Colaborações, respostas ágeis às ameaças e uso eficaz de dados

A publicação *Considerações de Segurança Cibernética para 2023*, elaborada pela KPMG, enfatiza a importância de colocar a segurança cibernética no centro dos negócios e de construir a confiança digital

Por **Edson Honda**, sócio de Cyber Security & Privacy da KPMG no Brasil, e **Daniel Argenta**, sócio-diretor de Cyber Security & Privacy da KPMG no Brasil.

KPMG Business Insights
100ª edição | Junho de 2023

Edson Honda

Daniel Argenta

A tecnologia desempenha um papel cada vez mais central em todos os aspectos de nossas vidas. Geramos e compartilhamos uma quantidade cada vez maior de dados: das transações financeiras às postagens em redes sociais, dos registros médicos às informações de localização, tudo gera dados, que são utilizados pelas organizações para identificar auxiliar na tomada de decisões, aprimorar a eficiência operacional, identificar tendências e oportunidades de negócios e proporcionar melhores experiências ao público.

Empresas, governos e entidades não governamentais, dos mais diversos setores. reconhecem que a transformação digital é essencial para se manterem relevantes e têm construído seus planejamentos considerando o uso estratégico de dados e a adoção de tecnologias disruptivas - como a inteligência artificial (IA), as máquinas de aprendizagem (ML), o *blockchain*, a Internet das Coisas (IoT) e a computação em nuvem - para impulsionar a inovação e a criar novas oportunidades.

Diante desses fatos, podemos afirmar que o futuro está intrinsecamente ligado aos dados e à infraestrutura digital. Hoje, testemunhamos uma ampla gama de colaborações público-privadas, ecossistemas hiper conectados e grandes infraestruturas de informação. Mas, ao mesmo tempo que esses avanços propiciam novas oportunidades de negócios, eles nos expõem cada vez mais a novos (e velhos) riscos: com o grande volume de dados, das interconexão e das interdependências aumentam, cresce também o interesse de agentes nocivos em busca por ganhos financeiros. Adicionalmente as tecnologias inovadoras trazem em seu esteio uma grande quantidade de desafios de segurança, privacidade e ética, suscitando questões fundamentais sobre a confiança nos sistemas digitais. Esse é o ambiente no qual o comércio global precisa prosperar. É crucial abordar essas preocupações à medida que avançamos com inovação. Assumir uma postura reativa isto é, somente respondendo aos ataques quando estes ocorrerem, talvez seja tarde demais.

Segurança cibernética no centro dos negócios

O estudo ***Considerações de Segurança Cibernética para 2023*** da KPMG traz um panorama sobre o papel da segurança cibernética no estabelecimento da confiança digital nas empresas, explorando oito áreas que os *Chief Information Security Officers* (CISOs) podem atuar para demonstrar aos executivos e à alta administração que a confiança digital pode e deve ser uma vantagem competitiva, apresentando recomendações voltadas a gestão de pessoas, processos, dados/tecnologia e regulatório. São elas:

1. **A confiança digital é uma responsabilidade compartilhada.**
2. **Uma segurança discreta leva a comportamentos seguros.**
3. **É preciso proteger um futuro "sem perímetro e centrado em dados".**
4. **Novas colaborações e novos modelos são necessários.**
5. **Temos que confiar na automatização.**
6. **O "mundo inteligente" requer proteção.**
7. **É necessário lidar com adversários cada vez mais ágeis.**
8. **É essencial ter resiliência; estratégias de segurança cibernéticas precisam ser adotadas desde já.**

Atentar para esses tópicos é essencial para agilizar a recuperação (em caso de incidente), reduzir o impacto de eventuais ocorrências sobre os funcionários, clientes, parceiros e demais *stakeholders*, e garantir que seus planos de segurança tenham eficácia. Um dos pontos destacados pelo estudo é a importância de reconhecer a confiança digital como uma responsabilidade compartilhada. **A confiança digital abrange diversas disciplinas, sendo a segurança cibernética uma parte crucial desse amplo espectro de questões intimamente relacionadas, como confiabilidade, segurança, privacidade e transparência.** Essas áreas afetam amplamente a forma como as empresas conduzem seus negócios.

Felizmente, esse tema está ganhando destaque nas discussões dos Conselhos de Administração, à medida que os debates sobre privacidade, segurança e ética adquirem maior relevância, impulsionados tanto por regulamentações quanto pela opinião pública.

O sucesso futuro de qualquer negócio habilitado digitalmente será alicerçado pela confiança digital, sendo a segurança cibernética e a privacidade de dados os fundamentos vitais para essa confiança. Assim, os CISOs devem estar preparados para auxiliar o Conselho e os executivos de alto escalão na geração e manutenção da confiança de seus *stakeholders*, criando assim uma vantagem competitiva. Alcançar esse potencial requer um compromisso coletivo de todos.

Segurança discreta e foco nos dados

Uma abordagem de segurança discreta leva a comportamentos seguros. Isso significa que é preciso incorporar a segurança de dados nos negócios, de forma que as pessoas possam trabalhar com confiança. Auxiliar as pessoas a fazerem escolhas produtivas e desempenharem satisfatoriamente seu papel na proteção da organização é um objetivo central para os CISOs. Além disso, eles têm a responsabilidade de promover a cultura de segurança em todos os níveis da empresa.

As empresas devem deixar de pensar em segurança corporativa em termos binários. No ambiente dinâmico de hoje 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.

Também é fato que os modelos operacionais de negócios sofreram significativas mudanças na última década, tornando-se mais flexíveis, centrados em dados e com ecossistemas conectados de parceiros internos e externos, bem como provedores de serviços. Nesse mundo de computação distribuída, os CISOs e as equipes de segurança devem adotar abordagens significativamente diferentes para ajudar a reduzir a dimensão de possíveis falhas ou violações, como *Zero Trust*, Serviço de Acesso Seguro de Borda (*Secure Access Service Edge* - SASE) e arquitetura *mesh* de segurança cibernética (CSMA). Saiba mais sobre elas no estudo completo.

Novas colaborações exigem novos modelos

Os dias em que as equipes de segurança se concentravam apenas nos sistemas de tecnologia da informação (TI) da própria organização ficaram para trás. A evolução das colaborações demanda novos modelos, por isso os CISOs precisam reconhecer a necessidade de terceirizar esforços de segurança cibernética e determinar quais habilidades devem ser mantidas internamente, tanto no presente quanto no futuro. A segurança tornou-se uma prioridade de negócio, sendo entregue por meio de um modelo de

responsabilidade compartilhada entre a organização, parceiros de negócios e os provedores de serviços.

Enquanto as empresas buscam inovar e aproveitar as tecnologias emergentes, questões como segurança, privacidade, proteção de dados e ética podem não receber a atenção adequada. Deve-se tomar cuidado com essa tendência, para que oportunidades interessantes não sejam desperdiçadas.

Também é ressaltada a preocupação com a agilidade crescente dos ataques: os intervalos entre o comprometimento inicial da segurança cibernética e a ativação de *ransomware* em toda a empresa estão diminuindo, deixando pouca margem de tempo para as ações de mitigação.

Isso ocorre porque os cibercriminosos estão utilizando ferramentas cada vez mais sofisticadas para invadir sistemas e acelerar suas explorações. Em resposta a essas ameaças, as operações de segurança precisam ser otimizadas e estruturadas de modo a acelerar a recuperação dos serviços prioritários em casos de incidente, reduzindo assim o impacto nos clientes, consumidores e parceiros.

Finalmente, a análise da KPMG salienta a importância de as organizações se manterem resilientes. Não se pode negar que todo sistema, por mais aperfeiçoado que seja a sua segurança, pode apresentar vulnerabilidades. Os reguladores sabem disso e estão pressionando as empresas, especialmente sobre aquelas que atuam em setores estrategicamente importantes.

Conforme os legisladores e reguladores aumentam suas demandas por transparência e supervisão, muitas organizações estão preocupadas com o cenário regulatório global cada vez mais complexo. Complementarmente, a constatação de que os cibercriminosos sempre darão um jeito de encontrar brechas na segurança cibernética nos traz um senso de inevitabilidade, como se todos soubéssemos que, em algum momento, ocorrerá um incidente.

Mesmo que seja impossível se blindar completamente, é viável, sim, reduzir possíveis danos; e **a melhor maneira de enfrentar as ameaças cibernéticas é proceder à implementação de medidas de segurança digital modernas, holísticas e arrojadas.**