Whitepaper

5 tecnologias essenciais para uma estrutura de resiliência cibernética

Patrocinado por: IBM

Frank Dickson Phil Goodwin
Outubro de 2020

OPINIÃO DA IDC

O ano de 2020 foi o ponto da virada. Pela primeira vez, as pesquisas sobre segurança da IDC mostraram que a quantidade de dados corporativos em nuvem ultrapassou a quantidade armazenada localmente. Além disso, a maior parte da computação agora reside na nuvem, com 53% das cargas de trabalho encontradas na IaaS.

Infelizmente, os hackers vêm seguindo os dados até a nuvem. Nos últimos dois anos, uma típica organização sofreu 2 violações de dados na nuvem que, para serem retificadas, exigiram "a atenção de recursos adicionais significativos".[1] Assim como as violações de ambientes físicos, as invasões dos ambientes de nuvem IaaS são causadas por vários fatores. Os fatores predominantes de invasões da nuvem IaaS incluem malware avançado (17,7%), falta de ferramentas de segurança suficientes (17,7%), credenciais comprometidas (14,6%), configuração incorreta do ambiente IaaS (14,3%), vulnerabilidades não corrigidas (13,9%), ameaça interna (13,3%) e vulnerabilidades de dia zero (8,5%). Moral da história: à medida que o mercado migra para a nuvem, os hackers também o fazem. Por isso, devemos ser diligentes na garantia da segurança dos dados.

Isso não quer dizer que as tecnologias de nuvem e as novas formas de comunicação sejam a raiz do problema das violações de dados e fracassos corporativos, e sim que, ao adotarem novas tecnologias, as empresas devem adaptar suas estratégias de proteção para acompanhar o ritmo das mudanças. Essas estratégias devem prever mecanismos de segurança mais fortes e variados, mas também devem incluir formas de recuperação rápida em caso de violação ou incidente.

Empresas no mundo todo vêm abrindo espaço para a transformação digital (DX), entendida como o processo de integração da tecnologia a todos os aspectos do negócio para acelerar atividades, permitir agilidade e capitalizar a visão estratégica e as oportunidades dinâmicas. Um dos elementos essenciais da DX é ser uma organização centrada em dados capaz de monetizar informações. Ao mesmo tempo, a DX introduz, inerentemente, novos riscos talvez imprevistos ou que podem complicar o perfil de risco de processos empresariais estabelecidos. Por isso, as empresas buscam níveis mais altos de integração entre as funções essenciais de suporte ao negócio e maior disponibilidade de dados, para assegurar que estejam prontas para enfrentar qualquer desafio. Chamamos isso de resiliência cibernética.

[1] *Pesquisa sobre segurança da nuvem,* realizada pela IDC em dezembro de 2019

A resiliência cibernética combina as melhores práticas de segurança de TI, continuidade do negócio e outras disciplinas para criar uma estratégia empresarial mais alinhada às necessidades e metas do negócio digital atual. Neste whitepaper da IDC, descrevemos como a DX rompe as salvaguardas tradicionais entre empresas e participantes da economia global à medida que as tecnologias empresariais tornam-se portas para riscos, ataques e falhas. Este documento também revela como as práticas de resiliência cibernética podem ajudar a empresa a se defender contra esses riscos e a se recuperar de uma violação ou falha de forma controlada e mensurável. Por fim, o estudo oferece uma estrutura para que as organizações iniciem suas jornadas de resiliência cibernética, além de estratégias para modificar a proteção de dados e as práticas de recuperação, para um melhor alinhamento aos ataques atuais mais direcionados e mal-intencionados.

NESTE WHITEPAPER

Será que chegou o momento da verdade: o dia em que suas operações empresariais entrarão em pane?
É hoje que sua empresa vai parar completamente? Essa é uma visão pessimista da realidade empresarial.
A qualquer momento, pode ocorrer um incidente que prejudique o tecido operacional da empresa e, no acelerado mundo atual dos negócios, cada segundo importa.

Esses eventos não precisam ser catastróficos para causar um impacto duradouro. Na maioria das empresas maduras, já existe uma gestão de riscos e algumas medidas de continuidade ou resiliência dos negócios. Essas organizações provavelmente sabem que grandes incidentes com impactos avassaladores têm menos probabilidade de ocorrer do que incidentes pequenos e discretos que podem causar repercussões operacionais. Tomemos, como exemplo, o pânico da gripe aviária. Muitos se lembram de uma época, em meados dos anos 2000, em que as empresas passaram a se preocupar com o potencial impacto de um vírus propagado pelo ar nos colaboradores e nas operações empresariais. Embora o conceito seja certamente algo digno de preocupação, a probabilidade de materialização da ameaça da gripe aviária ou de outra doença similar era, e ainda é, muito baixa. Essa baixa probabilidade não impediu que as organizações tentassem criar contingências operacionais baseadas na natureza do potencial impacto. O mesmo acontece com outros desastres naturais ou ameaças físicas. O potencial de consequências de alto risco gera apreensão, e, às vezes, concentrar-se na possível dimensão de que um único incidente pode desviar a atenção do foco em ameaças reais, tangíveis e discretas, que podem ter efeitos avassaladores sobre a empresa.

A DX desafia as visões tradicionais de resiliência empresarial. Trata-se do processo pelo qual a tecnologia é entrelaçada à experiência humana. Na empresa, a DX significa um nível maior de conectividade entre aplicações e processos empresariais, a fim de aumentar a agilidade da empresa e conectá-la mais rápido a clientes e parceiros de negócios, com a expectativa de uma experiência ininterrupta 24x7 para os usuários. A DX pode acontecer de várias formas. A empresa pode querer integrar melhor a infraestrutura existente aos sistemas legados ou caminhar pouco a pouco para a nuvem, ou precisar adotar uma estratégia *cloud first*. De qualquer forma, o conceito de empresa conectada é fundamental quando avaliamos a resiliência empresarial. Não importa se essa conectividade consiste no agrupamento de processos empresariais ou na criação de ambientes de nuvem híbrida ou multinuvem; à medida que os sistemas e processos empresariais se tornam hiperconectados, cresce a probabilidade de disrupção da empresa toda por um único incidente. O que antes poderia ser considerada uma marola agora dispara ondas de choque por toda a organização.

É por esse motivo que a resiliência cibernética passou a merecer tanta atenção de profissionais de segurança e de responsáveis pela continuidade e pelo planejamento da gestão de risco da empresa. A resiliência cibernética é a fusão de práticas de cibersegurança, gestão de riscos e continuidade/resiliência, com a finalidade de criar uma disciplina focada no aperfeiçoamento dos recursos de resposta a incidentes cibernéticos, desde a detecção e recuperação do incidente até a melhoria contínua do processo. Clientes reconhecem que as tradicionais estratégias de continuidade do negócio focadas nas falhas e interrupções do sistema precisam evoluir e atentar para as ameaças cibernéticas direcionadas aos seus dados. Os antigos procedimentos de recuperação em caso de interrupção do sistema provavelmente não protegerão a empresa contra ameaças cibernéticas de danos aos dados.

A ascensão e as falhas da DX

Haverá um aumento nas despesas de DX de práticas empresariais, produtos e organizações, apesar dos desafios econômicos provocados pela COVID-19 (ou por causa deles). Em 2021, o investimento mundial em tecnologias e serviços de DX terá um aumento de 16,6%, chegando a US$ 1,54 trilhão. Esse crescimento será notavelmente maior que os 10,4% estimados para 2020, porque, em 2021, as empresas procurarão implementar a DX para compensar os impactos econômicos negativos da pandemia da COVID-19, um fenômeno que a IDC chama de "achatamento da curva" da crise econômica (ver Figura 1). Até mesmo os setores que sofreram o maior impacto de fatores econômicos terão um crescimento contínuo no investimento em DX. O setor de serviços pessoais e ao consumidor, que inclui hotéis, parques temáticos, cassinos e cinemas, terá um aumento de 16,0% nas despesas de DX em 2021. Os setores que deverão apresentar o maior aumento em despesas de DX em 2021 são os de construção civil (27,9%) e varejo (20,3%).

FIGURA 1

Achatamento da curva: como a tecnologia cria resiliência e aumenta a agilidade

Fonte: IDC, 2020

Há graus variados de adoção da DX entre as organizações. Muitas adotaram uma abordagem proativa, indicando a existência de "um plano de investimento de longo prazo, e que a estratégia da empresa é usar a DX para transformar mercados e clientes ao criar novos modelos de negócio e experiências de produtos/serviços". Algumas estão procurando ser mais proativas. Fica claro que a DX é uma prioridade para as organizações, seja qual for o grau de adoção (ver Figura 2).

FIGURA 2

Posição sobre a DX

P. Antes da pandemia da COVID-19, como você classificaria a posição da sua organização com relação à transformação digital?

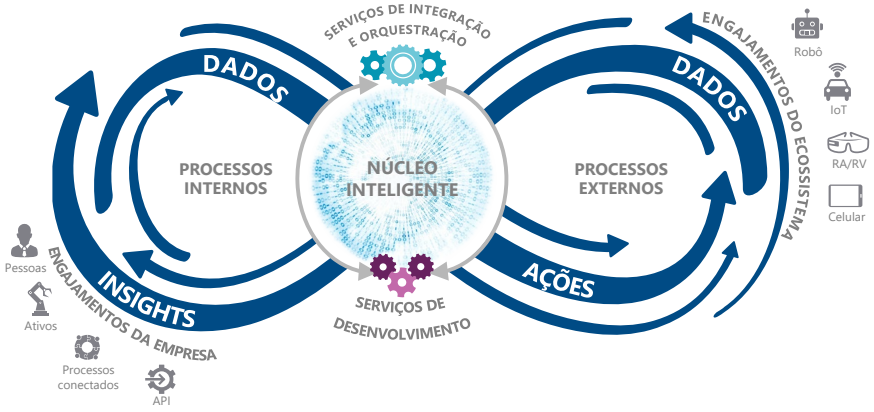
n = 880

Fonte: *Pesquisa da IDC sobre o impacto da COVID-19 nas despesas de TI*, 4 a 15 de junho de 2020

Por que gastar tanto? Em poucas palavras, as empresas acreditam que a DX é o caminho do futuro em um mundo hiperconectado. As empresas precisam descobrir inovação e agilidade para se manterem viáveis e devem estar preparadas para colocar novos produtos e serviços no mercado rapidamente e em grande escala, enquanto desenvolvem os insights fundamentais e necessários para alcançar os públicos desejados e abrir novos mercados. De fato, a IDC acredita que o pico da transformação permitirá que a maioria das organizações alavanque uma infraestrutura para o núcleo de inteligência que converterá o insight da atividade empresarial em inteligência acionável, de forma otimizada e contínua. A IDC descreve isso como a plataforma DX (ver Figura 3). Em seu núcleo, essa plataforma depende de dados diversos, distribuídos e dinâmicos para gerar oportunidades.

FIGURA 3

Plataforma DX: uma estrutura para o núcleo de inteligência



Fonte: IDC, 2020

Sem dados, o modelo falha. Os dados não podem mais ser produzidos ou monetizados. Não podem mais ser alavancados para melhorar a agilidade do negócio. Isso os torna essenciais à sobrevivência da empresa e, assim, torna sagrada a integridade e a acessibilidade aos dados. No entanto, os atributos e a localização dos dados relevantes à plataforma DX continuam mudando. Os dados ficaram ainda mais diversos e abrangem não apenas os sistemas estruturados, mas também os dados não estruturados, como os de série temporal, os gerados por máquina e os de fluxo. Os dados também estão cada vez mais dinâmicos; além de se basearem em processamento em lote, também têm natureza de tempo real, já que os dados telemétricos são gerados de um número cada vez maior de sensores e dispositivos. Além disso, os dados estão cada vez mais distribuídos, localizados não apenas em data centers centrais mas também em localizações de borda, em dispositivos e em serviços de nuvem. Com dados diversos, dinâmicos e distribuídos, acentua-se ainda mais a capacidade de empregar um programa de resiliência cibernética eficaz.

Isso não significa que os dados são a única coisa a ser levada em conta. Para a maioria das organizações, a jornada de DX começa com uma série de sistemas superficialmente conectados que, esperam elas, possa ser estabelecido como um sistema interconectado. Vamos pensar na DX em termos da máquina de Rube Goldberg. Para os leigos, Rube Goldberg foi um engenheiro, inventor e cartunista ganhador do Prêmio Pulitzer que ficou famoso pelos desenhos de sistemas complexos nos quais retratava artigos domésticos comuns interconectados por fios para realizar alguma tarefa banal. Se isso parece familiar, ótimo. As empresas estão conectando por fios os sistemas de RH, de gestão de contratos, de ERP, as aplicações voltadas para o cliente e outros na esperança de que eles operem em uma direção comum que impulsione os negócios. É aqui que a DX começa a apresentar desafios para os encarregados de reduzir os riscos empresariais.

O que acontece quando você enfia um cabo de vassoura entre os raios da roda de bicicleta? Se os raios não estiverem conectados a nada, provavelmente nada acontecerá; porém, os raios da roda estão conectados. Quando um ou dois raios são imobilizados por um objeto estranho, a roda inteira para de girar. Esse é o risco dos sistemas empresariais interconectados. Quando um único sistema cai, isso pode significar a paralisação da empresa inteira.

Em termos de resiliência cibernética, isso significa que qualquer processo empresarial poderia representar uma porta para outros. Ou seja, a superfície de ataque de um processo tem o potencial de garantir acesso lateral a praticamente qualquer outro processo.

Desafios na jornada de DX

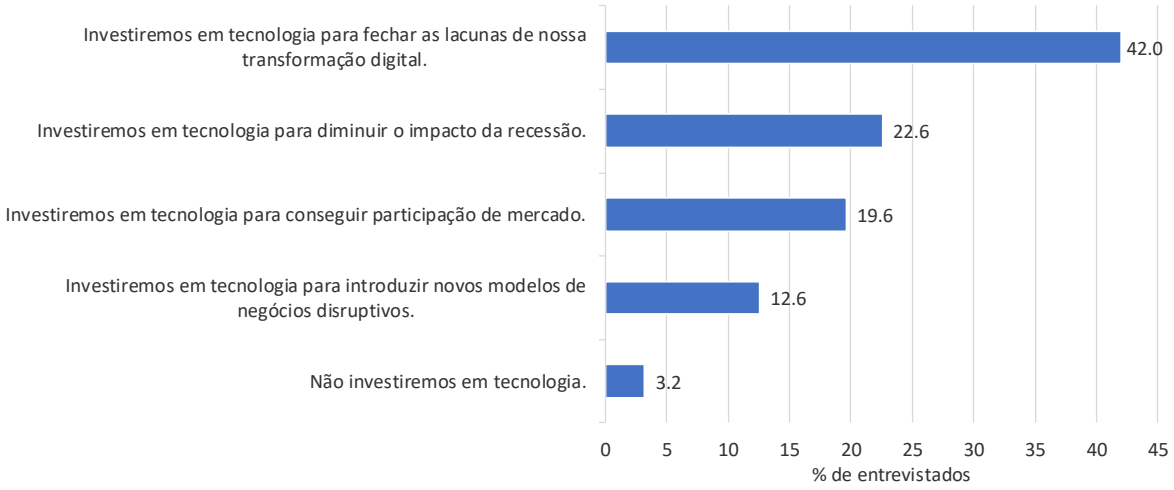
Embora o investimento em DX seja impressionante, a IDC já enxerga pressões externas cada vez maiores começando a ter impacto significativo sobre a estratégia de cibersegurança das organizações. Como mencionado antes, a interconexão de sistemas e a contínua dependência de serviços externos, como nuvem e IoT, trarão riscos para os quais muitas organizações não estão preparadas atualmente.

Além do mais, a DX não se desacelera em tempos de crise; ao contrário. Em uma recente pesquisa da IDC, apenas 3% dos entrevistados disseram que não vão investir em tecnologia para enfrentar a retração econômica (ver Figura 4).

FIGURA 4

Estratégias de investimento em tecnologia para enfrentar a retração econômica

P. Qual frase melhor corresponde à forma como sua organização vem tratando o investimento em tecnologia relacionado à iniciativa de transformação digital?



n = 880

Fonte: *Pesquisa da IDC sobre o impacto da COVID-19 nas despesas de TI*, 4 a 15 de junho de 2020

Muito embora um investimento agressivo seja impactante, não fica claro quantas dessas organizações reconhecem que a disponibilidade de dados e aplicações (informações) é fundamental para o sucesso da DX. Sem disponibilidade, não é possível monetizar os dados. Ter mais informações disponíveis proporcionará às empresas uma vantagem competitiva relativa sobre aquelas que enfrentam problemas de disponibilidade. Ainda que a IDC tenha identificado um aumento nas despesas com produtos e serviços de combate a DDoS, muitos clientes têm dificuldades de implantar uma estratégia coerente de disponibilidade de informações que ofereça a preservação rápida e completa dessa disponibilidade durante todo o processo de acesso aos dados.

Um outro desafio externo das organizações é o aumento da compliance regulatória. Até 2025, mais de 70% dos dados corporativos estarão sob compliance regulatória. Além de exigirem tratamento especial, esses dados criam riscos adicionais para a organização, que pode sofrer penalidades rigorosas se não protegê-los adequadamente.

Dependência crescente de nuvem e IoT

Propiciar a disponibilidade de dados sem fricção e assegurar o acesso menos privilegiado a dados de compliance às vezes são duas forças opostas que impactam significativamente o negócio mas, ao mesmo tempo, às vezes os recursos da organização de afetar cada uma podem ser limitados. À medida que mais empresas dependem da nuvem e de dispositivos IoT para funções críticas, a capacidade de oferecer acesso sem fricção e dentro das regras de compliance a dados sensíveis se torna um desafio cada vez maior.

Hoje em dia, as organizações usam a nuvem híbrida, e a maioria das aplicações futuras serão habilitadas para a nuvem. Em uma recente pesquisa da IDC, as organizações relataram que atualmente 53% de suas cargas de trabalho são implantadas em um modelo de nuvem IaaS. A segurança é tanto um incentivo como um freio para a adoção da nuvem híbrida. Dados críticos agora se espalham por diferentes áreas geográficas, data centers e nuvens. Estes dados devem ser protegidos de acordo com os requisitos corporativos, seja onde residam. As organizações pesquisadas calculam que metade de todos os dados corporativos são armazenados na nuvem. E desses, 48% são considerados sensíveis. O backup e recuperação e a avaliação do custo/valor dos dados são as principais prioridades.

As empresas coletam cada vez mais dados sensíveis, não apenas da nuvem mas também de dispositivos IoT. Embora esses dispositivos geralmente possuam um poder de processamento menor que sistemas completos, invasores têm recursos comprovados para aproveitar dispositivos IoT em suas estratégias de ataque. Esses recursos, combinados à falta generalizada de segurança dos dispositivos IoT, significa que as organizações devem definir como irão defender melhor esses dispositivos difíceis de acessar, monitorar e proteger, além dos equipamentos de computação tradicionais.

Interrupções cada vez mais complexas

Embora a IDC tenha percebido organizações mais confiantes na capacidade de proteger a nuvem e um aumento na taxa de migração para a nuvem e de adoção de soluções de segurança em nuvem, um dos desafios para os quais as organizações parecem estar menos preparadas é o problema iminente de potenciais violações.

Em uma pesquisa recente conduzida pela IDC, 73% dos entrevistados relataram ter sofrido graves violações de segurança em seus ambientes IaaS, nos últimos 2 anos, que exigiram despesas extras para a correção. De fato, o número mediano de violações nos últimos dois anos foi de 2,0.

Soluções legadas de backup e recuperação de desastre (DR) são proteções insuficientes contra as ameaças modernas. A IDC recomenda como boa prática um RTO de uma hora para aplicações de missão crítica e de quatro horas para as não essenciais. Certas cópias pontuais (instantâneos) podem estar incompletas ou ser ineficazes e vulneráveis ao ataque quando projetadas de forma inadequada. A abordagem é, muitas vezes, concebida para a recuperação do sistema e não para a recuperação ambiental, como danos à plataforma ou à configuração. Falhas de manutenção e teste também podem sabotar esquemas robustos de proteção com cópia de dados pontuais.

A pesquisa da IDC revela que o custo "médio" do tempo de inatividade ultrapassa US$ 200.000 por hora, embora isso varie de acordo com o tamanho da empresa e o setor. Em algumas organizações, decisores de TI contaram que o tempo de inatividade de aplicações ERP essenciais, como Oracle E-Business Suite e SAP Business One podem, sozinhos, custar US$ 200.000 por hora. Normalmente, esses custos podem ser usados para guiar a organização na criação de planos e infraestrutura de remediação. As estimativas de custo incluem a perda real de receita e os custos de recuperação, inclusive os regulatórios, que podem ser significativos. Os cálculos não abrangem o custo reputacional e os danos de longo prazo à marca que podem resultar de uma violação constrangedora. No entanto, eles podem ser usados para determinar a despesa organizacional adequada para a estratégia de infraestrutura de remediação de violações. Um exemplo recente de ransomware ilustra bem essa situação. Em abril de 2020, uma multinacional de serviços de TI confirmou publicamente que sua rede havia sido atingida pelo ransomware Maze, que criptografou servidores, restringiu os recursos de teletrabalho e neutralizou ferramentas usadas para automatizar e provisionar notebooks. O Maze é uma forma especialmente perniciosa de ransomware, pois além de criptografar dados, também os extrai do sistema infectado, permitindo que os cibercriminosos exijam mais recompensas, ameaçando expor publicamente os dados da empresa. O impacto nessa empresa de serviços de TI foi calculado em aproximadamente US$ 50 a US$ 70 milhões na primeira metade de 2020, com custos adicionais de advogados e outros profissionais associados à restauração e à remediação esperada do serviço.

Ataques avançados em alta

A IDC também continua observando um aumento no número de ataques avançados. As estatísticas do setor mostram que muitos ataques permanecem não detectados por mais de 200 dias. Com tanto tempo se escondendo na rede, o invasor pode plantar um malware que encontra o caminho dos conjuntos de backup; com isso, os dados de recuperação também são infectados. Os ataques podem permanecer inativos durante semanas ou meses, permitindo que o malware se propague pelo sistema. Até mesmo após a detecção do ataque, pode ser muito difícil remover um malware tão impregnado na organização toda.

VISÃO GERAL DA SITUAÇÃO

O conceito de resiliência cibernética

Os recursos de infraestrutura estão cada vez mais disponíveis na nuvem e nos dispositivos IoT. No entanto, as defesas tradicionais têm sido ineficazes para conter com êxito as ameaças emergentes. Com isso, as organizações precisam abordar a segurança de outra forma. O cenário de ameaças

atual exige uma solução integrada que abranja todo o ciclo de vida dos dados. As organizações precisam se concentrar em reduzir os estágios do ciclo de vida entre defesa, detecção, resposta e recuperação para desenvolver uma capacidade de resiliência cibernética. Em uma recente pesquisa da IDC, os entrevistados identificaram a "criação de planos de resiliência robusta" como prática tecnológica importante para proteger a rede.

A estrutura de resiliência cibernética

A resiliência cibernética é uma estrutura projetada para ajudar as organizações a resistir a ataques. Não se trata de uma mera camada de proteção ou de um único produto, mas de uma forma de estruturar as defesas da organização para que nenhum incidente se torne uma catástrofe. A resiliência cibernética é um processo iterativo que fornece medidas de recuperação após um ataque. Comparada às defesas tradicionais que se mostram inúteis uma vez ultrapassadas, a resiliência cibernética permite vigilância contínua na organização toda.

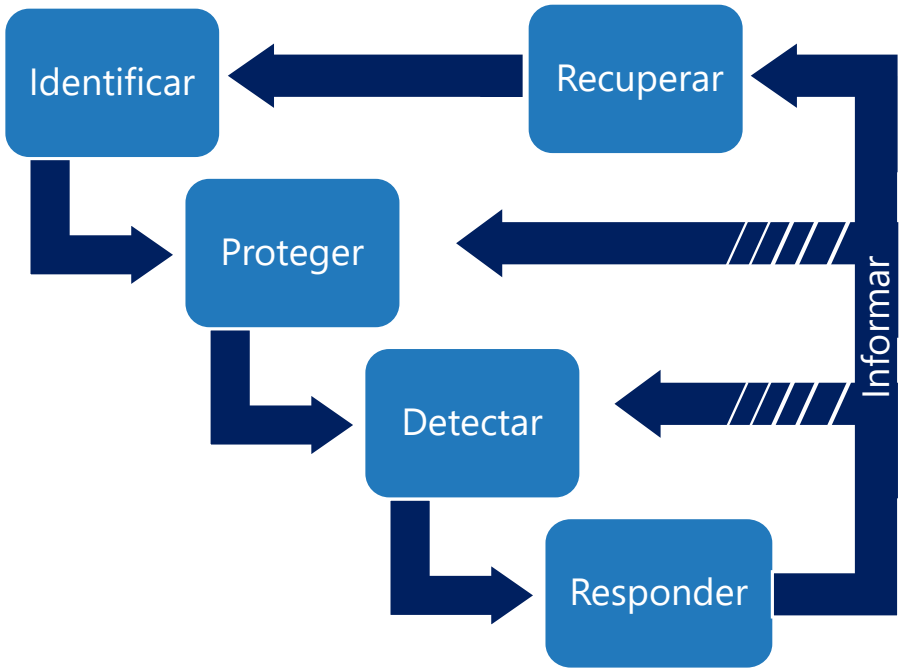
Os 5 componentes da estrutura de resiliência cibernética são (ver Figura 5):

- **Identificar:** mapeamento de ativos e processos essenciais, avaliação de risco e prontidão, etc;
- **Proteger:** mecanismos de segurança tradicionais de primeira linha de defesa;
- **Detectar:** análise de segurança, verificação da integridade de dados com configuração em tempo real;
- **Responder:** resposta a violações ou falhas de segurança;
- **Recuperar:** mecanismos coordenados de recuperação.

A principal vantagem da estrutura de resiliência cibernética é que coloca o negócio em primeiro plano. Tradicionalmente, a segurança opera em sobreposição ao negócio. A resiliência cibernética integra a segurança ao próprio negócio, permitindo que os 5 componentes se façam presentes em todas as áreas da empresa.

FIGURA 5

Estrutura de resiliência cibernética



Fonte: IDC, 2020

O incidente e o resultado

Não há dúvida de que, ao longo do tempo, sempre acontecerão ataques neste setor. A segurança é um assunto complexo, e simplesmente não existe maneira de comprovar que um ambiente é completamente seguro. Invasores continuarão usando métodos inéditos para entrar nas organizações, recorrendo a todas as táticas necessárias par lançar um ataque bem-sucedido. À empresa só resta ter uma infraestrutura forte, funções e processos auditáveis, usuários bem treinados, uma equipe de segurança de excelência e processos continuamente monitorados. Essa situação seria a ideal. No entanto, para a maioria das organizações, a chave pode ser redirecionar o foco para o que acontece após um ataque. Se, de posse de uma lista de controles e verificações, podemos saber que um ataque acontecerá em algum momento, não faz sentido nos prepararmos para o resultado? Quando um ataque acontece, a empresa deve encontrar uma maneira de reduzir o tempo entre detecção e resposta, e entre resposta e recuperação. Quanto mais próximo uma empresa conseguir chegar da operação contínua, melhor. Mesmo após um ciberataque bem-sucedido.

O negócio não perdoa. Para o negócio, tanto faz se foi um ataque avançado ou se o invasor conseguiu se infiltrar na organização. O negócio precisa continuar, mas persistência não é suficiente. Os clientes de hoje são exigentes, principalmente em tempos de crise. Nesse mundo digital, eles querem serviços sempre disponíveis, e as empresas não podem se dar o luxo da indisponibilidade. Antes da pandemia da COVID-19, as operações de negócio resilientes e os programas de experiência do cliente estavam

entre as menores prioridades. Depois que a pandemia começou, passaram a ocupar os primeiros lugares na lista. Em tempos de crise, a continuidade das operações e a atenção ao cliente são as maiores prioridades (ver Figura 6).

FIGURA 6

Prioridades da alta administração: antes e depois da COVID-19

Prioridades pré-COVID-19 (janeiro de 2020)

Classificação das prioridades	Itens da agenda futura da empresa
1	Programas de confiança digital
1	Resiliência da infraestrutura digital
3	Programas de dados (para ganhar insights para nossas operações empresariais, produtos e/ou ecossistemas)
4	Transformação do local de trabalho
4	Recursos de desenvolvimento de software para impulsionar a inovação de produtos/experiências
4	Novos ecossistemas do setor
7	Operações empresariais resilientes
8	Programas de experiência do cliente
9	Programas de conectividade

Prioridades pós-COVID-19 (maio de 2020)

Classificação das prioridades	Itens da agenda futura da empresa
1	Operações empresariais resilientes
2	Programas de experiência do cliente
3	Programas de dados (para ganhar insights para nossas operações empresariais, produtos e/ou ecossistemas)
4	Programas de conectividade
5	Recursos de desenvolvimento de software para impulsionar a inovação de produtos/experiências
6	Programas de confiança digital
7	Novos ecossistemas do setor
8	Resiliência da infraestrutura digital
9	Transformação do local de trabalho

n = 483 (prioridades pré-COVID-19); n = 908 (prioridades pós-COVID-19)

Obs.: os entrevistados são decisores de tecnologia do mundo todo.

Fonte: *CxO View of the Future Enterprise in the Digital Economy Survey,* janeiro-fevereiro de 2020 e *COVID-19 Impact on IT Spending Survey,* 7-14 de maio de 2020, ambos da IDC.

Ao aproveitar as estratégias para reduzir o tempo operacional de detecção, resposta e recuperação, as organizações podem diminuir o custo de um incidente e criar uma vantagem competitiva. A IDC acredita que as empresas que conseguirem minimizar as interrupções terão vantagem significativa sobre as empresas mal preparadas, pois obterão a confiança dos consumidores e dos parceiros de negócios.

VISÃO DO FUTURO

5 tecnologias fundamentais da resiliência cibernética

Embora possa parecer intuitiva, a estrutura de resiliência cibernética deve ser implementada com a seleção cuidadosa de tecnologias. Não existe um produto único para criar um ambiente de resiliência cibernética, mas há tecnologias fundamentais que uma organização pode implementar para lidar com o potencial de interrupção do negócio por um ciberataque. As 5 tecnologias descritas nas seções a seguir são decisivas para a criação de um ambiente resiliente.

Automação e orquestração para a recuperação de plataformas e dados de aplicações

Automação sempre foi um termo assustador para os profissionais da segurança. Desde o surgimento das soluções automatizadas, existe uma preocupação generalizada no setor com relação à resposta automática. Contudo, no atual ambiente de ataques automatizados, a automação da inteligência é

crucial, já que a falta de competências de TI continua a ser uma realidade incômoda; serão necessários mais 10,5 milhões de profissionais em tempo integral nos próximos cinco anos (ver Figura 7). Em vez de depender apenas dos métodos tradicionais como solução, os profissionais de segurança devem incluir a orquestração e a automação na resposta.

FIGURA 7

Falta de competências de TI

Fonte: IDC Worldwide Technology Employment Impact Guide. 2018H2

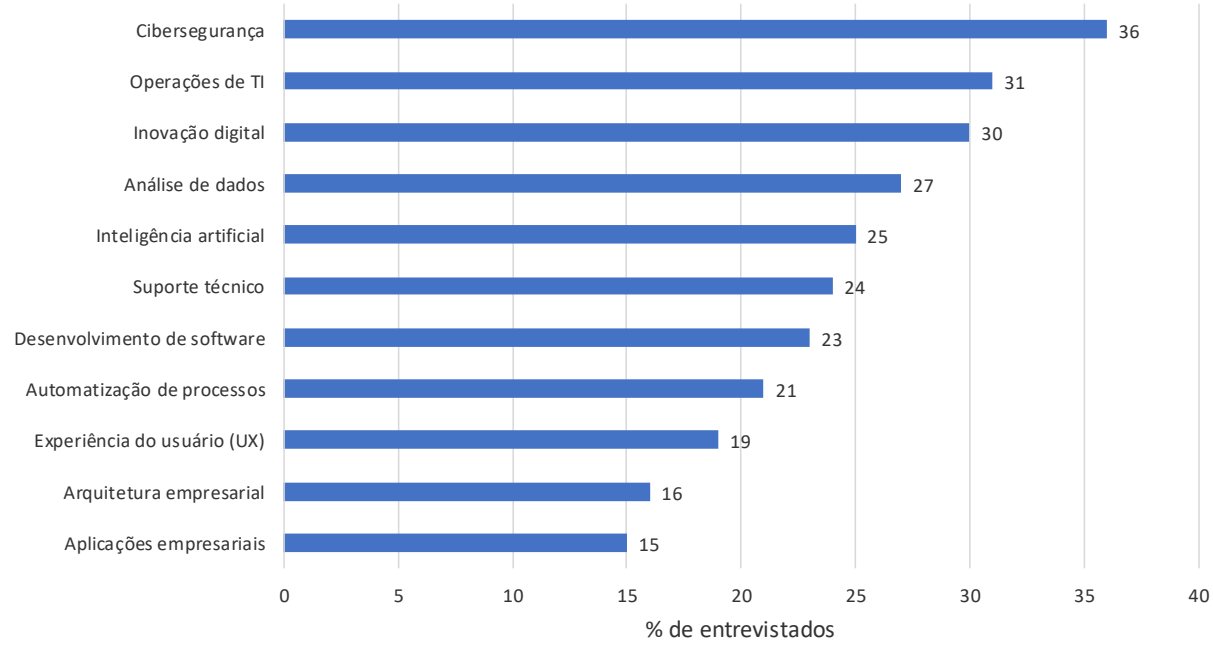
Fonte: IDC, 2020

As épocas de crise só fazem aumentar a demanda por competências escassas. As organizações apontaram a cibersegurança e as operações de TI como as principais competências de TI necessárias para a recuperação após a pandemia da COVID-19 (ver Figura 8).

FIGURA 8

Competências de TI importantes a serem adquiridas/recriadas/contratadas na primeira onda de recuperação econômica

P. *Quais serão as competências de TI mais importantes a serem adquiridas/recriadas/contratadas por sua organização na primeira onda de recuperação econômica [após a pandemia da COVID-19]?*



n = 888

Fonte: *Pesquisa da IDC sobre o impacto da COVID-19 nas despesas de TI,* realizada entre 4 e 15 de junho de 2020

Orquestração não significa eliminar seres humanos da equação ou permitir mudanças cegas nas políticas, e sim, aumentar o número de analistas e oferecer-lhes acesso rápido às informações e a capacidade de responder mais rápido do que manualmente. Além disso, o sucesso na recuperação de aplicações exige uma recuperação de sistemas e dados interconectados realizada em vários estágios. A recuperação manual desses sistemas pode introduzir erros humanos, ao passo que a codificação dos processos de recuperação com modelos de software validados e testados pode diminuir os riscos.

Proteção hermética como cópia à prova de erros contra a propagação de malware

Hermético se refere a sistemas ou redes física ou virtualmente separados uns dos outros. As empresas, por exemplo, podem optar por separar completamente as redes ou sistemas que contêm dados altamente sensíveis daqueles usados nas operações diárias.

Embora o perímetro tenha desaparecido e as empresas contem com a fluidez de seus dados na organização toda, a capacidade de criar segmentos de rede herméticos é mais importante do que nunca. Como vimos nas infecções recentes por ransomware, é possível designar um fragmento automatizado de malware para atravessar rapidamente a rede e causar devastação imediata. Isso deixa a organização exposta internamente e talvez na parte externa, dependendo do sistema ou sistemas infectados. Atualmente, a melhor prática é criar uma cópia hermeticamente fechada dos dados críticos para diminuir a exposição externa, proteger a organização contra a indisponibilidade operacional e evitar custos desnecessários.

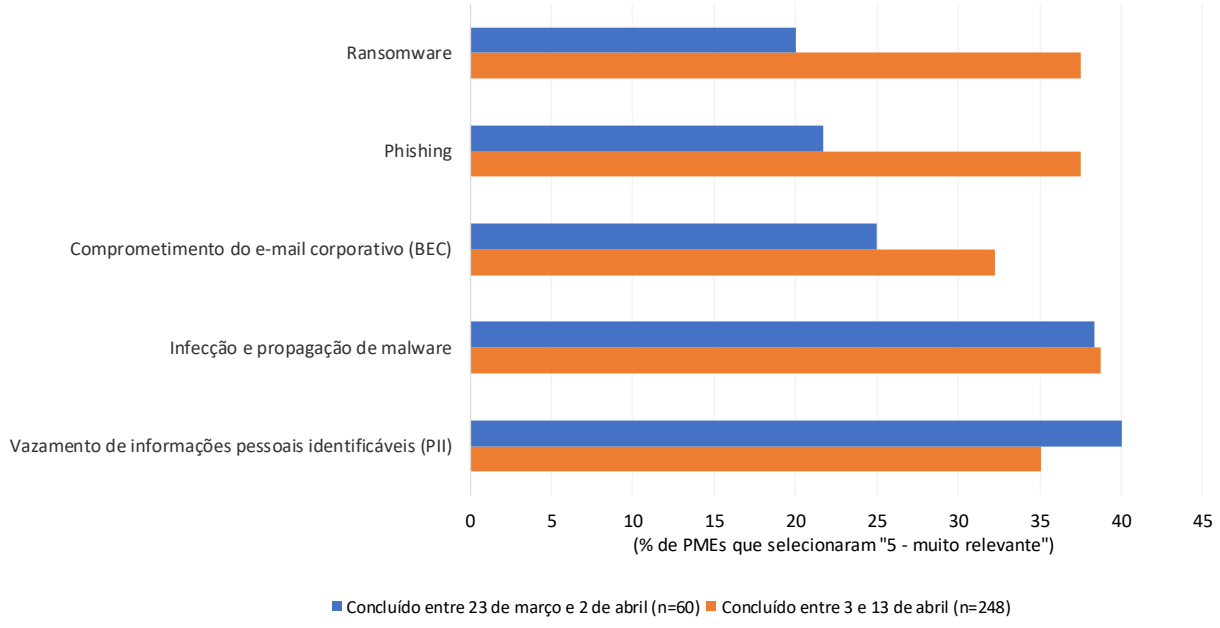
Tecnologia write-once, read many/armazenamento imutável para impedir danos ou exclusões

O recente sucesso dos ataques de ransomware ilustrou a necessidade de proteção mais forte contra danos ou exclusões de dados. Os criminosos digitais são oportunistas e esperam momentos de fraqueza para atacar. O recente pico de malware relacionado à COVID-19 ilustra isso (ver Figura 9).

FIGURA 9

Visões da evolução do risco com a pandemia

P. Classifique a relevância dos produtos de segurança na redução dos seguintes riscos (onde 1 = irrelevante e 5 = muito relevante).



Fonte: *Pesquisa da IDC sobre segurança de pequenas e médias empresas nos EUA,* 2020

Sabe-se que invasores procuram eliminar registros para apagar suas pegadas, mas a exclusão ou danificação de dados pode destruir uma empresa. No rescaldo de RobbinHood, Maze e REvil, assim como de outros ataques de ransomware, várias organizações descobriram que o pagamento do resgate não resultava necessariamente na entrega da chave de criptografia pelo criminoso. Em alguns casos, a chave fornecida pelo malfeitor sequer funcionou.

As organizações precisam de tecnologias que ofereçam dados inalteráveis. As tecnologias write-once, read-many (WORM)/armazenamento imutável podem ser a resposta para essa questão. Com as tecnologias WORM/armazenamento imutável, a organização pode manter a integridade de seus dados e a resiliência da empresa contra os ataques considerados os mais devastadores dos últimos tempos. Existem diferentes formas de tecnologia WORM na camada de software e de hardware. Ambas proporcionam um meio de impedir a adulteração de dados e oferecem uma cadeia de custódia eletrônica.

Cópias pontuais eficientes e verificação de dados para a rápida identificação de dados recuperáveis

Ocorrido um ataque, a organização precisa de uma forma de validar e recuperar rapidamente as boas cópias de dados mais recentes ("cópias de ouro"). Como mencionamos antes, muitos invasores moram dentro das redes por quase um ano, o que significa que geralmente os backups também são infectados. É por tal motivo que é necessário ter uma tecnologia pontual altamente eficiente para manter várias cópias dos dados. É preciso fazer uma verificação contínua dos dados dessas cópias para identificar proativamente as potenciais infecções e tomar as medidas corretivas. Isso também ajuda a identificar rapidamente uma boa cópia de dados para o processo de recuperação. Existem diferentes abordagens à verificação de dados de backup, com recursos incorporados a software e hardware para assegurar que os dados não tenham sido infectados.

A verificação de dados é obrigatória nos processos de teste de recuperação de desastre e operações. Em primeiro lugar, convém garantir que os dados de backup/replicados estejam íntegros e que o backup/replicação seja realizado conforme esperado. Em segundo lugar, deve-se inspecionar os dados de backup/replicados para garantir que a mesma infecção que atingiu os dados de produção não tenha se espalhado para os dados de backup/replicados. Dependendo do sistema em processo de backup, o usuário pode empregar diferentes técnicas de verificação de dados. Por exemplo: o sistema de banco de dados pode ter ferramentas de triagem e inspeção nativas úteis para complementar os recursos de uma solução de proteção de dados mais ampla.

Painel unificado e relatórios orquestrados para ganhar visibilidade e controle

Embora a compliance regulatória tenha ganho a reputação de ser uma mera burocracia que não melhora a segurança geral da organização, a verdade é que, validar a existência e a operação correta dos controles adequados de dados pode ser extremamente eficaz para promover uma gestão proativa. Além disso, com multas cada vez maiores nos casos de falta de compliance, ter um sistema de relatórios competente pode ajudar a organização a provar que está observando as regras e a economizar o tempo e dinheiro associados a auditorias dispendiosas e potenciais penalidades. O relatório de auditoria não precisa ser complicado ou entediante; um painel eficaz e relatórios pré-configurados e automatizados resolvem isso e melhoram drasticamente o moral das pessoas responsáveis por administrar a tarefa.

DESAFIOS E OPORTUNIDADES

A cibersegurança é o principal desafio do cenário empresarial atual. O ritmo e o volume das ameaças à segurança são obstáculos que organizações de todos os tamanhos querem superar. Com isso cresce a importância do planejamento e implantação de estratégias de resiliência cibernética. Uma estratégia de resiliência cibernética eficaz é ampla em termos de alcance e stakeholders, reunindo diferentes componentes.

Entre os principais interessados estão, não apenas os profissionais de segurança, operações, engenharia, direito e risco, mas também os proprietários de dados e os executivos de linha de negócio. Exige-se colaboração e planejamento envolvendo organizações com diferentes prioridades e graus de conhecimento. Essa dinâmica organizacional é um desafio comum em grandes empresas, mas que pode ser gerenciada por meio de um planejamento estratégico e a definição de prioridades pela alta administração.

CONCLUSÃO

A resiliência cibernética é fundamental para a disponibilidade de dados e aplicações. Também é um componente essencial da jornada de DX. Sem uma resiliência cibernética adequada, as organizações se veem cada vez mais suscetíveis a ataques que podem paralisar seus negócios. Além dos ataques nocivos, o número cada vez maior de regras que se estendem por diferentes áreas geográficas e setores pode sujeitar a empresa a multas altíssimas sem a validação contínua dos controles.

A prática também consiste em mais do que uma simples detecção de malware, backup e recuperação. Ela usa a abordagem de ciclo de vida integrado, envolvendo interessados de todos os departamentos da empresa, inclusive CIO, CSO, CRO e Operações de TI, todos trabalhando em conjunto para proporcionar disponibilidade de dados contra todas as ameaças, inclusive a plataforma. A resiliência cibernética deve abarcar os repositórios locais e da nuvem. As organizações de TI devem adotar uma abordagem abrangente com relação à resiliência cibernética e procurar produtos que lidem com a grande variedade de ameaças cibernéticas e ofereçam a capacidade de recuperação rápida após ataques.

Por fim, a resiliência cibernética é uma estrutura para a recuperação após ataques. No entanto, é necessário um sólido conjunto de tecnologias de apoio para garantir que cada estágio da estrutura possa ser alcançado. A segurança não pode mais ser descrita em termos de níveis variados de confidencialidade, integridade e acessibilidade. Ela deve sempre englobar todos esses três pilares. A organização que implementar resiliência cibernética estará em vantagem competitiva no futuro, pois o cliente encontrará lacunas na disponibilidade das empresas. Uma organização resiliente é aquela que consegue se adaptar e se recuperar rapidamente após um ataque.

Sobre a IDC

A International Data Corporation (IDC) é a principal fornecedora global de inteligência de mercado, serviços de consultoria e eventos para os setores de tecnologia da informação, telecomunicações e tecnologia de consumo. A IDC ajuda profissionais de TI, executivos e a comunidade investidora a tomar decisões baseadas em fatos para a compra de tecnologia e estratégias de negócios. Mais de 1.100 analistas da IDC oferecem conhecimento global, regional e local sobre tecnologia e oportunidades e tendências do setor em mais de 110 países. Há 50 anos, a IDC fornece informações estratégicas para ajudar o cliente a atingir seus objetivos de negócios. A IDC é subsidiária da IDG, a maior empresa de mídia, pesquisa e eventos de tecnologia do mundo.

Sede global

5 Speen Street
Framingham, MA 01701
EUA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com