IDC #BR23003 | Maio 2023 | Patrocinado por:
kyndryl

IDC VENDOR SPOTLIGHT

A busca pela resiliência cibernética em meio às complexidades digitais

Luiz Monteiro
Luiz Monteiro, Research and Consulting Senior Analyst – IT Services.
IDC Brazil

O cybercrime evoluiu e introduziu complexidades que potencializaram os reflexos dos ataques, contando com um elemento essencial para a sobrevivência e crescimento dessa indústria: a monetização. Os fabricantes de soluções, prestadores de serviços e as organizações, no entanto, não ficaram parados.

Introdução

Na primeira década do atual milênio, passamos a conviver com elementos que até então não eram tidos como uma ameaça realmente ofensiva ou preocupante. As ameaças digitais não se mostravam tão sofisticadas, eram citadas apenas em publicações especializadas e ocupavam pouco espaço nos noticiários e na agenda de prioridades das organizações. Os chamados vírus e as ameaças digitais, que já existiam desde muitos anos antes, ganharam bastante atenção logo no início da década de 2000: o emblemático I Love You inaugurou uma era em que as ameaças digitais e as consequências de ataques cibernéticos extrapolaram o mundo da tecnologia, garantindo lugar numa lista de agentes causadores de incidentes que desde então só aumentou. A motivação dos atacantes naqueles tempos iniciais, era, principalmente, a de causar danos e transtornos para as operações e para a rotina dos usuários e das empresas.

Com o passar dos anos, o que podemos chamar de indústria do cybercrime evoluiu e introduziu complexidades aos malwares, que inovaram nas formas de causar danos e potencializaram os reflexos causados pelos ataques, somando a isso um elemento que se tornou essencial para a sobrevivência e crescimento dessa indústria: a monetização. Esse mercado, que se organiza, troca mensagens, experiências e informações prioritariamente pela deepweb, passou a retroalimentar suas capacidades e, de forma ampla, a própria indústria do cybercrime. Com a introdução do Bitcoin e de outras criptomoedas, a rastreabilidade de pagamentos e da remuneração dos profissionais dessa indústria através, por exemplo, da exigência de pagamentos de resgates, foi dificultada. Com essas inovações, passou a ser desnecessário o uso do sistema bancário tradicional ou pagamentos em dinheiro, que poderiam ser rastreados.

Em destaque

O aumento da produtividade passou a ser apontado como prioritário pelos decisores de TI em 2022, superando a preocupação com custos, enquanto a Segurança da Informação permanece líder dentre as principais iniciativas de TI desde 2017.

Dados importantes

30,1%

é a expectativa receita proveniente de produtos e serviços digitais previstos pelo mercado brasileiro em 2026.

53%

de um total superior a 800 empresas consultadas em âmbito global sofreu consequências de ataques de Ransomware em 2021.

Enquanto isso, no contexto dos mercados consumidor e corporativo, observou-se o uso cada vez mais intensivo da internet em múltiplas plataformas, através de diversos devices e para inúmeros fins. Diante desse cenário, surgiu a oportunidade para, gradativamente, profissionalizar os agentes causadores de dificuldades para qualquer usuário que se valesse da tecnologia e de devices com acesso à internet ou a redes corporativas locais, já a partir dos meados da década de 2000.

Seguindo a linha do tempo, no início da década seguinte, o Ransomware ainda em suas formas iniciais, emergiu como uma opção com intenso potencial ofensivo. Especificamente em 2017, outra ameaça digital ganhou as manchetes e grande notoriedade devido à quantidade de empresas e usuários infectados: o WannaCry, que explorou brechas de segurança de sistemas Microsoft Windows desatualizados, realizou o sequestro de dados e informações com objetivo de obter valores através do pagamento de resgates. O alcance e os estragos chegaram à casa de centenas de milhares de devices infectados.

Nessa ocasião, o cenário tecnológico já contava com tráfego de dados crescendo à altas taxas, dependência tecnológica para as operações das empresas, além de um mercado corporativo que alimentava de forma acelerada bancos de dados alocados em estruturas locais, em data centers ou plataformas em cloud, em busca de maior conhecimento e comunicação com seus clientes, parceiros de negócios e fornecedores.

Assim, diante desse cenário, os temas ligados à segurança da informação chegaram de vez aos noticiários e ganharam relevância na agenda dos decisores, que, desde então, mantém suas preocupações e atenções ao tema constantemente em alta.

Corporações, fabricantes de soluções e prestadores de serviços, no entanto, não ficaram parados e buscaram formas de minimizar a possibilidade de ataques. Contando com processos específicos e uso intensivo da tecnologia, as soluções de segurança cibernética permitem que os decisores e as operações das empresas possam se manter com preocupações em níveis mais saudáveis, mesmo diante de um inimigo invisível e com alto potencial para causar danos.

Contexto de mercado

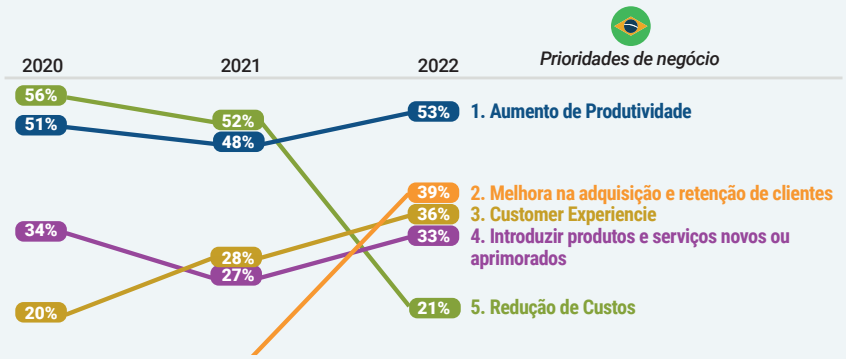
A criação, alimentação, manutenção e uso de bases de dados pelas corporações vem crescendo ao longo dos anos e permanece nesse movimento com taxas bastante significativas. O volume de dados que é criado anualmente e que circula pelas redes é enorme.

Segundo o IDC's Global DataSphere, 2022, no ano de 2017, mesmo ano em que o WannaCry causou inúmeros danos às empresas e usuários, foram gerados em torno de 30ZB globalmente. Para se ter uma ideia, um zettabyte (ZB) é uma unidade de armazenamento de informações digitais igual a 1.024 exabytes, ou 1 trilhão de gigabytes. Em 2022, a IDC estima que tenham sido gerados mais de 101ZB de dados, um crescimento expressivo e contínuo cujo CAGR (taxa de crescimento anual composta) ultrapassa os 27%.

Para que esses dados, que estão a todo momento sendo criados, replicados e armazenados, possam ser utilizados pelas organizações, a comunicação entre todos os interessados precisa ocorrer de forma fluida e desimpedida. Para isso é essencial que o caminho entre o requisitante da operação, seja ele um usuário em um smartphone ou uma aplicação de gerenciamento logístico em busca da atualização da localização de determinada carga, ocorra sem alterações sem interrupções e preferencialmente sem latência. Trata-se de fatores críticos e essenciais para que a experiência do usuário, ou os processos, ocorram com sucesso e sem intercorrências.

Esse contexto, de alta criticidade para manutenção das operações, direciona a atenção dos decisores das organizações. As prioridades de negócios das empresas brasileiras sofreram mudanças nos últimos anos, mas estão se estabelecendo com grande foco no aumento da produtividade e melhorias voltadas ao user experiente, conforme a Figura 1, que mostra as principais prioridades de negócios apontadas pelo mercado no estudo anual IDC Latin América Investment Trends 2022.

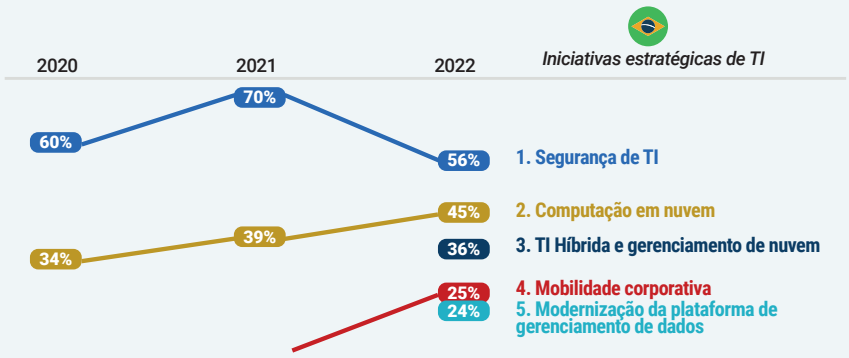
FIGURA 1: Série Histórica - Prioridades de Negócios



Fonte: IDC Latin America IT Investment Trends 2022.

Considerando o atual cenário, é quase uma questão de sobrevivência que os sistemas estejam disponíveis ininterruptamente para que, pensando de forma ampla, os indivíduos, a sociedade, as instituições públicas ou privadas possam realizar suas operações, que ocorrem a todo momento no mundo digital. Mas como manter a qualidade e a disponibilidade num cenário que, segundo o IDC´s Future Enterprise Resiliency & Spending Survey, pesquisa realizada em dezembro de 2021 apontou que 53% de 858 empresas consultadas em âmbito global sofreram consequências de ataques de Ransomware? Ainda no IDC Latin América Investment Trends 2022, quando perguntados a respeito das iniciativas estratégicas de TI, a segurança da informação foi apontada como prioridade pelos decisores. Nessa amostra, também é possível observar uma tendência de consolidação das iniciativas das organizações, em direção a uma linha que adiciona a segurança de TI ao entorno de infraestrutura e utilização de ambientes híbridos (cloud pública, privada e data centers locais ou de terceiros) das corporações. Também vale destacar as iniciativas que apontam para os temas ligados à mobilidade corporativa e o foco na modernização, conforme pode ser observado na Figura 2.

FIGURA 2: Série Histórica - Iniciativas Estratégicas de TI



Fonte: IDC Latin America IT Investment Trends 2022.

Confirmando o que foi apontado pelo mercado, a versão mais atual do estudo IDC Worldwide Security Spending Guide - Forecast 2023, mostra a tendência dos investimentos das organizações direcionadas ao tema de segurança. Nesse estudo, é possível confirmar crescimentos relevantes no mercado corporativo de segurança da informação no Brasil. As perspectivas de crescimento são de 12,4% em 2023, chegando a números próximos a US$2,8 Bi no ano. A previsão é de crescimento sustentado e acelerado nos próximos anos, resultando CAGR de 12,8% no intervalo entre 2022 e 2026.

Como base de comparação, nas Américas a perspectiva nacional se mostra mais interessante que a de outros países com participação relevante na região, como por exemplo o líder global, Estados Unidos ou o México, segunda maior economia da América Latina depois do Brasil. No mesmo período, citado (de 2022 a 2026) o GAGR dessas geografias, segundo o IDC Worldwide Security Spending Guide - Forecast 2023 apontam 10,7% e 12,1% respectivamente. A perspectiva de crescimento no Brasil mostra números bastante positivos para Software, Hardware e Serviços de segurança, mas a principal alavanca de crescimento será Software, com CAGR na casa dos 20,0% entre 2022 e 2026.

O contexto atual ainda aponta para a necessidade de apoio por parceiros especializados, que tenham condições de orientar as empresas em um mundo que busca cada vez mais receitas através de produtos e serviços digitais. Considerando dados extraídos do IDC Latin América Investment Trends 2022, vemos que, em média, o mercado aponta que 20,1% das receitas são provenientes de produtos e serviços digitais, mas a perspectiva é de um salto bastante considerável, com esse número chegando a 30,1% em 2026.

Resiliência **Cibernética**

Os avanços das corporações em direção à modernização, ao intensivo uso de dados e da tecnologia são evidentes. Para conseguir atender a um mercado com alto grau de exigência e expectativas, as empresas buscaram se modernizar e para tanto se valeram da multiplicidade de opções disponíveis no mercado.

Para grande parte das organizações, a cloud se mostrou como um meio rápido e relativamente simples para evoluir, avançar e se modernizar. E o avanço em direção à cloud fica evidente quando analisamos as nuvens (seja na modalidade privada ou pública), que mostram crescimentos significativos historicamente e previstos para os próximos anos. O destaque, no entanto, fica com a nuvem pública, que acumula crescimentos anuais que superaram 30% ou até 40% em alguns períodos analisados no IDC Brazil Semiannual Public Cloud Services Tracker desde 2014. Na publicação mais recente do estudo semestral que acompanha a evolução e o forecast do mercado de nuvem pública no Brasil (IDC Brazil Semiannual Public Cloud Services Tracker 2022H2), a previsão não é diferente do histórico: crescimento estimado acima de 30% em 2023.

Com a modernização na pauta das empresas, dois fatores, dentre muitos outros, se destacaram e favoreceram o aumento da superfície disponível para ataques maliciosos: o uso mais acentuado de ambientes híbridos e multicloud e a implementação ou ampliação da quantidade de empresas que se valem do trabalho remoto.

Com isso, a solução da equação que resulta no aumento da capacidade das organizações de se manterem operando colocou a resiliência corporativa e, em especial, a resiliência cibernética, como tema central a ser discutido e endereçado pelos decisores de TI.

Resiliência cibernética pode ser definida como a capacidade de uma organização em se adaptar e se recuperar de eventos adversos relacionados à tecnologia da informação. Essa capacidade engloba

medidas preventivas, detecção e resposta a ataques cibernéticos, alternativas a falhas de hardware ou software e outras ameaças que possam afetar a segurança ou o funcionamento dos sistemas, e, consequentemente impactar as operações das empresas. Planos de continuidade de negócios e recuperação de desastres são alguns dos elementos que visam habilitar as organizações a uma retomada rápida das operações no caso de haver eventos que causem interrupções. Trata-se de um conceito fundamental no que toca a segurança da informação e continuidade dos negócios, num mundo cada vez mais dependente da tecnologia.

Para alcançar a resiliência cibernética, é necessário que os ambientes estejam aptos a serem gerenciados da forma mais simples e consolidada possível, através do ferramental adequado para isso. Mesmo considerando que os ambientes atualmente se encontram bastante pulverizados geograficamente (além de baseados em múltiplas tecnologias e fabricantes) se torna essencial que as diversas tecnologias e soluções utilizadas para a segurança da corporação troquem informações que permitam respostas rápidas e assertivas no caso de eventos de cibersegurança.

Além de fatores técnicos, é necessário direcionamento para que a corporação desenvolva uma cultura de divulgação de informação e treinamento recorrente para todas as suas equipes, independentemente do nível de utilização das ferramentas tecnológicas. O objetivo da resiliência cibernética também passa por minimizar as probabilidades de eventos iniciados inadvertidamente por colaboradores. As ações de treinamento também visam conscientizar o uso adequado de devices corporativos ou não, bem como atentar para a confidencialidade de informações, que podem ser utilizadas em iniciativas maliciosas, envolvendo engenharia social e outras metodologias atualmente utilizadas pela indústria do cybercrime. O ferramental tecnológico precisa ter condições de impedir, tanto quanto possível, invasões externas e a eventual atuação de agentes internos às corporações.

O desafio para alcançar a resiliência cibernética, não é simples. Trata-se de uma jornada tecnológica e cultural onde os resultados não são imediatos e onde diversas ações e iniciativas são necessárias. Mas o resultado certamente é muito positivo para as corporações que decidem trilhar essa jornada.

Kyndryl

A Kyndryl é uma das principais fornecedoras globais de serviços de infraestrutura de TI, atendendo a milhares de clientes corporativos em mais de 60 países. Como empresa focada e independente, tem em sua base de excelência parceiros que complementam as ofertas e entregam serviços que buscam cocriar soluções para ajudar as empresas a atingir seu desempenho digital máximo.

Criada em 2021, a Kyndryl atende a uma carteira internacional de clientes que contempla 75 das 100 maiores organizações globais através de seus mais de 90.000 profissionais qualificados e relevante atuação, não apenas no Brasil, mas em todo mundo. Com expertise e uma abordagem integrada voltada à resiliência cibernética, que permite aos seus clientes se anteciparem, se protegerem, resistirem e se recuperarem de eventos cibernéticos, a Kyndryl tem condições de prover aos seus clientes soluções que se apoiam em 4 pilares, formando um ciclo contínuo na busca pela resiliência cibernética.

Security Assurance Services – atuação na avaliação da maturidade da resiliência cibernética, realização de testes de invasão (Offensive Security Testing), gerenciamento de riscos e vulnerabilidades, além de foco para a conformidade, através da implementação de políticas, controles, governança e programas consistentes com o Compliance Management.

Zero Trust Services – serviços que buscam proteger os dados e a infraestrutura críticas de negócios, mantendo a infraestrutura segura através de serviços de monitoramento prestados ininterruptamente em regime 24x7 e apoiados Digital Identity Services, Data & Application Protection, Cloud Security e Zero Trust.

SecOps & Response – análise de eventos, de comportamento de usuários e aplicações, além de resposta a incidentes através de Advanced Threat Detection, Incident Response e Análise Forense.

Incident Recovery Services - busca minimizar impactos e interrupções com capacidades de recuperação rápida, simplificada e confiável dos dados e processos críticos em ambientes multicloud híbridos por meio de serviços de recuperação de incidentes através de Advisory, Managed Backup and DR services, além de Cyber Incident Recovery.

Juntamente com a Microsoft, a Kyndryl lançou no início do ano de 2023, o CoE, Centro de Excelência conjunto que visa apoiar e impulsionar o mercado da América Latina no que toca a Transformação Digital. Com equipes multidisciplinares distribuídas pelo Brasil, México, Peru e Colômbia, o CoE une a experiência da Kyndryl na modernização e gerenciamento de sistemas de missão crítica com soluções da Microsoft. Essa parceria também engloba as soluções que tocam a segurança: Os quatro pilares de serviços da Kyndryl têm por base o portfólio de soluções da Microsoft, que se coloca não apenas como fornecedora do ferramental de software, mas também como parceira no entendimento dos ambientes para implementação e adequação da solução que melhor se adeque e atenda aos requisitos, a maturidade e a realidade de cada organização. O ecossistema de segurança da Microsoft inclui as ofertas:

Microsoft Sentinel

Microsoft Defender for Cloud

Microsoft Defender for Endpopint & Servers

Microsoft 365 Defender

Microsoft Entra

Essas soluções contam com inúmeras ferramentas e opções que endereçam desde o gerenciamento, autorização de acesso, validação de transações, até identificação e bloqueio de atividades suspeitas. As soluções disponíveis também permitem a integração de SOCs ou NOCs proprietários com toda a cadeia de ferramentas e soluções de segurança da Microsoft, que inclui SIEM, Zero Trust e XDR. Em conjunto, todas essas soluções permitem a visibilidade completa e atuação para manutenção da segurança dos ambientes, independente dos fabricantes das aplicações ou do hardware utilizados, sejam esses endpoints ou servidores componentes do core das redes, de ambientes locais ou alocados em provedores de infraestrutura de cloud.

Os serviços ofertados pela Kyndryl, afinal, englobam desde o entendimento da necessidade do cliente, passando pelo assessment, avaliação da maturidade dos ambientes, implementação das soluções e ferramental, governança e realização de testes de invasão num ciclo que visa o amadurecimento da resiliência cibernética através dos serviços gerenciados de segurança.

Todo esse arcabouço de soluções e alternativas é trabalhado pela Kyndryl com especial atenção voltada ao fornecimento do serviço, seguindo o conceito do more with less, onde fatores como a qualidade e a possibilidade de redução de custos se destacam através da sinergia e facilidade para integração do gerenciamento entre as soluções. Dessa forma, é possível priorizar e focar nas migrações e adaptações necessárias, sem deixar de lado os benefícios como agilidade e simplificação das complexidades envolvidas na integração e implementação das soluções de segurança, que em última análise podem favorecer os CISOs e decisores dentro das organizações.

Desafios

A Kyndryl atende um mercado que se encontra imerso em um cenário de alta sofisticação e organização no que tocam as ameaças cibernéticas. A indústria do cybercrime adicionou elementos de complexidade e incertezas que tornam muito difícil para qualquer fabricante de tecnologia ou prestador de serviços desenvolver soluções que evitem ataques antes que esses ocorram e sejam rápida e devidamente entendidos. É importante para todas as equipes de empresas prestadoras de serviços como a Kyndryl, que estejam cientes de que não há barreiras impenetráveis para a indústria do cybercrime. O que é exequível, portanto, vai na direção do apoio para reforçar as blindagens e todos os sistemas de defesa das corporações, através da busca permanente por soluções que permitam enfrentar, evitar ou, ao menos, minimizar os impactos operacionais e eventualmente financeiros provenientes de ataques cibernéticos. Para se posicionar como um provedor com as condições necessárias para ajudar seus clientes a construírem suas fortalezas defensivas, é importante para a Kyndryl, muito mais do que deter um amplo e moderno ferramental tecnológico, ter seus times internos constantemente treinados e habilitados. O fator humano é essencial para um provedor que vise, não apenas o entendimento e utilização do potencial tecnológico disponível, mas a disseminação do conhecimento e das melhores práticas no que toca o provimento de serviços de segurança da informação.

Conclusão

As organizações buscam a resiliência digital de forma ampla, no que toca suas operações de campo, logística, produção, atendimento ao público e comunicação com stakeholders de forma geral. Trata-se de uma visão estratégica abrangente que busca manter, tanto quanto possível, ininterruptas as operações das corporações. E a capacidade necessária para isso tem como um dos pilares centrais a resiliência cibernética.

A IDC acredita que, para alcançar a resiliência cibernética, é valido e positivo o estabelecimento de parcerias junto a fornecedores de serviços que possuam condições de avaliar, propor e implementar todo o ferramental necessário para enfrentar, com barreiras e sistemas defensivos mais adequados, as consequências de iniciativas oriundas da indústria do cybercrime.

A capacidade de reagir e se recuperar de interrupções ou mudanças drásticas, que porventura ocorram devido a eventos ligados à segurança cibernética e restaurar as condições operacionais o quanto antes, é crucial para as empresas. Inicialmente pode-se ter a impressão de que o caminho para alcançar e possuir essas capacidades, é complexo e longo. De fato, não se trata de um processo trivial, mas sim de uma jornada que exige esforços para ser concluída. Para a necessária preparação das corporações contra um inimigo criativo, com grande poder de fogo e inúmeras formas de ataque, é essencial que as linhas de defesa corporativas estejam prontas e em condições de reagir para restabelecer as condições que permitam a continuidade de suas operações.

Sobre o Analista

Luiz Fernando Monteiro Francisco,
Analista Sênior de Serviços de TI, IDC Brasil.

Luiz Monteiro é analista sênior em Serviços de TI na IDC com foco no mercado brasileiro, seus provedores e organizações. Os estudos desenvolvidos pela equipe de Serviços de TI fornecem insights detalhados aos clientes da IDC por meio de análises de tamanho de mercado, análises competitivas e previsões de avanço das soluções, serviços e tendências referentes ao mercado de Serviços em TI.

IDC América Latina
4090 NW 97th Avenue Suite 350, Doral, FL, EUA 33178
+ 1-305-351-3020
Twitter: @IDCLatin
www.idclatin.com
www.idc.com

Sobre a IDC

O conteúdo deste documento foi adaptado de estudos IDC publicados em www.idc.com.

A International Data Corporation (IDC) é a empresa líder mundial em inteligência de mercado, serviços de consultoria e eventos para os mercados de Tecnologia da Informação, Telecomunicações e Tecnologia do Consumidor. Com mais de 1.100 analistas em todo o mundo, a IDC oferece experiência global, regional e local em tecnologia e tendências e oportunidades da indústria em 110 países.

O insight e a análise da IDC ajudam os profissionais de TI, executivos de negócios e a comunidade de investidores a tomar decisões tecnológicas informadas e atingir os principais objetivos de negócios. Fundada em 1964, a IDC é uma subsidiária da IDG, empresa líder em tecnologia, pesquisa e mídia de eventos. Para saber mais sobre a IDC, visite www.idc.com e www.idclatin.com

Siga-nos no Twitter como @IDCLatin / @IDC.