Guardians of digital trust
Cybersecurity Awareness Month

Principais ameaças cibernéticas e previsões para 2025

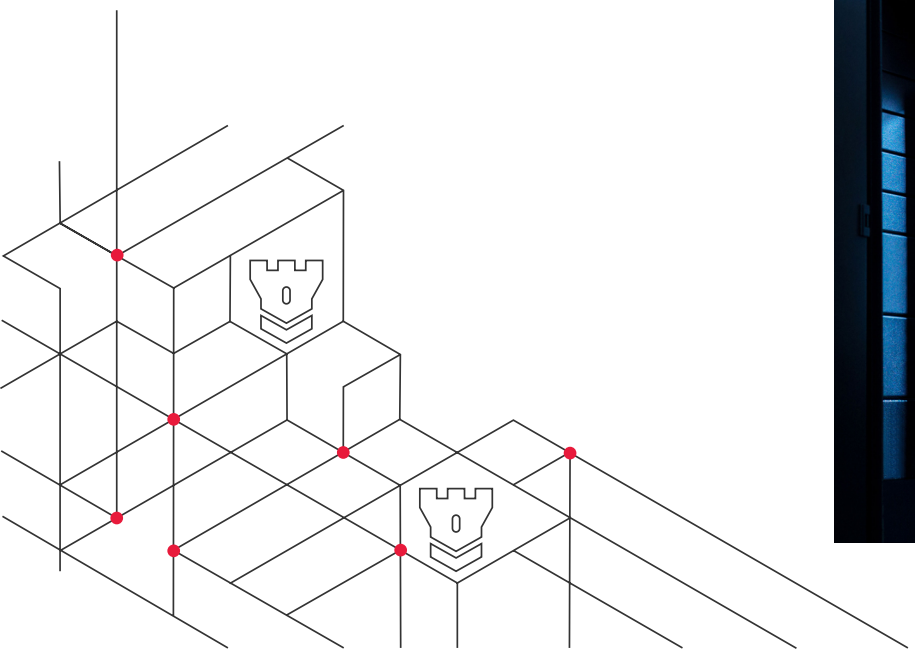
BDO

Principais ameaças cibernéticas e previsões para 2025

Novas tecnologias deram às empresas maiores capacidades de análise de dados, comunicação e eficiência operacional. No entanto, também tornaram os agentes de ameaça, que vão desde atores de estados-nação a cibercriminosos, mais sofisticados. À medida que o nosso mundo se torna mais digitalmente interconectado, observamos a integração da inteligência artificial com ataques cibernéticos, aumentando a gravidade desses ataques.

Manter-se um passo à frente nesta corrida digital requer a adoção de medidas de vanguarda. Por exemplo, a utilização de soluções de segurança potenciadas por IA Generativa pode melhorar drasticamente a forma como as equipas de segurança operam, promovendo eficiências e reduzindo riscos. As tecnologias de segurança baseadas em IA Generativa podem ajudar a identificar riscos de maior prioridade e a implementar procedimentos de resposta automatizados. Estas soluções podem ajudar a sua equipa de segurança a libertar tempo valioso, melhorar a deteção e acelerar a resposta e a recuperação, mantendo o seu negócio em crescimento.

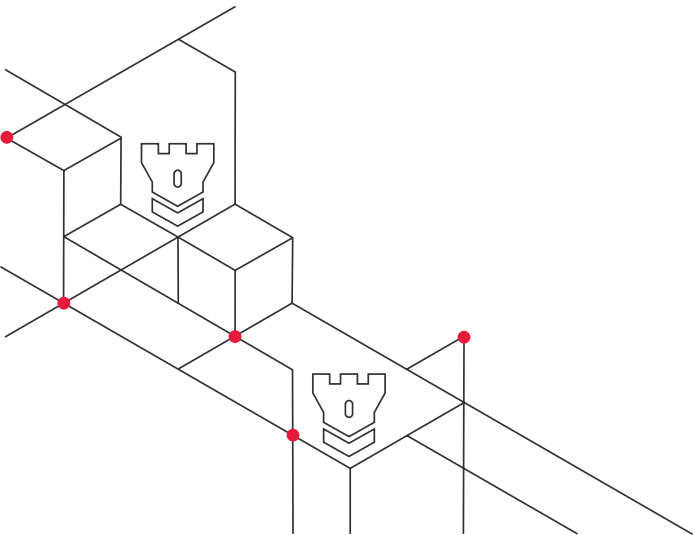
Compreender as ameaças emergentes que as empresas enfrentarão em 2025 também é crítico. Este artigo discute as maiores ameaças e as principais estratégias para ajudar a manter a sua proteção.



O aumento do custo dos ataques cibernéticos e a importância da resiliência

De acordo com o Relatório de Custo de uma Violação de Dados da IBM de 2024, os custos das violações aumentaram 10% em relação ao ano anterior, a maior subida anual desde a pandemia. Além disso, 26% mais organizações enfrentaram graves escassezes de pessoal em comparação com o ano anterior e observaram um aumento médio de 1,76 milhões de dólares nos custos de violações do que aquelas com problemas de pessoal de segurança de baixo nível ou inexistentes. Esta constatação sublinha a alarmante lacuna na capacidade das organizações de identificar, detetar e responder a ameaças cibernéticas antes que o impacto seja sentido. No entanto, há boas notícias. O relatório também revelou que 42% das violações de dados foram descobertas por equipas de segurança, uma melhoria de 9% em relação ao ano passado. Este aumento é atribuído a um maior investimento em planeamento cibernético e deteção de ameaças, bem como à adoção de tecnologia de IA para colmatar lacunas de recursos.

Embora estas melhorias sejam promissoras, ainda há um espaço significativo para crescimento. O panorama de ameaças em evolução, alimentado por tensões geopolíticas e métodos de ataque inovadores, sublinha a necessidade de as organizações desenvolverem e testarem regularmente os planos de resiliência cibernética. Aproveitar ferramentas de IA pode libertar tempo valioso para que as equipas de segurança se concentrem em melhorias contínuas nos seus programas. Capacitar as equipas com ferramentas e estratégias para realizar mais com recursos limitados continua a ser um desafio crítico.



Quais são as principais ameaças cibernéticas para as empresas?

A sua postura em matéria de cibersegurança não é apenas uma preocupação de TI, mas um aspeto fundamental da sua estratégia de negócios e resiliência. A capacidade de navegar na complexa teia de ameaças cibernéticas já não é uma questão de vantagem competitiva, mas uma obrigação legal e ética. Foram aprovadas leis e regulamentos rigorosos, que obrigam as empresas a manterem-se vigilantes e proativas na proteção dos seus dados, a fim de preservar a sua integridade e manter a confiança e a privacidade dos seus clientes e parceiros.

Para mitigar eficazmente os riscos, as organizações devem identificar e abordar as seguintes ameaças em 2025:

Atores de Estados-nação

Os estados-nação estão entre os grupos mais organizados e capazes no panorama de ameaças cibernéticas. Estes agentes de ameaça investem significativamente em capacidades cibernéticas, tanto ofensivas como defensivas, para obter vantagens geopolíticas. As suas atividades muitas vezes ditam tendências mais amplas em cibersegurança. Com as atuais tensões geopolíticas na Europa de Leste e no Pacífico Ocidental, estes atores continuarão a impulsionar novas tendências em cibersegurança.

No lado ofensivo, os estados-nação desenvolvem plataformas e ferramentas de ataque cibernético que são frequentemente altamente sensíveis e secretas, destinadas a serem usadas de forma furtiva, no momento e no local de sua escolha. Às vezes, esses sistemas são tornados públicos ou expostos e usados deliberadamente por gangues criminosas ou mesmo aproveitados por outros estados-nação.

No lado defensivo, agências governamentais, como a Securities and Exchange Commission (SEC) nos Estados Unidos, estão a apertar as regulamentações de cibersegurança para as empresas, em parte em resposta às sofisticadas ameaças apresentadas pelos estados-nação. Neste caso, os responsáveis pelas empresas são responsabilizados diretamente pelas medidas de cibersegurança nas quais investem ou não.

O papel duplo dos atores de estados-nação na promoção de tecnologias cibernéticas ofensivas e defensivas pode ter um impacto misto nas empresas.

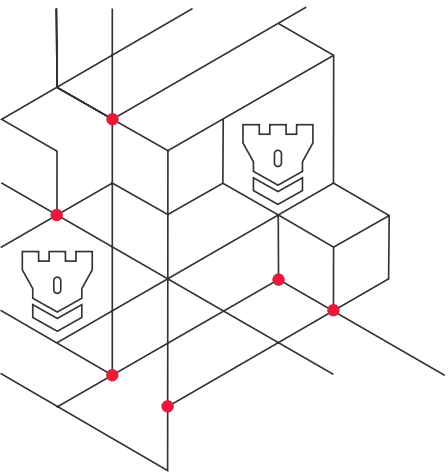
Cibercriminosos

Os grupos de cibercriminosos concentram-se frequentemente no ganho financeiro e variam desde organizações sofisticadas, que às vezes operam com um certo nível de apoio estatal (para agir como proxies), até equipas menos organizadas, mas altamente qualificadas. Além disso, as ferramentas utilizadas pelos atores estatais às vezes acabam nas mãos desses criminosos, seja de forma deliberada ou inadvertida, aumentando ainda mais os riscos.

Hackers Individuais

No outro extremo do espectro, estão os hackers individuais e pequenos grupos, muitas vezes chamados de entusiastas do hacking. Embora os seus motivos variem desde ativismo até ganho financeiro ou notoriedade, apresentam desafios organizacionais diferentes. As tecnologias que permitem o hacking estão a tornar-se mais acessíveis através de plataformas que oferecem "hack-as-a-service", permitindo até mesmo que indivíduos menos experientes representem um risco significativo.

SAIBA MAIS SOBRE AMEAÇAS CIBERNÉTICAS



Compreendendo o panorama de ameaças cibernéticas: Quem são os agentes de ameaça?

No mundo interconectado de hoje, nenhuma organização está completamente segura de ameaças cibernéticas, tornando imperativo para as empresas compreenderem o panorama de ameaças em evolução. Este ecossistema é uma teia complexa de vários agentes, cada um com motivações e capacidades únicas, representando uma variedade de riscos para a integridade financeira e operacional das organizações.

Ciberespionagem

Esta ameaça encoberta envolve o acesso não autorizado a sistemas e redes de computadores com a intenção de reunir informações sensíveis, podendo causar consequências severas. Pode variar desde a destruição de reputações corporativas ou perda de vantagem competitiva até a comprometimento da segurança nacional. Neste contexto, compreender as táticas comuns de ciberespionagem é fundamental para implementar contramedidas eficazes.

Comprometimento de Email Empresarial

Caracterizado pela sua simplicidade enganadora, os ataques por email empresarial envolvem a impersonificação de um indivíduo ou entidade de confiança através da comunicação por email para manipular funcionários, clientes ou consumidores a revelarem informações sensíveis ou a executarem transações financeiras fraudulentas. Isso pode resultar frequentemente em perdas económicas substanciais e danos à reputação.

Credential stuffing

Os agentes de ameaça usam nomes de utilizador e palavras-passe roubados de um site ou serviço para obter acesso a outras contas, explorando indivíduos que utilizam as mesmas credenciais de login em várias plataformas. Esta tática depende da reutilização de palavras-passe, tornando-a um método eficaz para comprometer contas e aceder a informações sensíveis.

Ameaça Interna

De acordo com um relatório recente da Verizon, a ameaça externa média compromete cerca de 200 milhões de registos, enquanto os incidentes envolvendo um agente de ameaça interno resultaram na exposição de 1 mil milhões de registos ou mais. Esta é uma tática significativa de ameaça cibernética em que indivíduos com acesso autorizado aos sistemas e dados de uma organização exploram a sua posição. Estes indivíduos podem ser funcionários, subcontratados ou parceiros de negócios.

Ataques à Supply chain

Nestes ataques, os agentes procuram comprometer fornecedores ou prestadores de serviços de terceiros para aceder aos sistemas ou dados da organização-alvo. Podem, assim, minar a segurança de toda a supply chain, potencialmente levando a violações de dados, compromissos de sistemas ou outras consequências adversas. A mitigação proativa de riscos é essencial para contrariar esta ameaça em múltiplas camadas e em evolução.

Sabotagem Cibernética

Esta campanha envolve atos deliberados para interromper a infraestrutura digital com a intenção de comprometer a integridade, confidencialidade ou reputação da empresa-alvo por razões ideológicas, pessoais ou competitivas. É crucial compreender quais as táticas a observar ao desenvolver estratégias de defesa eficazes contra a sabotagem cibernética. Familiarize-se com as seguintes táticas:

Ransomware

O Microsoft Digital Defence Report 2023 indicou que as organizações enfrentaram uma taxa aumentada de ataques de ransomware em relação ao ano anterior, com o número de ataques de ransomware operados por humanos a subir mais de 200%. O ransomware é caracterizado pela encriptação, ou às vezes pela modificação, de dados críticos para extorquir um resgate das vítimas-alvo. Os cibercriminosos estão cada vez mais a colaborar, a partilhar ferramentas e táticas, e a alargar o seu alcance para visarem organizações de todos os tamanhos. Estes fatores têm contribuído para a frequência e sofisticação crescentes dos incidentes de ransomware, representando um risco significativo para empresas e infraestruturas críticas em todo o mundo.

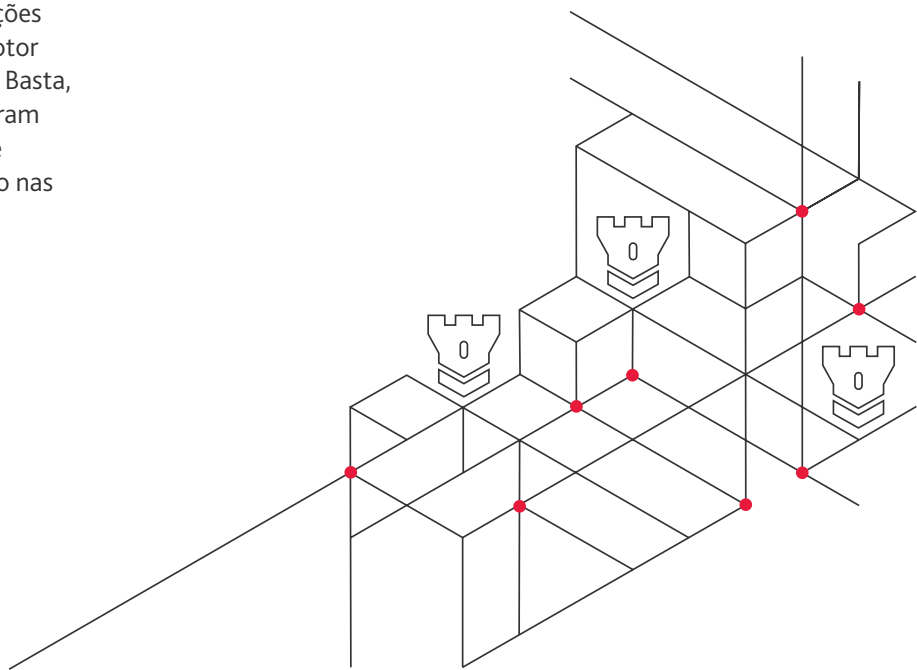
Em outubro de 2023, a Biblioteca Pública de Toronto, a maior rede de bibliotecas do Canadá, foi vítima de um ataque de ransomware. Os cibercriminosos encriptaram os sistemas informáticos da biblioteca e roubaram dados de funcionários, causando uma interrupção generalizada nos serviços. Em maio de 2024, a Ascension, um dos maiores sistemas de saúde sem fins lucrativos nos EUA, foi atingida por um ataque de ransomware que interrompeu operações durante semanas. E em fevereiro, a Hyundai Motor Europe sofreu um ataque de ransomware Black Basta, no qual três terabytes de dados corporativos foram roubados. Estes são apenas alguns exemplos de incidentes que tiveram um impacto significativo nas organizações e nas pessoas em todo o mundo. .

Denial of service

Os ataques de Denial of Service (DoS) visam interromper a disponibilidade de serviços ou websites online, sobrecarregando os seus servidores com um fluxo de tráfego, tornando-os inacessíveis para utilizadores legítimos. Isto envolve tipicamente o uso de vários dispositivos comprometidos ou uma botnet para gerar pedidos ou tráfego excessivo. O principal objetivo não é roubar dados, mas causar interrupções operacionais à organização-alvo.

Sabotagem de Processos

Estes ataques focam-se em processos dependentes de dados que são essenciais para o funcionamento fluido das operações. Ao alterar ou eliminar dados críticos, os ataques tornam os protocolos operacionais ineficazes. Por exemplo, considere uma frota de veículos a operar sob um rigoroso cronograma de manutenção. Se os registos de manutenção forem manipulados ou eliminados, a prontidão dos veículos pode ser comprometida, causando disrupção em toda a cadeia logística.



Fraude Cibernética

Uma ameaça omnipresente e em constante evolução, a fraude cibernética é um termo abrangente para uma vasta gama de atividades ilícitas destinadas ao lucro financeiro ou à comprometimento de dados. As táticas envolvem o uso de emails e técnicas de engenharia social para explorar vulnerabilidades numa organização, muitas vezes levando a consequências prejudiciais. As contramedidas devem incluir protocolos de autenticação robustos, programas de sensibilização para colaboradores e sistemas de monitorização para detetar atividades incomuns.

Exposição de Credenciais

Talvez uma das formas mais elementares de fraude cibernética, a exposição de credenciais manifesta-se frequentemente através de tentativas de phishing por email, chamadas telefónicas ou até mensagens de texto. Normalmente, a narrativa envolve uma necessidade urgente de verificação de conta ou um processo de reembolso. A sensibilização é a primeira linha de defesa neste caso — sabendo, por exemplo, que instituições financeiras legítimas ou entidades governamentais nunca solicitarão informações pessoais através de comunicações não solicitadas.

Assumir o controlo de conta

Account takeover (ATO) ocorre quando um ator malicioso ganha controlo de uma conta legítima (bancária, email, redes sociais) sem a permissão do proprietário. Isto é frequentemente possível ao explorar vulnerabilidades nas medidas de autenticação ou de segurança. A inércia humana em relação às mudanças de palavra-passe favorece os fraudulentos. O ATO pode ser especialmente prejudicial para as organizações onde os perfis de clientes em aplicações externas podem ser monetizados, como em programas de fidelização.

Fraude de Pagamento

Frequentemente interconectada com a fraude de email empresarial, a fraude de pagamento visa iniciar transações financeiras não autorizadas. Normalmente, envolve a impersonação de uma entidade de confiança e a solicitação a um responsável por contas a pagar para alterar os dados bancários de um pagamento pendente. O timing é frequentemente meticulosamente planeado para coincidir com períodos em que a vigilância pode estar reduzida — como o início do fim de semana ou quando a administração está fora do escritório.

Desinformação

Uma forma poderosa de ataque digital, a desinformação envolve a disseminação deliberada de informações falsas ou enganosas com a intenção de enganar, manipular ou causar confusão — é uma ferramenta poderosa usada para manipular a opinião pública e criar agitação. Estas campanhas frequentemente utilizam canais online como redes sociais, emails e websites, sublinhando a importância da literacia mediática, do pensamento crítico e da verificação de factos.

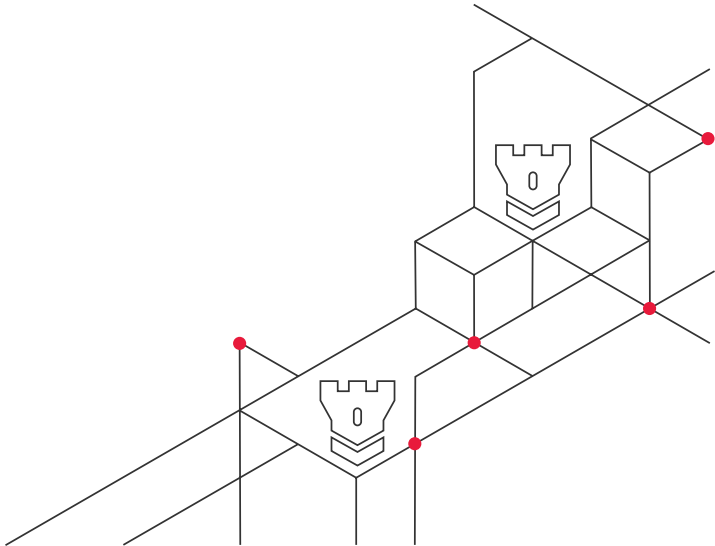
Os impactos da desinformação são vastos, variando desde a perda de confiança e credibilidade pública até danos financeiros ou sociais reais. Combater a desinformação requer uma abordagem multifacetada que envolve vigilância individual e ação coletiva. Usando as capacidades de proteção contra riscos digitais da sua organização, como inteligência sobre ameaças cibernéticas, pode detetar a desinformação precocemente e removê-la para minimizar o seu impacto na marca e no público. Os principais tipos de táticas de desinformação são:

Abuso de Marca

Os defraudadores cibernéticos ou atores maliciosos podem usar a desinformação para manchar a reputação de uma marca. Isto pode variar desde a disseminação de avaliações e informações falsas, a criação de contas falsas em redes sociais que impersonam a marca, ou o estabelecimento de websites fraudulentos que se assemelham a legítimos. Tais táticas podem confundir os clientes, prejudicar a marca e até resultar em perdas financeiras.

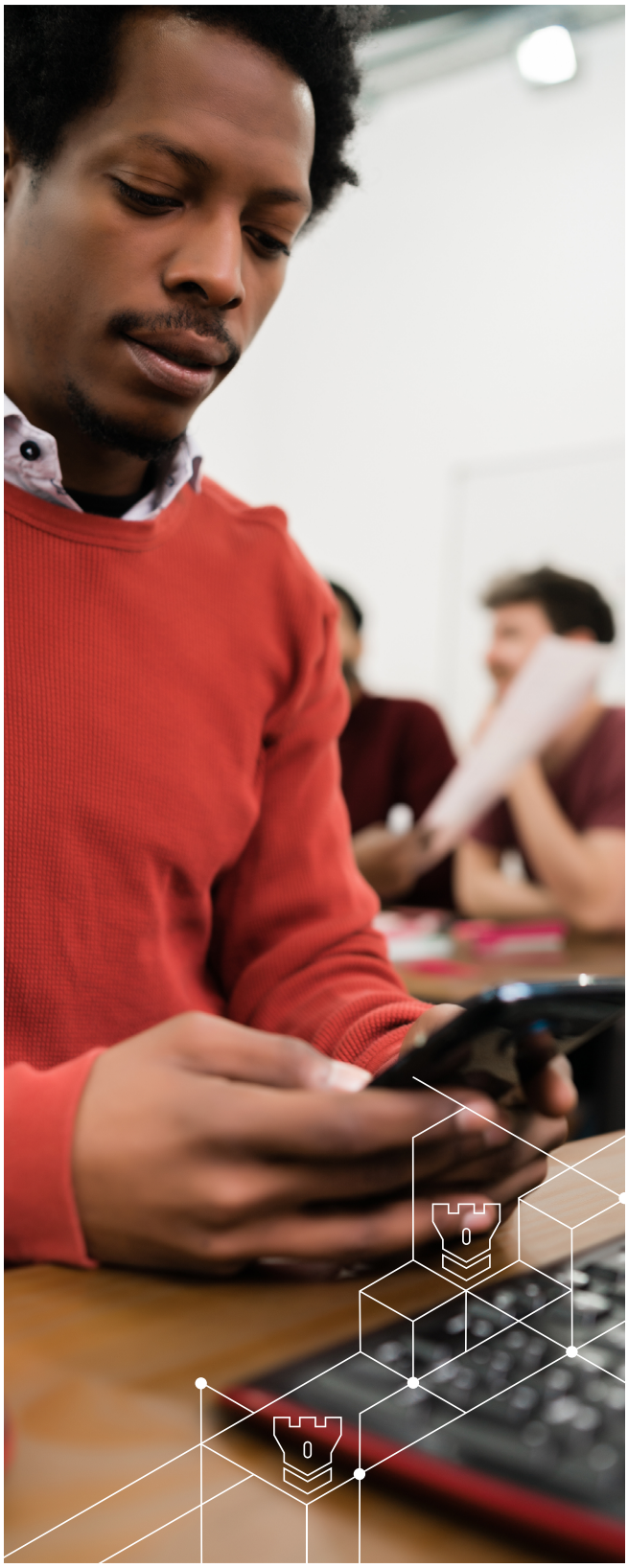
Fraude Eleitoral

A desinformação também pode ser utilizada como uma arma para perturbar o processo democrático. Narrativas falsas ou materiais alterados podem ser distribuídos para enganar os eleitores, minar candidatos ou manipular resultados eleitorais.



Práticas Adicionais de Cibersegurança para Empresas

- A consciência de riscos e a identificação de pontos cegos é o primeiro passo para a proteção. Implemente medidas direcionadas para salvaguardar os ativos digitais da sua organização, identificando vulnerabilidades e potenciais lacunas na sua infraestrutura de segurança.
- Monitorize a sua exposição aproveitando a inteligência para deteção precoce de ameaças, como a vigilância de mercados e fóruns online ilícitos, onde os cibercriminosos frequentemente negoceiam dados roubados.
- Monitorize e faça a gestão dos comportamentos da rede 24/7 para prevenir entradas não autorizadas na sua infraestrutura digital, reduzindo o risco de ameaças cibernéticas e violações de dados.
- Mantenha-se em conformidade com a evolução das regulamentações de privacidade e segurança para evitar repercussões legais e financeiras.
- Realize uma avaliação de continuidade de negócios e resiliência. Avalie a capacidade da sua empresa e dos fornecedores em manter operações durante interrupções, garantindo a continuidade ininterrupta dos negócios face a potenciais ameaças cibernéticas.
- Alinhe os riscos cibernéticos com a sua estratégia global de negócios para ajudar os conselhos de administração e investidores a tomar decisões informadas e a alocar recursos de forma eficaz. Leia o nosso primeiro artigo da série: **Como os conselhos de administração podem aprofundar os seus conhecimentos em cibersegurança: seis estratégias para proteger a sua organização de ameaças cibernéticas.**
- A complexa natureza do panorama de ameaças cibernéticas demonstra que abordar a cibersegurança não é do domínio exclusivo dos departamentos de TI. Em vez disso, é uma responsabilidade partilhada que requer estratégias abrangentes de gestão de riscos que envolvem múltiplas partes interessadas, incluindo os decisores financeiros, como os CFOs.



Como é que a BDO poderá ajudar?

A equipa de cibersegurança da BDO compreende os riscos associados à tecnologia disruptiva e oferece um conjunto abrangente de serviços de cibersegurança projetados para proteger a sua organização. A nossa abordagem inclui uma avaliação exaustiva do nível de maturidade da sua cibersegurança, testes à rede para identificar vulnerabilidades e uma análise abrangente dos riscos. Marque uma consulta com a nossa equipa hoje mesmo para rever a estrutura da sua organização em termos de preocupações de segurança.

A BDO foi reconhecida como vencedora de vários Prémios Microsoft Partner of the Year 2024 e é um dos principais fornecedores de soluções de cibersegurança para empresas. Fornecemos soluções de ponta a ponta, aproveitando as capacidades avançadas de segurança e identidade do Microsoft 365 e do Microsoft Azure Security.

CIBERSEGURANÇA AVANÇADA PARA A SUA ORGANIZAÇÃO

Ricardo Moreira
Digital Director
BDO Portugal