Desafios crescentes na sociedade hiperconectada

Quais são os fatores-chave para a segurança cibernética e quais são os principais desafios das empresas em 2022?

Por **Leandro Augusto,** sócio-líder de Cyber Security & Privacy da KPMG no Brasil e na América do Sul.

É fato que o mundo está cada vez mais digital, o que por si só já aumenta os riscos relativos à segurança cibernética. "Sequestro" de dados, invasão de contas e outros crimes cibernéticos estão mais frequentes e são vistos com preocupação pelos líderes empresariais. Segundo 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, os criminosos estão mais sofisticados. Por isso, os diretores de segurança da informação (Chief Information Security Officers, ou CISOs) e suas respectivas equipes lidam com o desafio de mudar seus próprios paradigmas de atuação, passando de executores a influenciadores, ou, mais exatamente, a fomentadores de uma mentalidade de capacitação, já que a segurança cibernética não se limita à implementação de ações de proteção técnicas.

Cada vez mais, esses especialistas são essenciais nos processos de tomada de decisão, por serem os mais capacitados a proteger os ecossistemas dos seus parceiros e as cadeias de suprimentos. Simultaneamente, as lideranças corporativas precisam concentrar seus esforços nas iniciativas prioritárias para a proteção virtual da empresa e na elaboração de um plano de segurança baseado na responsabilidade compartilhada no ecossistema.

A KPMG identificou oito principais fatores-chave para a segurança cibernética e os colocou em pauta no estudo "**Fatores-chave sobre Segurança Cibernética em 2022"**.

Neste artigo, falaremos a respeito desses fatores-chave e daremos ênfase às medidas que o estudo aponta como "fundamentais" para este ano.

O primeiro desses fatores-chave consiste em **ampliar a conversa estratégica sobre segurança**, para alinhar os objetivos do negócio com as medidas de segurança. Partindo dessa premissa, como fatores-chave para a segurança cibernética em 2022, o levantamento aponta a inclusão da segurança cibernética no DNA da empresa; a conscientização de que a segurança cibernética é uma responsabilidade coletiva, de todos da empresa – sendo que os CISOs devem atuar como agentes dessa conscientização; a mudança de mentalidade em relação à confidencialidade e disponibilidade de dados, com uma maior reflexão acerca de como assegurar a integridade e a resiliência; o engajamento dos públicos de interesse para que estes se comprometam com uma estratégia de segurança voltada à proteção dos dados da organização e dos clientes, com foco em gerenciamento de riscos e maior sensibilidade às prioridades de negócios de curto e longo prazos; maior foco, por parte dos executivos, em relação aos riscos práticos para a empresa; a redução do foco em indicadores-chave de desempenho operacional (KPIs) e nos indicadores-chave de risco (KRIs), para que seja possível concentrar-se em temas e tendências relativos às ameaças; e a consolidação dos relacionamentos com as principais áreas de negócios, de modo a aumentar a conscientização sobre a rapidez com que elas podem atingir objetivos incorporando

Leandro Augusto

a segurança – sendo que uma violação poderia comprometer os resultados e despertar a aversão de consumidores e clientes.

Nova postura dos especialistas em segurança cibernétic

O segundo fator-chave refere-se aos **talentos e conjuntos de habilidades críticas**. Seu foco consiste em transformar a postura dos CISOs e suas equipes, para que migrem do papel de executores da segurança cibernética para o de influenciadores.

O estudo aponta que, em 2022, serão necessárias medidas como: mudar a narrativa, de modo que esses especialistas passem a falar mais sobre negócios e menos sobre tecnologia; não se limitar à definição tradicional de segurança cibernética; continuar estabelecendo relacionamentos com outras áreas da organização, construindo assim uma rede de parceiros de negócios internos; ser um divulgador/motivador, para que mais pessoas se envolvam na segurança cibernética; adotar a postura de que a segurança cibernética está no DNA da empresa.

O terceiro fator-chave consiste em **adaptar a segurança para a nuvem**. Ressaltando que a segurança cibernética e a segurança em nuvem estão se

tornando sinônimos, é cada vez mais importante automatizar a segurança em nuvem, especialmente em relação à implementação, ao monitoramento e à recuperação de dados, eliminando processos manuais ou a falta de visibilidade dos ativos da organização.

O estudo aponta que são medidas fundamentais: montar uma equipe de segurança em nuvem centralizada, proveniente das áreas de desenvolvimento, em vez de liderar com as habilidades tradicionais de segurança; 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*; procurar ferramentas de gerenciamento de segurança que tenham verificações de políticas preconfiguradas e mapeadas para diferentes regimes regulatórios; construir um processo de resposta a incidentes sintonizado com uma estratégia em nuvem mais ampla e integrando a visibilidade da segurança para o negócio.

Como quarto fator-chave, a análise sugere c**olocar a identidade no centro do modelo Zero Trust (confiança zero).** O raciocínio por trás desse fator é o seguinte: hoje, as empresas têm muitas pessoas trabalhando remotamente, além de lidarem com grandes volumes de clientes, fornecedores e outros stakeholders, com os quais se relacionam remotamente. Assim, proteger dados confidenciais é essencial e requer medidas à altura dos desafios e da complexidade inerentes a esse cenário. Afinal, os criminosos cibernéticos podem estar a apenas um clique de distância. Não pode haver qualquer brecha.

Nesse sentido, entre as ações a serem consideradas para 2022, o estudo sugere adotar e/ou testar uma estratégia de autenticação; certificar-se de que o seu programa de identidades dispõe de uma base sólida de dados e análises; inserir a mentalidade de *Zero Trust* na sua estratégia de segurança cibernética; 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; automatizar a funcionalidade de segurança para possibilitar que profissionais altamente qualificados se concentrem nas atividades mais estratégicas; e aceitar que a adoção de uma abordagem de *Zero Trust* é uma jornada de longo prazo para implementação.

> “Manter os dados pessoais seguros e levar a privacidade a sério são medidas que requerem uma mudança cultural”

Mais agilidade nas respostas e menos erros humanos

Explorar a automação da segurança para obter vantagem competitiva é o quinto fator-chave destacado pelo estudo. Como ações para 2022, são sugeridas a adoção de uma abordagem proativa para a automação da segurança, concentrando-se nas ameaças e não nos incidentes; a automatização das tarefas cotidianas; o melhor aproveitamento da tecnologia existente e da *expertise* dos especialistas em automação; e a racionalização de investimentos, evitando a engenharia complexa de soluções ou a aquisição de ferramentas de automação que não atendam ao problema ou gerem valor para a empresa.

O sexto fator-chave consiste em **proteger a fronteira da privacidade.** E como fazer isso? Migrando para uma abordagem multidisciplinar de gerenciamento de risco de privacidade que incorpore os conceitos de *privacy by design* e *security by design*. O estudo destaca que manter os dados pessoais seguros e levar a privacidade a sério são medidas que requerem uma mudança cultural. As empresas devem adotar uma mentalidade de *privacy-first* ou *privacy-by-design*.

Entre as medidas que o estudo aponta para atender ao sexto fator-chave, constam a necessidade de conscientizar a alta administração e a gerência de negócios acerca da importância de garantir a correta base legal na coleta de dados dos indivíduos; o alinhamento do programa de privacidade de dados com as prioridades e a visão de liderança dos altos executivos e da linha de negócios, de modo que todos estejam em sintonia no que tange às perspectivas de coleta, bases legais e uso; a adoção de um padrão de *privacy-by-design* para complementar regras, regulamentos e expectativas regulatórias em torno da privacidade; o delineamento de políticas baseadas em práticas de negócio que possam ser testadas, para convencer consumidores e órgãos regulatórios do seu compromisso em respeitar os direitos do cliente e proteger seus dados.

Também estão em destaque a importância de explorar oportunidades para implementar tecnologias de gerenciamento de privacidade de dados para automatizar processos, cumprir regulamentos, agilizar respostas e reduzir erros humanos.

Incentivar uma ampla cadeia de suprimentos a ter segurança cibernética são os principais objetivos

do fator-chave de número sete, que consiste em **proteger além das fronteiras.** Ora, o mundo continua caminhando a passos largos para a digitalização. Tornar-se uma organização que prioriza o digital significa adotar uma abordagem centrada em dados, com o constante compartilhamento de informações em ecossistemas complexos e interconectados.

As ações fundamentais para viabilizar o sétimo fator-chave em 2022 consistem, dentre outras, em acompanhar os requisitos regulatórios na medida em que eles evoluem; concentrar-se na segurança da cadeia de suprimentos; explorar as oportunidades para automatizar; e não negligenciar a cadeia de suprimentos de tecnologia operacional: conforme os sistemas de tecnologia da informação (TI) e de tecnologia operacional (OT) convergem, os invasores tentarão explorar os sistemas de OT com o objetivo de comprometer os dados da empresa. Assim, convém investir em uma perspectiva de capacitação, aplicando medidas de segurança para proteger não apenas o seu próprio ambiente digital, mas todo o ecossistema em que ele estiver inserido.

O oitavo e último fator-chave apresentado pelo estudo refere-se a **reformular a conversa sobre resiliência cibernética,** de modo a ampliar a capacidade de manter as operações, recuperar-se rapidamente e administrar as consequências quando um ataque cibernético ocorrer. Para que esse fator-chave seja colocado em prática, a análise destaca a importância de avaliar 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. Importante salientar aqui a necessidade de junção das disciplinas de segurança cibernética e continuidade dos negócios com o olhar dos eventos cibernéticos, suas derivações e dependências para o atendimento aos clientes, fatores estes muitas vezes desconectados dos planos e testes das empresas.

O estudo ressalta ainda que é necessário: refletir a respeito de como um evento cibernético significativo afetaria a sua dependência dos fornecedores; levar para o Conselho os temas de segurança cibernética e resiliência cibernética; avaliar se os atuais planos de resiliência bastam para fazer frente a um ataque cibernético; abrir-se para reconhecer que suas premissas podem estar erradas e que talvez um plano alternativo precise ser operacionalizado rapidamente; concentrar-se nos fundamentos e, ao mesmo tempo, investir em recursos de detecção, agilidade de resposta e capacidade de recuperação; e não se fechar para a eventual colaboração de especialistas externos.

E agora, o que nos espera?

Não restam dúvidas de que a nossa sociedade hiperconectada estará sujeita a riscos cibernéticos crescentes. Se, de um lado, a digitalização se traduz em possibilidades de negócios e interação, por outro ela acarreta novos desafios. A Internet das Coisas Industrial (IIoT), que conectará milhões de dispositivos em todo o mundo, ampliará os pontos vulneráveis a ataques. É primordial que os fabricantes contemplem o quesito segurança cibernética na arquitetura de produtos que possibilitam a IIoT. O mesmo se aplica ao uso de Inteligência Artificial (IA), em especial no que se refere a *Machine Learning* (ML).

As redes 5G também deverão priorizar a segurança dos dispositivos. Incomparavelmente mais ágil e sofisticada do que o 4G, o 5G possibilitará grande evolução em conectividade – por isso, é importante que haja arquitetura, monitoramento e controles de segurança adequados. Como ainda há muitos pontos nebulosos no que se refere à adoção do 5G, parece razoável sugerir que as empresas adotem uma mentalidade de *Zero Trust*, reduzindo os espaços que possam levar à quebra da segurança dos dados.■