnologia para torná-la segura, confiável e sensível à privacidade. Os governos precisam estabelecer uma agenda digital abrangente para inspirar o mercado a continuar investindo em inovação. Enquanto vários órgãos governamentais às vezes parecem abordar a IA como uma competição, reguladores também estão começando a tentar limitar as aplicações das novas habilidades de IA que podem ser intrusivas e de alto risco.

Após a adoção dos princípios do G20 para IA confiável, houve grandes desenvolvimentos na gestão e regulamentação de riscos de IA. Singapura estabeleceu seu padrão de segurança de IA, o NIST (*National Institute of Standards and Technology*) publicou seu *framework* de gerenciamento de risco de IA e a regulamentação da União Europeia (EU) está em discussão. Espera-se que a regulamentação neste tópico tenha um impacto tão significativo quanto a LGPD/GDPR teve na privacidade. Muitas empresas precisam se preparar.

Saiba mais

Is my AI secure?

Compreendendo os riscos cibernéticos da inteligência artificial para o seu negócio.

Trust in artificial intelligence: Global insights 2023

Pesquisa global que explora a confiança das pessoas na IA, e seus benefícios e riscos para os negócios e sociedade.

The path to transparency — and trust

Pesquisa de responsabilidade de dados corporativos.

[5] *KPMG Cyber Trust Insights 2022. Op cit.*

Consideração 6

Protegendo um mundo inteligente

Empresas de quase todos os setores estão mudando para uma mentalidade de produto, focando em desenvolvimento de serviços conectados e no gerenciamento dos dispositivos que os suportam. Os CISOs e suas equipes estão sendo envolvidos em discussões com equipes de engenharia, desenvolvimento e suporte ao produto, à medida que as organizações percebem que a segurança de seus produtos é igualmente importante.

No ambiente focado em produtos inteligentes de hoje, alguns *drivers* ou facilitadores emergentes estão dominando:

5G
Oferece velocidade, hiperconectividade e latência reduzida.

Computação quântica
Reduz drasticamente o tempo de cálculo e processamento.

Arquiteturas de confiança
Ajuda a garantir que dados e identidades sejam seguros e confiáveis de um dispositivo conectado para outro.

***Software* 2.0**
Código ágil e escrito por IA que pode reduzir a complexidade, e diminuir o tempo de desenvolvimento de meses para semanas.

IA aplicada
Aplicação real da inteligência artificial para aprimorar e acelerar para o desenvolvimento de produtos inteligentes.

> ***O ritmo da inovação tecnológica não está diminuindo, e muitas vezes os reguladores e equipes de segurança são forçados a se adequarem. Os CISOs não devem esperar pela próxima onda de regulamentações, nem confiar apenas na regulamentação atual, em vez disso, devem adotar uma abordagem proativa e pragmática para implementar controles de segurança em todo o ciclo de vida do produto e na cadeia de suprimentos. Isso não é algo pequeno, sendo que o sucesso provavelmente dependerá de quão bem os CISOs se envolvem com outras funções por toda a organização.***

Walter Risi
Sócio de Cyber Security Services da KPMG na Argentina

Panorama de segurança cibernética dos CEOs

Os recentes desafios da segurança cibernética estão dando aos CEOs uma visão mais clara de como eles podem estar bem ou mal preparados.

24% dos CEOs reconhecem que estão despreparados para um ataque cibernético, em comparação com 13% em 2021.

56% dizem que estão preparados.

3/4 dizem que suas organizações têm um plano para lidar com ataques de *ransomware*.

3 a cada 4 dizem que proteger o ecossistema e cadeia de suprimentos de seus parceiros é tão importante quanto suas próprias defesas cibernéticas.

Fonte: *KPMG 2022 CEO Outlook*

Existem muitos riscos relacionados a dispositivos inteligentes, como senhas padrão fracas, criptografia fraca ou ausente, falha no fornecimento tempestivos de atualizações de *software*, *malware*, falta de proteção para vulnerabilidade de negação de serviço, entre outros. Os CISOs devem perceber que para esses dispositivos, a segurança não é baseada apenas na tríade da CID (confidencialidade, integridade, disponibilidade). A segurança também é uma consideração importante porque sistemas do mundo real, hiperconectados e tangíveis, estão envolvidos. Os profissionais de segurança cibernética devem aplicar esses riscos à um *framework* de segurança, pois ataques direcionados em escala são uma possibilidade real.

À medida que nos movemos para um mundo de ecossistemas, sensores, produtos e dispositivos conectados e eles vem se tornando alvos de ataques sofisticados, os reguladores estão colocando uma maior importância sobre como as organizações incorporam a segurança em todo o ciclo de vida do produto.

Existem inúmeros desafios na integração da segurança no ciclo de vida de um produto inteligente, incluindo o monitoramento proativo, a identificação e o tratamento das vulnerabilidades cibernéticas. Um dos principais desafios do CISO deve ser trabalhar junto ao departamento de controle de qualidade para incorporar a segurança nos processos de desenho de produtos e inspeções pré-lançamento.

Motoki Sawada
Sócio de Technology Risk Services
da KPMG no Japão

Aplicando segurança em um mundo hiperconectado

Os CISOs devem considerar riscos relacionados a dispositivos inteligentes em quatro componentes principais que abrangem o ciclo de vida, e cada um com prioridades específicas relacionadas ao DevSecOps: 1 - desenvolvimento de produtos, do design da implementação ao lançamento do produto; 2 - gestão da cadeia de suprimentos em expansão; 3 - manutenção e atualização de *software*; e 4 - o usuário final, independente de ser outra empresa ou consumidor. Estas quatro áreas irão ajudar os CISOs a organizar seu plano de segurança e ter a confiança de que seu produto é o mais seguro possível. Tornou-se essencial que os CISOs tenham uma linha de conexão com todas as áreas de negócio.

Os CISOs devem trabalhar com toda a empresa para garantir que a segurança cibernética seja vista como uma prioridade de gerenciamento de riscos. Além disso, apenas pensar em segurança em termos dos processos técnicos aplicados aos dispositivos é uma abordagem insuficiente. Deve-se considerar um impacto mais amplo em áreas como cadeia de suprimentos e atendimento ao cliente.

Jayne Goble
Diretora de Cyber Security Services
da KPMG no Reino Unido

Um *software* incorporado em dispositivos inteligentes tem a complexidade adicional de não ser facilmente atualizado, o que é atribuível a vários fatores, como conectividade e incapacidade de aplicar *patches* durante o uso, dependendo da criticidade do dispositivo. Isso representa um desafio adicional para os desenvolvedores: ter que incorporar, de forma antecipada, mecanismos de garantia, bem como ter um mapeamento de ativos de software organizado e atualizado, que permite às empresas detectar e, eventualmente recolher, dispositivos no caso de descoberta de vulnerabilidades críticas enquanto os mesmos estiverem em uso.

A segurança cibernética tornou-se um diferencial de mercado. Talvez pareça óbvio, mas é importante para os clientes atuais e potenciais, e todo o mercado, saber que o programa de segurança cibernética da organização, e os controles de dispositivos em particular, estão em constante evolução, nunca estáticos e gerenciados juntamente com o ciclo de vida do dispositivo. É esperado que os reguladores em todo o mundo tenham um interesse crescente na segurança desses sistemas e nos padrões mínimos exigidos.

Saiba mais

Relatório Anual 2022: Segurança Cibernética para os Sistemas de Controle Industrial (ICS)

Superando os obstáculos para o verdadeiro progresso à medida que as ameaças cibernéticas crescem.

Um caminho para a resiliência cibernética industrial

Avaliando e se preparando contra vulnerabilidades cibernéticas em setores industriais.

Accelerating OT security for rapid risk reduction

Protegendo os ambientes de tecnologia operacional à medida que se tornam cada vez mais digitalizados e conectados.

Consideração 7

Combatendo adversários ágeis

O tempo desde o comprometimento inicial até a ativação do *ransomware* em toda a empresa está diminuindo. Cada vez mais, atacantes cibernéticos podem invadir os sistemas com ferramentas automatizadas e acelerar a sua exploração. As operações de segurança devem ser otimizadas e estruturadas para acelerar a recuperação de serviços prioritários quando ocorre um incidente, o que pode reduzir o impacto em clientes, consumidores e parceiros.

Os atacantes cibernéticos têm dois motivos aparentes: exploração e disrupção. A exploração de sistemas tem foco em roubar ou manipular dados, seja por inteligência ou fraude, e disrupção para extorsão ou ganho político. As táticas podem ser bem diferentes.

Alguns atacantes patrocinados por estados se concentram em infraestrutura crítica, como oleodutos, plantas de energia elétrica e sistemas financeiros. A missão é causar danos ou caos e exercer influência política ou econômica para beneficiar o atacante e seu patrocinador. A intenção é monetizar a adversidade dos outros.

A probabilidade do sucesso de incidentes de segurança cibernética aumentou substancialmente, resultando no crescimento ataques de *ransomware* nos últimos anos. E provavelmente continuará crescendo se os profissionais de segurança não dificultarem para os atacantes.

> ***Os invasores vão obter acesso, e isso é um fato que temos que aceitar. Trata-se de reduzir seu tempo de permanência. O mais crítico é se a presença do invasor e suas ações são detectadas dentro de horas, dias, semanas ou meses.***

Charlie Jacco
Diretor de Cyber Security Services da KPMG nos EUA

Times de segurança estão custando para acompanhar

As equipes de segurança cibernética estão sob pressão para acompanhar as ameaças em evolução, e enfrentando a escassez de talentos o que frequentemente prejudicam os esforços de segurança.

Mais de 1/2 das organizações admitem que estão atrasadas em termos de segurança cibernética.

Acima de 50% estão muito ou extremamente confiantes no combate a várias ameaças cibernéticas, incluindo de grupos de crime organizado, *insiders* e de cadeias de suprimentos comprometidas.

59% concordam que os invasores estão explorando vulnerabilidades em compras e cadeia de suprimentos, mas não sabem se suas defesas são fortes o suficiente para impedi-los.

#1 desafio interno para alcançar as metas de segurança cibernética é a falta de habilidades cruciais (40%).

Fonte: *KPMG Global Tech Report 2022.*

Para piorar a situação, o trabalho híbrido expandiu a superfície de ataque, aumentando o número de *endpoints* potencialmente vulneráveis. Somando-se aos desafios, o "*shadow IT*" dentro das empresas geralmente inclui aplicações de negócios e SaaS (*software as a service*) sobre o qual os CISOs e CIOs têm entendimento e conhecimentos limitados.

Aprimorando a estratégia das operações de segurança

O tempo importa. Quão rápido um invasor pode ser detectado, contido e os serviços podem ser restaurados, e com isso, como podemos minimizar o comprometimento das informações e do sistema? É menos sobre como eles conseguiram e mais sobre quais informações eles obtiveram. Foram dados críticos? Houve vazamento e/ ou está mantido como "refém"?

O tempo que os invasores levam para passar do comprometimento inicial para a exploração bem-sucedida dos sistemas está reduzindo. Atualmente isso pode levar apenas alguns dias, ou até menos, para um invasor implantar um *ransomware* em uma empresa. Os invasores também estão cada vez mais criativos na automação de suas táticas, chegando ao ponto de explorar o potencial da IA para ajudá-los a planejar e orquestrar seus ataques. Conclusão: os CISOs e suas equipes têm consideravelmente menos tempo para detectar intrusões e tomar ações de contenção rápidas e decisivas.

Há uma estrutura triangular nos centros de operações de segurança (SOC) de hoje, com uma time pequeno, mas especializado, de *threat-hunt* no topo, vários investigadores de nível 2 no centro e inúmeros analistas de alerta de nível 1 na parte inferior, testando um volume cada vez maior de alertas. Esse triângulo precisa ser invertido. Os SOCs de hoje exigem menos Nível 1, mais Nível 2 e consideravelmente mais *threat-hunters* à procura de eventos potencialmente catastróficos. Uma forma para de fazer isso e responder no ritmo e volume dos ataques é automatizando o Nível 1.

Um SOC eficaz exige o aproveitamento de tecnologias mais avançadas, agrupamento dos dados mais relevantes, confiança nas ferramentas disponíveis para gerenciar os alertas e a estabelecendo uma correta parceria entre analistas humanos, ML e automação de processos robóticos. Ao fazer isso você poder estabelecer novas fontes de dados que fornecem maior contexto de negócios para a análise de possíveis ataques, explorando a fusão de operações de segurança cibernética com segurança física, prevenção de fraudes e gerenciamento de ameaças internas.

Alcançar esse nível de confiança é um desafio para a maioria dos departamentos e organizações de segurança. Suponha que os CISOs e suas equipes possam aproveitar a IA para fazer esse trabalho de triagem, examinar o *firewall* e o sistema de gerenciamento de informações e eventos de segurança (SIEM), além de avaliar as várias fontes de inteligência de ameaças e ferramentas de *scan* de vulnerabilidades. Eles podem começar a confiar. É para onde o SOC se encaminha, mas ainda não chegou lá.

Aproveitar e reter conhecimentos técnicos

Quanto aos talentos, a manutenção e retenção devem ser prioridade. Muitas organizações precisam de ajuda para criar um modelo e plano de carreira durável para o SOC. As equipes são consumidas com o monitoramento do sistema e são colocadas mais pessoas para atuar no problema em vez de treinar adequadamente os profissionais que já estão trabalhando.

Como resultado, as pessoas se sentem presas e acabam buscando outros empregos, deixando os CISOs com um ciclo vicioso perpétuo no SOC. Tudo porque eles não priorizaram o treinamento. E enquanto isso, os atacantes evoluem continuamente suas técnicas, táticas e estratégias, tornando-se melhores e mais rápidos no que fazem, os CISOs não têm os recursos para acompanhá-los.

Saiba mais

KPMG global tech report 2022

Descubra como os líderes estão usando a tecnologia para impulsionar seus negócios e fortalecer a maturidade digital.

Really ready for a ransomware attack?

Desafiando as premissas de negócios sobre a prontidão para riscos, hoje e amanhã.

Uma Ameaça Tripla nas Américas

Uma revisão dos riscos de fraude, conformidade e segurança cibernética enfrentados pelas Américas.

Consideração 8

Seja resiliente quando - e onde - importa

Todo sistema de segurança tem suas falhas. Há um ar de inevitabilidade que, em algum momento, uma organização sofrerá um incidente, grande ou pequeno, ou provavelmente mais de um. Os reguladores estão cada vez mais focados em cenários plausíveis e pressionando as empresas, particularmente aquelas em indústrias estrategicamente importantes como energia, finanças e saúde, a serem resilientes e organizadas para se recuperarem.

Talvez o problema mais evidente seja que as organizações muitas vezes não veem que o impacto, e a recuperação, de um incidente cibernético podem ser prolongados. Normalmente não é um evento de 72 ou 96 horas. Deve-se assumir os piores cenários, como a interrupção de negócios em larga escala. Em muitos casos os líderes seniores não avaliaram totalmente os links de tecnologia em toda a empresa ou as dependências operacionais do negócios para com os mesmos - pagamento de pessoal e de fornecedores, comunicação com clientes e investidores.

"É fundamental que os CISOs se envolvam com os negócios desde o início e com frequência, para ajudar a garantir uma estratégia de resiliência clara, mas flexível, e adequadamente definida com antecedência, em vez de testá-la no meio de uma crise."

Dani Michaux
Sócia de Cyber Security Services
da KPMG na Irlanda

O panorama regulatório

Legisladores e reguladores estão atentos e aumentando suas demandas por transparência e supervisão. Muitas organizações estão preocupadas por percorrerem um cenário regulatório global cada vez mais complexo.

36% se preocupam com sua capacidade de atender às novas e atuais regulamentações de segurança cibernética quando as atividades são terceirizadas para provedores de serviços digitais.

31% se preocupam com as crescentes demandas em torno de infraestruturas críticas, que é objeto de uma crescente regulamentação no Reino Unido, na UE e nos EUA.

28% se preocupam com as novas e atuais regulamentações relacionadas à resiliência de seus principais sistemas.

26% se preocupam com requisitos de reportes de incidentes mais rigorosos.

Fonte: *KPMG Cyber Trust Insights 2022.*

Muitas organizações ainda precisam considerar o que precisam proativamente fazer para serem resilientes. Elas presumem que têm um plano de backup e controles de segurança suficientes. E se não tiverem um plano para um cenário específico e as operações de negócio pararem? Isso tem sérias consequências financeiras e reputacionais, muito mais que regulatórias. Há também um componente psicológico.

Os CISOs precisam ter conversas contínuas com seus pares *C-level* e com o conselho sobre a natureza e motivações dos atacantes: quanto mais forte eles o atingem, mais provável é que você pague, e eles sabem disso. A maioria das organizações ainda luta para entender o que realmente estão enfrentando.

Coordenação proativa é necessária, dentro e fora da batalha

Durante o caos de um ataque ativo, o principal objetivo do CISO é fornecer ao negócio os *insights* necessários para continuar operando. Eles devem se afastar dos detalhes técnicos do dia-a-dia e se envolver proativamente e estrategicamente com a organização sobre a gravidade da situação e como, coletivamente, a empresa deve responder se quiser se recuperar rapidamente.

Uma grande parte do trabalho do CISO é ser um comunicador e articular, em toda a empresa, sobre o potencial impacto no negócio de uma violação e o valor de manter a segurança cibernética em mente. Além disso a resposta e a recuperação, componentes da resiliência, exigem coordenação. Isso pode ser alcançado através de um pequeno "Comitê de Crise" composto pelo CISO, CEO, CFO e o representante do Jurídico.

Infelizmente, esse importante grupo não existe formalmente em muitas empresas porque elas acham que isso não acontecerá com elas. E se isso acontecer, eles acreditam que seu plano de continuidade de negócios, que em muitos casos foi feito anos atrás e está alinhado a um conjunto desatualizado de casos de uso, é suficiente. Não é.

Recuperando o negócio em um nível minimamente viável

Os controles falham porque isso se trata de ir além do que arquitetar uma boa segurança. É sobre ganhar clareza em torno do que é preciso para se recuperar.
Os líderes das empresas tendem a olhar para o horizonte imediato, porque a maioria não consegue pensar além quando está no meio de um incidente. Nesse ponto, o CISO deve ser a voz da razão e falar pragmaticamente sobre voltar os processos de negócios aos estados minimamente viáveis: manter as luzes acesas, pagar pessoas e garantir que as operações sejam retomadas.

Quanto mais tempo leva para voltar aos processos de negócios a um nível minimamente viável, o mais provável é que o negócio tenha uma crise existencial. Os atacantes não trabalham no seu cronograma. Eles inovam mais rápido porque são motivados financeiramente. Esse é o desafio que os CISOs enfrentam, sempre tentando alcançá-los.

"Deve haver uma estrutura e uma compreensão da trajetória potencial de um evento cibernético. Ter um plano e uma abordagem clara para organizar recursos pode ser a diferença entre um pesadelo de 60 dias e de 30 dias."

Jason Haward-Grau
Sócio de Cyber Security Services da KPMG nos Estados Unidos

O papel da regulação na resiliência

Quando se trata de resiliência, os regulamentos podem ser vistos como um alicerce ou um teto. A maioria das organizações o vê como o último - algo que deve cumprir - portanto, eles fazem o mínimo necessário. Alternativamente, pode ser visto como um alicerce porque frequentemente há ações novas ou diferentes a serem tomadas.

A regulamentação desempenha um papel vital na resiliência organizacional, mas muitas vezes precisa ser coordenada ou alinhada. Este é um dos maiores desafios que os CISOs enfrentam à medida que os imperativos regulatórios se expandem para abranger toda a cadeia de suprimentos de uma empresa. Não é mais apenas uma questão de se preocupar somente com a sua organização. Os CISOs precisam considerar a extensão das implicações para os fornecedores e outros parceiros-chave e se eles estão em conformidade com os regulamentos relevantes, bem como as implicações em saber se os clientes e investidores estão em conformidade com os órgãos reguladores.

A resiliência é, em última análise, uma questão da organização como um todo, em que a segurança cibernética tem um papel vital, juntamente com outras capacidades e disciplinas de recuperação, como a continuidade dos negócios. Os CISOs podem desempenhar um papel fundamental para ajudar as organizações a planejar proativamente eventos cibernéticos disruptivos, que podem variar em natureza, escala e resposta, e responder a incidentes clássicos de tecnologia ou propriedade. Muitos CISOs também podem assumir responsabilidades de resiliência mais amplas à medida que as organizações se concentram cada vez mais em tais cenários e suas consequências. Mais uma evolução do papel do CISO.

Saiba mais

The day after

Recuperação, resistência e resiliência após um ciberataque industrial.

From continuity to resilience

A dependência crescente da eletricidade torna mais importante construir uma organização proativa e resiliente para ajudar a garantir a continuidade dos serviços.

Incident readiness: A playbook for your worst day

Estar preparado para um incidente cibernético pode minimizar a disrupção da infraestrutura crítica de energia e serviços públicos.

Estratégias de segurança cibernética para 2023

Quais ações os CISOs e as linhas de negócios podem tomar para ajudar a garantir que a segurança seja o fio condutor da organização? A seguir apresentamos uma pequena lista de etapas tangíveis que os CISOs devem considerar ao buscar acelerar os tempos de recuperação, reduzir o impacto de incidentes em funcionários, clientes e parceiros e procurar garantir que seus planos de segurança habilitem, e não exponham, seus negócio.

Recursos humanos

- Priorize uma cultura robusta de segurança cibernética que seja interessante, envolvente e divertida para inspirar os funcionários a fazerem a coisa certa e atuarem como *firewalls* humanos.
- Estabeleça uma equipe de segurança com a combinação de habilidades necessárias para gerenciar uma organização sem perímetro, incluindo nuvem e terceiros.
- Comunique-se de forma ampla e clara. Pergunte aos líderes de em outras funções organizacionais sobre seus problemas e como processos automatizados podem ajudar.
- Adote uma abordagem multidisciplinar e multicultural. Estabeleça um ecossistema de segurança composto por especialistas de negócios, profissionais de segurança, cientistas de dados, advogados de privacidade e profissionais da indústria.
- Incorpore-se à organização e aja como um colega, um bom ouvinte e um conselheiro.

Processos

- Desenvolva abordagens consistentes para o gerenciamento de riscos cibernéticos com uma compreensão dos cenários de ameaças e ataques para ajudar a reduzir a superfície de ataque e priorizar melhorias de controles.
- Concentre-se em processos de segurança adequados aos objetivos e que apresentem consistentes experiências de usuário.
- Estabeleça rigorosos controles de identidade e trabalhe para alcançar um estado maduro de governança e serviços de identidade.
- Segmente ambientes legados para limitar a superfície de ataque e ajudar a conter quaisquer violações.
- Tenha um plano de recuperação proativo com foco nos fluxos de trabalho mais críticos da organização, e que conte com uma estrutura de comunicação e testes de estresse frequentes.

Dados e tecnologias

- Adote a automação da função de segurança — confie nas ferramentas mais recentes, como processos robóticos, orquestração de segurança, automação e resposta (SOAR) e sistemas de detecção e resposta estendida (XDR).
- Trabalhe com provedores de nuvem para ajudar a garantir ampla visibilidade de como os produtos e serviços são configurados para evitar vulnerabilidades surpresas.
- Considere os problemas de segurança cibernética e privacidade antecipadamente, ao explorar tecnologias emergentes, incluindo os riscos em evolução associados à adoção de sistemas de IA.
- Atribua responsabilidades e estabeleça *accountability* sobre como os dados críticos são processados e gerenciados, e como eles suportam os processos de negócios críticos.
- Em questão da velocidade, escalabilidade e confiança, uma transição para a *Identity as a Service* (IaaS) na nuvem precisa acontecer mais cedo ou mais tarde.

Regulatório

- Esteja ciente da constante mudança das tendências e direcionadores regulatórios e o que eles podem significar para a futura estratégia tecnológica, de desenvolvimento de produtos e de operações da empresa.
- Considere os impactos regulatórios em relação a IA e automações, estabeleça um conceito claro do que o negócio pode e não pode fazer nesses ambientes e esteja atento às preocupações e expectativas de mudanças públicas.
- Aproveite a automação do monitoramento e reportes de conformidade, além de designar um colaborador para ficar por dentro das tendências regulatórias de privacidade e segurança.
- Alinhe a estratégia de conformidade de segurança e privacidade com a estratégia de negócios da empresa para ajudar a garantir que os *stakeholders* de toda a organização estejam na mesma página.
- Olhe além do regulamento, e esteja preparado para fazer perguntas fundamentais sobre a confiança digital e como isso é central para o pensamento estratégico.

Como os profissionais da KPMG podem ajudar

As firmas-membro da KPMG tem experiência em todos os níveis, desde a sala do conselho até o *data center*. Além de avaliar como está sua segurança cibernética e alinhá-la às suas prioridades de negócios, os profissionais da KPMG podem ajudá-lo a desenvolver soluções digitais avançadas, implementá-las, monitorar riscos contínuos e ajudá-lo a responder efetivamente a incidentes cibernéticos. Não importa onde você esteja em sua jornada de segurança cibernética, a KPMG pode ajudá-lo a alcançar o seu objetivo.

Como um dos principais fornecedores e implementadores de segurança cibernética, os profissionais da KPMG sabem como aplicar as principais práticas de segurança e adequar ao seu propósito. A abordagem progressiva à segurança cibernética também inclui como eles podem fornecer os serviços, portanto, não importa como sejam envolvidos, você pode esperar pessoas que entendam sua empresa e sua tecnologia.

Se você está entrando em um novo mercado, lançando produtos e serviços ou interagindo com os clientes de uma nova maneira, os profissionais da KPMG podem ajudá-lo a antecipar o amanhã, mover-se mais rápido e obter uma vantagem com tecnologia segura e confiável. Isso porque podem trazer uma combinação incomum de experiência tecnológica, conhecimento de negócios e criatividade para ajudá-lo a proteger e construir a confiança de todos os *stakeholders*.

KPMG. Fazendo a diferença.

Autores

Akhilesh Tuteja
Líder Global de Cyber Security
KPMG International
E: atuteja@kpmg.com

Além de atuar como líder da prática de Segurança Cibernética Global, Akhilesh lidera as práticas de consultoria de TI e riscos para a KPMG na Índia. Akhilesh aconselhou mais de 200 clientes sobre segurança cibernética, estratégia de TI e seleção de tecnologias, ajudando-os a perceber seus benefícios comerciais. Ele também tem experiência em psicologia comportamental e aborda os problemas de riscos de forma holística, sobretudo através da aplicação de análise de comportamento do usuário.

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

Líder da prática de segurança cibernética da KPMG nos EUA, Kyle tem mais de 20 anos de experiência em sistemas de informação, segurança cibernética, privacidade de dados, conformidade regulatória, gerenciamento de riscos e questões gerais de tecnologia. Kyle utiliza uma abordagem centrada nos negócios para resolver problemas de tecnologia, abordando causas-raiz em vez de sintomas técnicos. Ele atua com inúmeras organizações da Fortune 500, trabalhando com executivos seniores, incluindo conselhos de administração, comitês de auditoria, diretores de informação e financeiros, entre outros.

Dani Michaux
Sócia de Cyber Security Services
da KPMG na Irlanda
E: dani.michaux@kpmg.ie

Em mais de 22 anos de experiência em segurança cibernética, Dani trabalhou com agências governamentais em estratégias nacionais de segurança e com órgãos reguladores internacionais sobre riscos cibernéticos. Ela tem vasta experiência trabalhando com clientes para melhorar suas compreensões em questões de segurança cibernética. Ela construiu e gerenciou equipes de segurança cibernética como CISO em empresas de telecomunicações e energia na Ásia. Dani defende a inclusão, diversidade e a participação das mulheres na ciência da computação e na segurança cibernética. Ela anteriormente liderou as práticas de Segurança Cibernética e Risco de Tecnologias Emergentes para a KPMG na Malásia e região Ásia-Pacífico, além de ter liderado o grupo de trabalho global de IoT da KPMG.

Matt O'Keefe
Sócio de Cyber Security Services
da KPMG na Austrália
E: mokeefe@kpmg.com.au

Matt é responsável pela estratégia cibernética da KPMG dentro das 12 firmas-membros na região Ásia-Pacífico. Ele tem mais de 25 anos de experiência em tecnologia, finanças, auditoria e consultoria, com foco em serviços financeiros. Matt é especialista em consultoria tecnológica, particularmente em fundos de aposentadoria, gestão de patrimônio, bancos e seguros, fornecendo uma gama de serviços em governança e risco de tecnologia, segurança cibernética, gerenciamento de projetos, estratégia e desempenho de TI. Ele usa a tecnologia para alavancar objetivos organizacionais, permitindo estratégias digitais e modelos operacionais para clientes e protegendo seu dados, ativos e sistemas.

Prasad Jayaraman
Diretor de Cyber Security Services
da KPMG nos EUA
E: prasadjayaraman@kpmg.com

Com mais de 17 anos de experiência na prática de gerenciamento de identidades, Prasad tem um histórico de desempenho em organizações de serviços profissionais relacionados à tecnologia. Ele atua com vendas, recursos humanos, jurídicos, finanças e operações.

Agradecimentos

O desenvolvimento deste relatório não seria possível sem as contribuições de planejamento, análise, redação e produção de profissionais de todo o mundo.

Considerações para o time global

Jessica Booth
David Ferbrache
John Hodson
Billy Lawrence
Leonidas Lykos
Michael Thayer

Nossos profissionais globais

John Anyanwu
Sócio de Cyber Security Services
da KPMG na Nigéria
john.anyanwu@ng.kpmg.com

Jonathan Dambrot
Diretor da KPMG nos EUA
jdambrot@kpmg.com

David Ferbrache
Diretor de inovações em cyber
da KPMG no Reino Unido
david.ferbrache@kpmg.com

Jayne Goble
Diretora de Cyber Security Services
da KPMG no Reino Unido
jayne.goble@kpmg.co.uk

Jason Haward-Grau
Diretor de Cyber Security Services
da KPMG nos EUA
jhawardgrau@kpmg.com

Lisa Henegan
Sócia-líder global de Digital
da KPMG no Canadá
lisa.heneghan@kpmg.co.uk

Charles Jacco
Sócio da KPMG nos EUA
cjacco@kpmg.com

Prasad Jayaraman
Diretor de Cyber Security Services
da KPMG nos EUA
prasadjayaraman@kpmg.com

Sylvia Klasovec Kingsmill
Sócia de Privacy
da KPMG no Canadá
skingsmill@kpmg.ca

Markus Limbach
Sócio de Cyber Security Services
da KPMG na Alemanha
mlimbach@kpmg.com

Deepak Mathur
Diretor de Cyber Security Services
da KPMG nos EUA
deepakmathur@kpmg.com

Dani Michaux
Sócia de Cyber Security Services
da KPMG na Irlanda
dani.michaux@kpmg.ie

Matt O'Keefe
Sócio de Cyber Security Services
da KPMG na Austrália
mokeefe@kpmg.com.au

Natasha Passley
Sócia de Cyber Security Services
da KPMG na Austrália
npassley@kpmg.au

Walter Risi
Sócio de Cyber Security Services
da KPMG na Argentina
wrisi@kpmg.ar

Motoki Sawada
Sócio de Technology Risk Services
da KPMG no Japão
motoki.sawada@jp.kpmg.com

Henry Shek
Sócio de Cyber Security Services
da KPMG na China
henry.shek@kpmg.com

Julia Spain
Sócia de Cyber Security Services
da KPMG no Reino Unido
julia.spain@kpmg.co.uk

Eddie Toh
Sócio de Cyber Security Services
da KPMG em Singapura
eddietoh@kpmg.com.sg

Akhilesh Tuteja
Líder Global de Cyber Security
KPMG International
atuteja@kpmg.com

Annemarie Zielstra
Sócia de Cyber Security Services
da KPMG na Holanda
zielstra.annemarie@kpmg.nl

Contate-nos

Cyber Security & Privacy Services Brasil

Leandro Augusto
Sócio-líder de Cyber Security & Privacy da KPMG no Brasil e na América do Sul
lantonio@kpmg.com.br

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

Klaus Kiessling
Sócio de Cyber Security & Privacy da KPMG no Brasil
kkiessling@kpmg.com.br

Daniel Argenta
Sócio-diretor de Cyber Security & Privacy da KPMG no Brasil
danielargenta@kpmg.com.br

Marcos Fugita
Sócio-líder de Managed Risk & Security Services da KPMG no Brasil
mfugita@kpmg.com.br

Edson Honda
Sócio de Cyber Security & Privacy da KPMG no Brasil
edsonhonda@kpmg.com.br

Marcelo Marchi
Sócio-diretor de Cyber Security & Privacy da KPMG no Brasil
msantos2@kpmg.com.br

Thiago Leme
Sócio-diretor de Managed Risk & Security Services da KPMG no Brasil
tleme@kpmg.com.br

Os serviços descritos neste material, no todo ou em parte, podem não ser permitidos a ser prestados a clientes de auditoria da KPMG e suas afiliadas ou entidades relacionadas.

kpmg.com.br

/kpmgbrasil

Projeto gráfico e diagramação: Gaudí Creative Thinking.