GLOBAL PERSPECTIVES & INSIGHTS

Cibersegurança

PARTE 1: Ciberameaças em um Mundo Aprimorado pela IA

PARTE 2: Assegurando a Resiliência Cibernética

PARTE 3: Estabelecendo um Novo Limite de *Zero Trust*

The Institute of Internal Auditors

PARTE 1

Ciberameaças em um Mundo Aprimorado pela IA

Sobre os Especialistas

Antonio Cacciapuoti, CIA

Antonio Cacciapuoti é o chefe de auditoria interna da Eurizon Capital S.A. Luxembourg, a empresa de gestão de ativos do Grupo Intesa Sanpaolo.

Bradley Niedzielski, CPA

Bradley Niedzielski é sócio de auditoria e avaliação e líder de Transformação Financeira e GenAI na Deloitte & Touche LLP, onde atende empresas públicas e privadas da indústria de serviços financeiros.

Durante o último ano, os avanços na inteligência artificial (IA) fizeram com que as organizações se esforçassem para acompanhar e entender as oportunidades e ameaças que essas tecnologias representam. Como parte desse esforço, as empresas precisam considerar o perigo crescente que a IA pode representar para seus esforços de segurança, especialmente devido à dependência quase total das empresas em relação a informações e transações on-line. Os malfeitores voltaram-se rapidamente para ferramentas aprimoradas por IA para melhorar sua capacidade de romper as defesas cibernéticas das empresas. Este resumo examina como as ameaças cibernéticas mudaram em um mundo impulsionado pela IA e como a auditoria interna pode ajudar as empresas a desenvolver novas abordagens de cibersegurança em resposta a isso.

Uma Evolução no Crime Cibernético

Embora fortes defesas cibernéticas sempre tenham sido essenciais, os malfeitores agora estão usando a IA para aprimorar e ampliar sua capacidade de superar as defesas das organizações. “A IA não é um novo tipo de ciberataque, é uma evolução”, diz Antonio Cacciapuoti, chefe de auditoria interna da Eurizon Capital S.A. Luxembourg. A IA é usada de formas mais avançadas do que os ciberataques tradicionais em termos de velocidade, escala, complexidade e adaptabilidade. Além disso, “como um vírus, ela cria resistência ao longo do tempo, o que a torna mais perigosa”, diz ele.

A IA está sendo usada em ataques que variam de um foco restrito a um ataque amplamente destrutivo. Por exemplo, embora muitos no mundo dos negócios agora usem regularmente documentos gerados por IA para e-mails ou relatórios, malfeitores também usam documentos criados por IA para fins criminosos, diz Bradley Niedzielski, sócio de auditoria e avaliação da Deloitte em Nova York.

Em outra frente, os ataques de phishing visam romper as barreiras de segurança e obter acesso a dados valiosos. Embora o phishing não seja algo novo, o FBI alerta para os ataques de phishing orientados por IA, “caracterizados por sua capacidade de criar mensagens convincentes adaptadas a destinatários específicos e contendo gramática e ortografia devidamente corretas, aumentando a probabilidade de sucesso em enganar e roubar dados”.

O *spear phishing* automatizado, por exemplo, é personalizado para uma pessoa ou um grupo e tem como objetivo roubar informações confidenciais ou obter acesso a um sistema. “A IA pode analisar as redes sociais, os padrões de comunicação e os dados disponíveis sobre um alvo e, em seguida, criar mensagens com maior probabilidade de enganar os destinatários para que revelem informações confidenciais ou cliquem em links maliciosos”, explica Cacciapuoti. Ao mesmo tempo, embora no passado fosse possível confiar em um vídeo ou em uma chamada com base no conhecimento da voz ou das características de uma pessoa, com os *deepfakes* (vídeos simulados de um indivíduo) e o hacking de voz, que replica a voz de uma pessoa, é possível enganar e manipular alvos específicos.

Essas não são as únicas ameaças relacionadas à IA que as organizações enfrentam. O malware com tecnologia de IA pode se adaptar e mudar seu comportamento com base no ambiente-alvo, dificultando a detecção pelo sistema de segurança tradicional, de acordo com Cacciapuoti. “Ele pode escapar facilmente da detecção básica e usar técnicas polimórficas para alterar seu código e até mesmo analisar medidas defensivas para evitá-las”, diz ele. Ainda mais importante, ele pode introduzir dados envenenados em um modelo de aprendizado de máquina de IA usado em um sistema de detecção de fraude, levando a IA a fazer previsões imprecisas e ignorar alguns indicadores de fraude.

Usando a exfiltração inteligente de dados, a IA pode analisar dados e propriedades intelectuais roubados em tempo real e priorizar quais informações são as mais valiosas para exfiltração. Em seguida, ela pode criptografar essas informações e exigir um resgate para liberá-las, diz ele. Os ataques orientados por IA também podem comprometer credenciais que autenticam usuários válidos, permitindo que se movimentem pelo sistema.

Os riscos dos ciberataques orientados por IA são importantes, porque o que está em jogo é muito valioso. O vazamento ou o uso indevido de informações confidenciais poderia prejudicar a posição competitiva de uma organização ou sujeitá-la a penalidades por não cumprir as regulamentações de privacidade de dados. Qualquer violação poderia fazer com que clientes e parceiros de negócios perdessem a confiança na organização. Os ataques de ransomware e malware podem causar a disrupção das operações e o desligamento de sistemas críticos.

Muitos usos seriam inimagináveis até pouco tempo atrás, mas estão ocorrendo em tempo real hoje. Por exemplo, um funcionário de uma empresa multinacional em Hong Kong pagou, sem querer, US$ 25 milhões a fraudadores depois de ser convencido a fazê-lo por uma simulação deepfake do diretor financeiro da empresa em uma chamada de vídeo, de acordo com a CNN.

Em outro lugar, The Drive reporta que um executivo da Ferrari recebeu uma ligação telefônica de um deepfake que alegava ser o CEO da empresa. A tentativa foi frustrada quando o executivo desconfiado fez uma pergunta que somente o CEO poderia responder. Em um caso citado pela Greylock Partners, um espião norte-coreano usou uma identidade falsa para ser contratado por uma empresa de cibersegurança e, em seguida, instalou imediatamente um malware em seus dispositivos corporativos.

A Melhor Defesa

Felizmente, a IA também pode ajudar as organizações a impedir os malfeitores. “Para deter a IA, você precisa usá-la”, diz Cacciapuoti. As organizações precisam adotar medidas mais sofisticadas de cibersegurança com tecnologia de IA para acompanhar a evolução das ameaças. “Se você não tiver um conhecimento profundo da tecnologia que os criminosos estão usando, como poderá detê-los?”, pergunta ele. As organizações deveriam se familiarizar com as ferramentas e estratégias que os criminosos cibernéticos estão usando e entender as diversas formas de ajudar a melhorar a cibersegurança.

A publicação *“The Need for AI-powered Cybersecurity to Tackle AI-driven Attacks,”* da ISACA, identifica várias formas pelas quais as tecnologias avançadas podem ajudar a prevenir ataques:

Formas de Prevenir Ataques

- Análise de vastos conjuntos de dados, para determinar como os recursos organizacionais são usados, identificar áreas expostas, criar um inventário de ativos e identificar tendências de tráfego de rede e atividades/comportamentos de usuários.
- Detecção de anomalias, incluindo “logins incomuns, solicitações de acesso de uma nova localização geográfica ou endereço IP, acesso de novos usuários, alteração de permissões em arquivos e outros recursos, extração ou exclusão de grandes volumes de arquivos e um aumento exponencial no tráfego”.
- Uso da IA para proativamente banir, desconectar ou bloquear suspeitos de serem malfeitores e alertar os administradores do sistema sobre suas atividades.
- Monitoramento contínuo dos sistemas, para permitir respostas rápidas.
- Uso da análise preditiva para antecipar potenciais ameaças à segurança e tomar medidas para evitá-las.
- Detecção e prevenção de ameaças de dia zero, ou vulnerabilidades novas e invisíveis.
- Redução do número de falsos positivos quanto a potenciais ameaças.
- Automação de avaliações de segurança, para agilizar respostas e minimizar erros humanos.
- Expansão para se adaptar a novos acontecimentos e ambientes, para fornecer proteção contínua.

As organizações podem alavancar a IA para agregar, analisar e correlacionar dados de diversas fontes, a fim de criar insights mais profundos, diz Cacciapuoti. Elas também podem usar o processamento de linguagem natural (PLN) para analisar grandes volumes de dados textuais. Por exemplo, quando for solicitado aos auditores internos que analisem contratos, o PNL pode extrair dados textuais importantes para o sistema analisar.

Abordando Considerações sobre a IA

Como uma organização nunca pode abordar 100% dos riscos, Niedzielski recomenda começar pela avaliação estratégica das ameaças em diferentes áreas da empresa. Isso incluirá a identificação de possíveis vetores de fraude de IA e a avaliação da probabilidade de serem atacados e da magnitude e do impacto potenciais. O próximo passo, segundo ele, é determinar a eficácia dos controles existentes.

Como parte desse esforço, Niedzielski recomenda usar os recursos emergentes da IA generativa, como raciocínio avançado e reconhecimento de padrões, para reconhecer táticas comuns, como tentativas de phishing geradas por IA e deepfakes. Algumas empresas usam protocolos e tecnologias para verificar se uma chamada foi feita de um número interno ou externo.

“Essas tecnologias avançadas podem ajudar a minimizar o risco associado”, diz ele. Em alguns casos, no entanto, como para determinar imediatamente se um chamador ou participante de uma reunião é um deepfake, os funcionários podem ter que confiar em suas intuições ou estar prontos para questionar por que um CEO está ligando e pedindo uma transferência de fundos, por exemplo. Nessas situações, os funcionários deveriam ser encorajados a confiar em seus instintos e ligar de volta para a pessoa pelo número da empresa ou, se o suposto interlocutor estiver no mesmo escritório, simplesmente andar até sua mesa para confirmar quem é.

Uma equipe multidisciplinar composta por profissionais de áreas como auditoria interna, gerenciamento de riscos, TI, cibersegurança e outras funções relevantes pode monitorar os avanços da IA e fornecer atualizações continuamente sobre o gerenciamento de riscos, protocolos de segurança e sistemas de detecção de fraudes. A equipe pode trabalhar em conjunto para identificar e responder aos esforços, considerando questões como quais controles evitarão ou limitarão melhor os danos, diz Niedzielski.

Ele também recomenda que as empresas compartilhem regularmente suas experiências e discutam as vulnerabilidades de IA que outras empresas enfrentaram. “Não apenas os esforços bem-sucedidos, mas também os momentos em que algo deu errado e como a empresa aprendeu com isso”, orienta. “O compartilhamento de conhecimento, o treinamento e as devidas avaliações de riscos permitirão minimizar o risco de fraude induzida por IA.”

Nesse ambiente, o treinamento deveria ser uma prioridade máxima para aumentar a conscientização dos funcionários sobre potenciais atividades suspeitas e, ao mesmo tempo, reforçar as medidas apropriadas para remediar as violações, diz Niedzielski. Cacciapuoti observa que também é possível usar simulações de IA para fornecer treinamento em cibersegurança em tempo real para situações do mundo real. A IA pode analisar o comportamento individual dos funcionários no treinamento cibernético e fornecer insights para melhorias.

A Contribuição da Auditoria Interna

A auditoria interna pode ajudar a garantir que os esforços da organização se adequem aos desafios da IA, diz Cacciapuoti, incluindo alavancar seu potencial e, ao mesmo tempo, mitigar o risco. “A auditoria interna deveria realizar uma avaliação de riscos abrangente, auditando os sistemas de IA quanto à segurança, ética e conformidade e apoiando a inovação segura”, diz ele. “Ela pode participar da formação de uma estratégia cibernética que seja robusta o suficiente para lidar com as ameaças de IA.”

Além disso, embora a auditoria interna seja tipicamente uma linha de defesa essencial, Cacciapuoti diz que ela também deveria servir como uma linha de ataque no que diz respeito à IA, adotando uma abordagem dinâmica no gerenciamento de riscos.

> “A IA nunca substituirá os auditores internos, mas pode ser um assistente poderoso.”
>
> **— Antonio Cacciapuoti, CIA**

“Por que esperar que o risco chegue quando você pode atacá-lo de frente?”, pergunta ele. Isso significa estar na vanguarda do uso de novas tecnologias, para que a organização possa maximizar as oportunidades e, ao mesmo tempo, assegurar os devidos controles de governança e melhoria contínua.

Dentro da função de auditoria interna, “a IA nunca substituirá os auditores internos, mas pode ser um assistente poderoso”, de acordo com Cacciapuoti. Ele diz que a auditoria interna pode se beneficiar do uso da IA para:

- Analisar grandes volumes de dados e expandir amostras em testes, para que fiquem muito próximas do tamanho total da população.
- Automatizar procedimentos de teste e monitorar controles principais, assumindo tarefas repetitivas, para que os profissionais de auditoria interna possam se concentrar em tarefas de nível superior.
- Usar algoritmos de IA para monitorar os dados continuamente, em vez de depender de auditorias periódicas, identificando e abordando atividades incomuns muito mais cedo.
- Usar a análise preditiva para projetar resultados futuros e tomar decisões e recomendações mais informadas.
- Resumir rapidamente os papéis de trabalho, para que os auditores internos possam usá-los na elaboração dos relatórios finais.

A IA permite uma gestão mais uniforme e eficiente das constatações em todas as funções de controle. “Em uma empresa muito grande, há muitos trabalhos de auditoria de várias funções a serem considerados”, diz Cacciapuoti. A IA permite que os auditores internos reúnam os dados de forma uniforme, para evitar duplicação.

Para mitigar os riscos e alavancar o valor, Niedzielski recomenda que os auditores internos atualizem continuamente seus conhecimentos sobre os avanços tecnológicos. “Há algo novo todo dia”, diz. Eles deveriam se concentrar na identificação de respostas proativas — em vez de reativas — aos riscos potenciais. Enquanto o mundo tenta aproveitar as novas tecnologias, os auditores internos também deveriam se concentrar na governança e na conformidade com novos regulamentos e normas éticas, para proteger a integridade organizacional, diz ele.

Ciberameaças Viabilizadas pela IA: Fatos Rápidos

- 97% dos profissionais de segurança estão preocupados com a possibilidade de sua organização sofrer um incidente de cibersegurança gerado por IA, pois a IA continua a causar esgotamento.
- 75% dos profissionais de segurança tiveram que mudar sua estratégia de cibersegurança no último ano, devido ao aumento das ciberameaças viabilizadas pela IA.
- 73% das equipes de segurança querem se concentrar mais nas suas capacidades de prevenção.
- 61% das organizações registraram um aumento nos incidentes de deepfake no ano passado.
- 75% desses ataques se fizeram passar pelo CEO de uma organização ou por outro membro da gestão executiva.

Fonte: *GenAI in Cybersecurity: Friend or Foe? Voice of SECOPS*, 5ª Edição, 2024.

“Os auditores internos deveriam se colocar no lugar de um malfeitor”, de acordo com Niedzielski. "Não pergunte como um malfeitor se infiltraria na organização, pergunte o que você faria se fosse um malfeitor, com base no que você sabe sobre a organização. Considere não apenas uma perspectiva quantitativa, mas também qualitativa da organização."

Os auditores internos não deveriam tentar fazer isso sozinhos, diz Cacciapuoti, que recomenda a coordenação com todos os prestadores de avaliação e stakeholders para prevenir e mitigar riscos, incluindo aqueles nas funções de controle, conformidade, gerenciamento de riscos, auditores externos e órgãos regulatórios. “A colaboração entre ferramentas de IA e profissionais de cibersegurança, juntamente com um framework sólido de governança, é essencial para navegar nesse cenário e responder a riscos novos e emergentes”, diz ele.

PARTE 2

Assegurando a Resiliência Cibernética

Sobre os Especialistas

DC Chang, CPA, CDPSE, CISSP, CRISC, CISA

DC Chang é diretor de auditoria, Tecnologia Digital e Cibersegurança da United Airlines em Dallas, Texas.

Michael Echols, CISSP

Michael Echols é CEO da Max Cybersecurity LLC em Washington, DC.

Justin Headley, CPA, CISSP, CISA, CRISC

Justin Headley é gerente sênior do grupo de serviços de consultoria e avaliação de riscos da Warren Averett em Birmingham, Alabama.

Mesmo enquanto as organizações trabalham para assegurar que tenham as ferramentas adequadas para evitar ciberataques, é quase certo que elas sofrerão violações ou incursões de alguma forma. Com isso em mente, as empresas também devem se concentrar em sua capacidade de responder e se recuperar rapidamente de um ciberataque. Este artigo discute a melhor forma de entender e instilar a resiliência aos ataques e descreve o papel do auditor interno no fortalecimento da resposta de uma organização.

Preparando o Terreno para a Recuperação

Em sua melhor forma, a resiliência cibernética não é apenas uma reação a uma situação terrível. É um conjunto contínuo de práticas — planejamento, processos, análise, treinamento, serviços críticos e gestão — que asseguram que uma organização possa manter suas operações, de acordo com Michael Echols, CEO da Max Cybersecurity LLC. Essas práticas possibilitam a restauração ou a manutenção das funções organizacionais após um ataque, mas devem ser implementadas muito antes da ocorrência de um problema.

Por exemplo, Echols atendeu um escritório de advocacia que recebia todas as indicações por meio de seu site. Tipicamente, a empresa recebia muitas indicações diariamente, mas, em um determinado momento, passaram-se dois ou três dias até que o escritório notasse que não estava recebendo indicações e, por fim, percebesse que havia sido hackeado. “A empresa já deveria ter tido um processo de monitoramento contínuo e algum tipo de notificação” sobre uma queda incomum nas indicações da Web, pois elas eram a principal fonte de negócios da empresa (uma função crítica), diz ele.

Os problemas a serem identificados — como uma queda no tráfego da Web — serão diferentes para cada empresa e provavelmente haverá mais de um. Em muitos casos, as organizações devem estar preparadas para um incidente que afete seu fornecimento de energia, por exemplo, com passos para implantar geradores independentes da empresa principal, para que não sejam afetados pelo ataque, diz Echols.

> A resiliência cibernética é “a capacidade de prever, resistir, recuperar-se e adaptar-se a condições adversas, estresses, ataques ou danos a sistemas que usam ou são habilitados por recursos cibernéticos. A resiliência cibernética destina-se a permitir que os objetivos de missão ou de negócios que dependem de recursos cibernéticos sejam concretizados em um ambiente cibernético contestado."
>
> **— *National Institute of Standards and Technology* dos EUA**

Para se preparar para o que está por vir, é necessário contextualizar o ambiente atual de cibersegurança, de acordo com DC Chang, diretor de auditoria de Tecnologia Digital e Cibersegurança da United Airlines. Há vinte anos, as organizações tinham seus próprios data centers e a cibersegurança era, até certo ponto, uma questão de trancar os servidores atrás de portas e janelas físicas. Hoje, os dados são armazenados em um ambiente virtual, que pode ser vulnerável a agentes mal-intencionados do mundo todo.

“Há milhares e milhares de janelas e portas que precisamos controlar agora que somos digitais, e elas são adicionadas e removidas diariamente”, diz Chang. As organizações precisam estar conscientes do ritmo e do escopo da aceleração digital, para desenvolver a resiliência de que precisarão em uma crise.

Governança e Cultura

A governança tem um papel fundamental na construção da resiliência cibernética, de acordo com Justin Headley, gerente sênior do Grupo de Serviços de Consultoria e Avaliação de Riscos da Warren Averett. “Ouvimos constantemente que os funcionários são o ponto fraco, porque usam uma senha fraca ou clicam em links suspeitos”, diz ele. “Mas se os líderes não estiverem comprometidos, não se pode esperar que os funcionários façam sua parte.”

De muitas formas, a cibersegurança não é inteiramente uma questão tecnológica, mas uma preocupação cultural. “Se você mudar a mentalidade de 90% das pessoas na organização e *uma* pessoa abrir um link em um e-mail, isso poderia afundar a empresa”, diz Echols. Uma cultura consciente da cibersegurança esclarece as expectativas da organização e tranquiliza os consumidores e parceiros comerciais. “Os bancos foram um dos primeiros grupos a desenvolver resiliência cibernética”, diz ele, porque dependem da confiança de seus stakeholders.

Headley recomenda que os líderes promovam uma cultura de cibersegurança que vá além das abordagens comuns, como e-mails trimestrais com dicas de cibersegurança ou treinamento anual rudimentar de segurança. Os passos que a empresa dele segue incluem o envio de seus próprios e-mails falsos de phishing para os funcionários e, em seguida, treinamento para aqueles que clicam nos links suspeitos incorporados. “É preciso mostrar como a governança cibernética funciona na prática, não apenas na teoria”, diz ele.

Os líderes também podem fornecer passos específicos a serem seguidos em um ataque. “Uma organização pode interromper um ataque e se recuperar, se houver políticas e procedimentos práticos e repetíveis a serem seguidos em uma violação”, de acordo com Headley. Se os líderes estiverem envolvidos quando esses passos forem testados e participarem da resolução dos problemas, eles demonstrarão seu comprometimento com o esforço, o que pode desempenhar um papel importante no sucesso da estratégia de cibersegurança.

- 68% das violações envolveram um elemento humano não malicioso, como alguém que caiu em um ataque de engenharia social ou cometeu um erro.
- O tempo mediano para os usuários serem enganados por e-mails de phishing foi de menos de 60 segundos.
- 15% das violações envolveram um terceiro ou fornecedor, incluindo cadeias de suprimentos de software, infraestruturas de parceiros de hospedagem ou custodiantes de dados.

Fonte: Relatório *Verizon Business Data Breach Investigations* de 2024

O Impacto da Regulamentação

De acordo com a versão final de *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, a Comissão de Valores Mobiliários dos EUA aumentou as expectativas das organizações ao exigir que as empresas de capital aberto divulguem incidentes materiais de cibersegurança e façam divulgações periódicas sobre como avaliam, identificam e gerenciam os riscos cibernéticos. O regulamento “destaca uma questão importante que todas as entidades do planeta precisam considerar”, diz Chang.

Entre outros requisitos, o regulamento obriga as organizações a assegurar que suas práticas cibernéticas sejam operacionais, diz Headley. Ele observa que a função de TI geralmente opera em um silo, com a confiança implícita de líderes que talvez não compreendam totalmente seu funcionamento. “Isso terá que mudar”, diz ele. Será necessário um entendimento em toda a organização sobre como tratar dados internos e de clientes e abordar preocupações cibernéticas.

Como acontece com muitos regulamentos, “tudo se resumirá à transparência”, diz Echols. “Quando há uma violação material, a empresa deve ter um processo claro de como reagir a essa violação.”

Adicionando a IA à Equação

A inteligência artificial (IA) pode ser uma ferramenta inestimável para melhorar a prevenção de problemas cibernéticos e a resiliência após um ataque. Tecnologias como firewalls de última geração e sistemas de proteção de pontos estão facilitando a classificação do tráfego de dados e a descoberta de anomalias que deveriam ser investigadas, diz Headley. “O uso da IA tem sido um divisor de águas nos últimos anos e continuará ajudando as empresas a melhorar a detecção e a resposta a ataques.”

A IA também pode ser usada como uma arma contra as organizações. “Se você tiver vulnerabilidades que foram ignoradas, a IA ajudará os hackers a encontrá-las”, diz Echols.

Entre outras considerações, as organizações terão que equilibrar o impulso de obter maior eficiência com as novas ferramentas e a necessidade de proteger a segurança e a privacidade, de acordo com Headley. As novas tecnologias ajudam as organizações a eliminar tarefas repetitivas, que geralmente envolvem alimentar os programas com informações confidenciais. Ao mesmo tempo, “continuamos a ver ataques direcionados a essas tecnologias, porque os malfeitores sabem que as pessoas não entendem totalmente a tecnologia”, o que pode tornar especialmente vulneráveis os dados confidenciais contidos nos programas.

Ao desenvolver a resiliência, as organizações terão que treinar sua equipe sobre tecnologias em evolução e assegurar que o uso da tecnologia corresponda ao apetite a risco da organização. “Uma empresa poderia ter as melhores tecnologias e habilidades, mas um usuário ainda pode, sem saber ou às vezes conscientemente, vazar dados pela porta da frente usando uma ferramenta de GenAI”, diz Headley.

As organizações também deveriam ter o cuidado de não negligenciar as abordagens tradicionais de ciberataque. Muitos problemas cibernéticos são causados por questões que não são novas, como configurações incorretas ou falha em seguir uma prática estabelecida, diz Echols. Muitas violações estão relacionadas a vulnerabilidades conhecidas que nunca foram corrigidas ou a patches que não foram instalados, diz ele. Como resultado, educar os usuários finais sobre ameaças novas e existentes é especialmente importante. “Os auditores devem olhar por baixo do capô e fazer as perguntas certas aos clientes para descobrir vulnerabilidades ocultas criadas pela apatia”, diz ele.

> "Os stakeholders, principalmente o conselho e a alta administração de uma organização, contam com serviços de avaliação independentes, objetivos e competentes para verificar se os controles de resposta e recuperação de incidentes cibernéticos foram bem elaborados e implementados com eficácia e eficiência. A função de auditoria interna agrega valor à organização quando fornece esses serviços em conformidade com as Normas e com referências a frameworks de controle amplamente aceitos, especialmente aqueles expressamente usados pelas funções de tecnologia da informação e segurança da informação da organização.”
>
> **Fonte: *Global Technology Audit Guide: Auditing Cyber Incident Response and Recovery*, 2ª Edição, Guia Prático Global, The Institute of Internal Auditors, 2024**

Como a Auditoria Interna Pode Ajudar a Aumentar a Resiliência

Nesse ambiente, a auditoria interna deveria estar preparada para formular os resultados de suas auditorias para aumentar a resiliência e identificar vulnerabilidades de forma a ajudar os clientes a entender as potenciais consequências da cibersegurança negligente, diz Echols. Embora os clientes possam presumir que o pior nunca poderia lhes acontecer, os auditores internos devem ser capazes de suspender a descrença, o que os capacitará melhor a imaginar o inimaginável. Por exemplo, Echols tinha um cliente que tinha uma prática recomendada que proibia o uso de endereços de e-mail corporativos em contas de redes sociais, mas não era uma política oficial. O erro dessa abordagem ficou claro quando a MGM sofreu uma grande violação de dados significativa no fim do ano passado. A investigação da violação reportada revelou que um funcionário estava usando seu e-mail de trabalho em uma plataforma de rede social. Os hackers encontraram as informações do funcionário no LinkedIn e se fizeram passar por ele em uma chamada para o helpdesk de TI da MGM, obtendo assim credenciais para acessar e infectar os sistemas da MGM. “As práticas recomendadas são derivadas das experiências de muitos e deveriam ser transformadas em políticas, quando possível”, diz Echols.

Os auditores internos também devem entender que o aspecto de conformidade da auditoria é apenas o primeiro passo para ajudar a construir a resiliência cibernética. “Conformidade não é segurança”, diz Echols. Os auditores internos deveriam se concentrar em traduzir suas constatações em insights melhores, que a equipe do cliente possa usar para melhorar a segurança, e em fazer perguntas que a equipe talvez ainda não seja capaz de responder.

“Você deveria ser capaz de instruir o cliente de que não buscar e encontrar a resposta para essa pergunta, na verdade, cria uma vulnerabilidade”, de acordo com Echols.

Entre as auditorias, a auditoria interna deveria manter as linhas de comunicação abertas, agendando horários para verificar e aprender sobre os desafios das equipes. “Quando os auditores internos são capazes de se posicionar como conselheiros confiáveis, isso muda completamente o jogo”, diz Headley.

A transparência é crucial. Os auditores internos deveriam ser claros sobre o escopo e os procedimentos de teste planejados, bem como sobre as questões que surgiram. “Certifique-se de se comunicar cedo e com frequência”, diz ele, “especialmente quando riscos de TI estiverem envolvidos.” Ele orienta que os auditores internos evitem julgar imediatamente, mas que, em vez disso, tenham uma conversa aberta sobre os processos de raciocínio da equipe do cliente e encorajem a colaboração.

Headley observa que as equipes de TI geralmente ficam atoladas em atender às demandas de diversas linhas de negócios, assumindo a responsabilidade por tudo, desde manter os aplicativos em funcionamento até lidar com falhas diárias de hardware. Como resultado, a cibersegurança pode nem sempre ser uma prioridade máxima. Os auditores internos podem promover a conscientização sobre esses desafios e educar as equipes sobre as oportunidades de abordá-los, assegurando, assim, que as auditorias sejam um verdadeiro exercício de valor agregado.

“Os auditores internos podem ser parceiros no fortalecimento da resiliência corporativa”, diz Headley. Entre outros passos, eles podem ajudar a suavizar quaisquer desconexões entre os líderes da empresa e as equipes de TI, que geralmente não falam a mesma língua. Como os auditores internos entendem tanto o risco comercial quanto o risco de TI, eles podem ajudar a preencher essa lacuna.

Os auditores internos também podem moldar a compreensão dos riscos cibernéticos e a solução de problemas relacionados de uma forma que se afaste da prática passada, diz Chang. Conforme as organizações se afastam do planejamento tradicional de continuidade de negócios ou da recuperação de desastres de negócios, os auditores internos podem ajudá-las a adotar abordagens mais multifacetadas e diferenciadas. Eles podem aprimorar esse esforço, assumindo o papel de contadores de histórias que processam informações e pontos de dados desconectados e os reúnem em uma narrativa convincente, que impulsiona uma melhor tomada de decisão.

Equilibrando as Probabilidades

No fim, resiliência significa aceitar a inevitabilidade do ataque e assumir que as paredes externas da organização não são impenetráveis, observa Echols. Como parte desse esforço, as organizações devem reconhecer que estão em uma luta injusta. Enquanto as organizações se esforçam para bloquear 100% dos ataques que enfrentam, os hackers só precisam abrir uma porta para causar estragos, observa Chang. “É muito mais difícil ser o defensor do que o agressor”, diz ele. A auditoria interna pode fornecer os insights e as informações de que suas empresas precisam para aumentar suas chances de sucesso na cibersegurança.

De acordo com uma pesquisa com tomadores de decisão de operações de TI e segurança:

- Apenas 2% dos entrevistados afirmam que conseguiriam recuperar seus dados e restaurar os processos de negócios em 24 horas após um ciberataque.
- 69% afirmam que sua organização pagou um resgate no último ano, embora 77% afirmem ter uma política ou um protocolo definido contra o pagamento de resgates.
- 42% dizem que suas organizações conseguiriam identificar dados confidenciais e cumprir as leis e regulamentações aplicáveis de privacidade de dados. Outras não têm os recursos devidos de TI e segurança para fazer as duas coisas.

Fonte: Relatório *Cohesity Global Cyber Resilience* de 2024

PARTE 3

Estabelecendo um Novo Limite de *Zero Trust*

Sobre os Especialistas

Adam Kohnke

Adam Kohnke, que mora em Madison, Wisconsin, é gerente de segurança da informação da empresa de fabricação de produtos químicos Charter Next Generation.

Julio Tirado

Julio Tirado é vice-presidente executivo e diretor de Auditoria Interna e Conformidade do SpiritBank, com sede em Tulsa, Oklahoma.

Deveria ser um requisito básico para todas as organizações ter processos e controles em vigor para manter suas redes seguras. No entanto, como a tecnologia avançou e as redes se tornaram maiores e quase inimaginavelmente complexas, a norma do que constitui uma rede segura mudou. Uma das mudanças mais importantes está na transição de um modelo de segurança centrado no local para um modelo mais centrado nos dados. Chamamos esse modelo de *"Zero Trust"* ("confiança zero").

O que é *Zero Trust?*

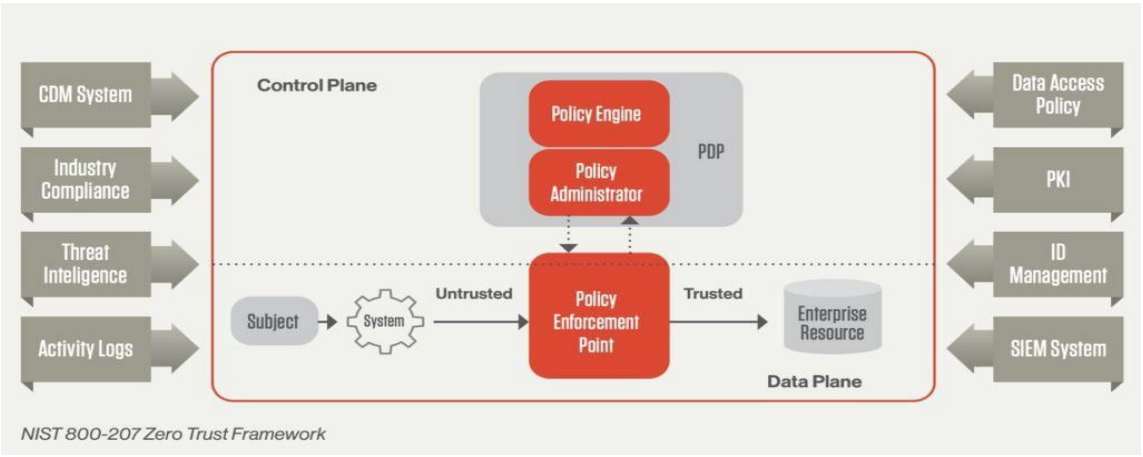
Geralmente, um framework de segurança Zero Trust exige que todos os usuários que operam em uma rede — tanto dentro quanto fora da própria organização — sejam autenticados antes de acessar aplicativos e dados e, em seguida, continuamente validados com regularidade. Como o nome indica, "confiança" ou, mais especificamente, "confie, mas verifique", não desempenha qualquer função nesse sistema, e o acesso a qualquer coisa relacionada à empresa deve ser continuamente justificado e avaliado com base nas políticas da organização.

Tradicionalmente, os modelos cibernéticos eram criados com base na localização da rede, mas em um sistema Zero Trust, o que constitui uma "rede" é menos estritamente definido, pois uma rede organizacional pode ser local, baseada em uma nuvem ou um híbrido dos dois. Especialmente após a pandemia da COVID-19, que deu início a uma nova era de trabalho remoto, os sistemas híbridos ou totalmente baseados na nuvem se tornaram a norma, e os frameworks de cibersegurança tiveram que evoluir para dar conta disso.

Há diversos frameworks formais de Zero Trust, incluindo:

- Standard 800-207, do *National Institute of Standards and Technology* (NIST). Esse é o framework obrigatório para uso pelas agências federais dos EUA desde 2021 (veja a Figura 1).
- Google BeyondCorp.
- Microsoft Zero Trust Strategy.
- Zero Trust Maturity Model, da *Cybersecurity and Infrastructure Security Agency* (CISA).

Figura 1



Fonte: Zero Trust Networks | NIST

Embora todos tenham seus atributos exclusivos, cada um deles compartilha os mesmos princípios básicos:

- Verificar continuamente o acesso a todos os recursos.
- Minimizar a área de impacto no caso de uma violação externa ou interna.
- Usar dados comportamentais para obter o contexto da infraestrutura de TI.

Embora a transição para esse sistema possa parecer substancial, é importante observar que ele não se destina a substituir os sistemas atuais. “A segurança Zero Trust não busca substituir totalmente os modelos atuais de proteção de rede, ou mesmo as mudanças de infraestrutura”, diz Adam Kohnke, gerente de segurança da informação da empresa de fabricação de produtos químicos Charter Next Generation, “mas sim aumentá-los para melhorar a proteção da rede. O objetivo é ser uma extensão, porque os sistemas tradicionais, como firewalls, proxies da Web e mecanismos de isolamento de limites, não estavam funcionando.”

De acordo com a IBM, o custo médio de uma única violação de dados em 2024 foi de US$ 4,88 milhões. Além disso, o ciclo de vida médio de uma violação foi de 292 dias, desde a identificação até a contenção. Claramente, a proteção de rede tradicional não tem sido suficiente e requer atenção significativa.

O Papel da Auditoria Interna

Embora os detalhes possam variar, os auditores internos podem ter uma variedade de responsabilidades associadas à implementação e à manutenção de um sistema Zero Trust. Para ilustrar, aqui estão as áreas em que uma avaliação de auditoria interna pode ter mais valor.

Definindo as Superfícies de Proteção

Tradicionalmente, um sistema de cibersegurança concentrava seus esforços em definir quais eram os parâmetros de segurança em torno de uma rede corporativa. Os firewalls e os sistemas VPN são criados com base nesse conceito, mantendo os dados confidenciais e as informações vulneráveis o mais longe possível do perímetro da rede. Em um sistema Zero Trust, no entanto, em vez de parâmetros, o foco está nos agrupamentos de dados, aplicativos, ativos e serviços (DAAS), conhecidos coletivamente como “superfícies de proteção”. Garantir que essas superfícies sejam devidamente identificadas deve ser o ponto central de uma avaliação abrangente de auditoria interna.

De acordo com Julio Tirado, vice-presidente executivo e diretor de Auditoria Interna e Conformidade do SpiritBank, “a avaliação deveria se concentrar na inspeção das políticas de classificação de dados da organização, para determinar se os sistemas e os dados estão devidamente classificados e se as políticas de proteção em vigor para cada um deles são apropriadas”.

Os serviços protegidos também não se limitam aos dados, diz Tirado. Os ativos físicos que desempenham um papel no acesso a dados confidenciais também devem ter processos e procedimentos implementados, para assegurar que sejam inventariados e avaliados periodicamente.

> A avaliação deveria se concentrar na inspeção das políticas de classificação de dados da organização, para determinar se os sistemas e os dados estão devidamente classificados e se as políticas de proteção em vigor para cada um deles são apropriadas.
>
> **— Julio Tirado, SpiritBank**

Verificando os Fluxos do Mapa de Transações

Uma vez que haja garantia de que as superfícies de proteção foram identificadas, o próximo passo no processo de avaliação é assegurar que haja entendimento dos stakeholders sobre como todos esses sistemas DAAS interagem entre si. As equipes de TI deveriam ter diagramas de documentação detalhados, dedicados a mapear a complexa rede de portas, linhas de base de tráfego de rede e protocolos que descrevem coletivamente como esses sistemas acessam uns aos outros e aonde seu uso pode levar.

Embora, na maioria das organizações, a função de auditoria interna possa não ter o conhecimento ou experiência suficiente para verificar a precisão desses diagramas por conta própria, Kohnke diz que a auditoria interna pode trabalhar com os stakeholders ou com terceiros confiáveis para verificar se testes de validação são conduzidos, para assegurar que o que está representado é suficiente. “O que é importante”, diz ele, “é que o DAAS relevante seja contabilizado em cada diagrama e se há detalhes suficientes... e se as políticas de segurança iniciais definidas nos passos anteriores foram modificadas ou exigem controles adicionais.”

Verificando a Criação e a Melhoria Contínua das Políticas de Zero Trust

As políticas de Zero Trust deveriam ser detalhadas para cada superfície de proteção e responder a perguntas críticas, como:

- Quem deveria ter permissão para acessar os sistemas DAAS corporativos?
- Quais aplicativos terão permissão para acessar os sistemas DAAS corporativos?
- Quando deveria ocorrer ou estar ocorrendo o acesso aos sistemas DAAS corporativos?
- Onde estão localizados os sistemas DAAS corporativos?
- Por que os sistemas DAAS corporativos precisam ser acessados?
- Como deveria ser concedido o acesso aos sistemas DAAS corporativos?

Para avaliar a relevância e a validade das políticas de Zero Trust criadas, a interação contínua com os stakeholders de TI é fundamental, pois a rede corporativa continua se expandindo e evoluindo. “A política de Zero Trust não é um destino”, diz Tirado, “portanto, a política de segurança e os requisitos de proteção do DAAS deveriam evoluir à medida que o processo se desenvolve.”

O objetivo, diz Tirado, deveria ser ter uma política em constante aprimoramento dedicada a abordar todos os tipos de tráfego que poderiam entrar, sair e atravessar uma rede. “Não deveria haver nada em uma rede cuja fonte ou propósito não possa ser identificado”, diz ele. “O auditor interno, em sua avaliação, precisa determinar se revisões são conduzidas, se têm extensão suficiente e se as políticas em vigor abordam com precisão o que as revisões encontram.”

> Monitoramento deveria ser concretizado em suas redes para mensurar o desempenho, identificar todos os dispositivos conectados à sua rede e detectar dispositivos desonestos e atividades maliciosas
>
> **— National Cyber Security Centre**

Monitoramento da Arquitetura Zero Trust

Como os exemplos anteriores indicam, o monitoramento contínuo é essencial para o sucesso de um framework de Zero Trust. Ao contrário de um sistema tradicional, em que o monitoramento se concentraria em parâmetros de segurança, os sistemas de monitoramento de um sistema Zero Trust se concentrarão em usuários, dispositivos e serviços. “Monitoramento deveria ser concretizado em suas redes para mensurar o desempenho, identificar todos os dispositivos conectados à sua rede e detectar dispositivos desonestos e atividades maliciosas”, diz o *National Cyber Security Centre* em sua orientação sobre segurança Zero Trust. Isso é especialmente verdadeiro se você estiver hospedando serviços no local, mas, como se tornou mais comum, a gestão de dispositivos móveis deveria ser considerada na mesma proporção.

“Empresas como a minha implementarão um software de gestão de dispositivos móveis que fornecerá uma medida de controle para aquele dispositivo em especial, desde que o usuário o aceite”, diz Tirado. “Ele monitorará a atividade, ajudará a restringir sites perigosos, restringirá determinados softwares que podem ser instalados no dispositivo e fornecerá um controle para a implementação de atualizações nesse sistema em especial.”

Além disso, o monitoramento deveria incluir não apenas o uso real dos sistemas, mas também por quanto tempo eles estão sendo usados. Conforme declarado pelo National Cyber Security Centre, “o comportamento do usuário, como o horário normal de trabalho ou o local normal de trabalho, é [uma] métrica importante a ser monitorada”.

Há diversos sistemas de monitoramento disponíveis, criados para atender às necessidades específicas da rede em questão, mas, em geral, esses sistemas transferem os dados coletados para um local central, onde podem ser

analisados. Essas informações, ao longo do tempo, estabelecerão uma “linha de base” para o que constitui um comportamento normal em relação a variáveis como volume de transações, comunicações de ativos e atividade do usuário.

Por meio de suas avaliações, os auditores internos podem assegurar que sejam realizadas revisões regulares desses dados — e que a gestão se aproprie dessa tarefa — e que suas constatações criem uma linha de base que reflita precisamente a realidade da rede.

“Para os auditores internos, muito disso se resume à governança”, diz Tirado. “A gestão deve ser informada sobre o papel que desempenha na segurança do sistema, porque o sistema não vai se sustentar por muito tempo sozinho. As alterações nas políticas de segurança são determinadas pelo que a linha de base estabelece como “normal” e “anormal”. As revisões da gestão definem essa linha de base."

Estabelecendo uma Linha de Base

Como muitos elementos da cibersegurança ou, de fato, do gerenciamento de riscos, não há um modelo “tamanho único” e, como tal, a forma como a função de auditoria interna contribui para isso varia significativamente. “Depende dos recursos”, diz Tirado. “Depende do tamanho da organização. Depende do mandato da equipe de auditoria interna.”

Uma boa forma de estabelecer uma linha de base, diz ele, é mapeando um processo de prestação de avaliação não muito diferente de qualquer outro sistema de auditoria. “Como exemplo, pense na Sarbanes-Oxley”, ele oferece. “Toda empresa pública deve mapear os controles internos relacionados às demonstrações financeiras, desenvolvendo essa matriz. E, como parte desse mapeamento, você criará procedimentos de teste em um determinado período — como, por exemplo, um determinado ano. Você adotaria a mesma abordagem no Zero Trust, dividindo a avaliação em partes ao longo do ano, considerando o porte da empresa, os recursos, etc.

A linha de base comum entre todos os casos, entretanto, é a obrigação da auditoria interna de defender continuamente a implementação e a melhoria contínua de um sistema Zero Trust. Há uma variedade de recursos no mercado que ajudam nessa tarefa, com base no elemento em que o modelo Zero Trust está se concentrando. Por exemplo, em relação aos riscos de ransomware, Tirado usa o InfraGard, uma ferramenta gratuita de compartilhamento de informações desenvolvida por meio de uma parceria com o FBI e membros do setor privado. Em apenas alguns minutos no início de cada dia, Tirado pode usar a ferramenta para se atualizar sobre os últimos ataques de ransomware e violações de dados dentro e fora de sua indústria. “A escala desses ataques exige uma abordagem que vá além de um modelo de segurança baseado em perímetro”, explica ele. “Manter os stakeholders informados sobre como está o ambiente de risco e o que está em jogo é a prioridade número um da auditoria interna.”

Além disso, é importante observar que essa não é uma transição que precisa acontecer de uma só vez. “Mesmo em forma parcial, um modelo Zero Trust tem um valor imenso”, diz Tirado. "No fim das contas, um modelo Zero Trust se resume a uma coluna de controles em uma planilha. Talvez sejam 20, talvez sejam apenas 10 ou 12. Bem, já é melhor do que cinco.”

Exemplos de controles simples a considerar nas etapas iniciais de um modelo Zero Trust incluem:

- Criptografia de dados.
- Treinamento de conscientização sobre segurança.
- Planos de resposta a incidentes.
- Sistemas de detecção e resposta de endpoints.
- Microssegmentação.
- Monitoramento de conformidade.
- Análise comportamental e análise do comportamento de entidades de usuários.

A base já está lá

Apesar da mudança filosófica central na rede, os auditores internos deveriam perceber que, uma vez que o Zero Trust seja entendido, as responsabilidades da função em si não deveriam ser totalmente diferentes do que se esperava deles antes. A implementação do Zero Trust em si não exige qualquer mudança na arquitetura ou na infraestrutura além da possível adoção de certas ferramentas comerciais, e o mesmo pode ser dito sobre os sistemas que prestam avaliação para ele.

uma dessas responsabilidades permanece intacta. Com uma mão firme, adesão às *Global Internal Audit Standards™* (Normas Globais de Auditoria Interna) e disposição para aprender, a transição para uma arquitetura de rede de Zero Trust não é nada que uma organização deva temer.

Edições Anteriores

Para acessar edições anteriores do *Global Perspectives and Insights*, visite theiia.org/GPI.

Feedback do Leitor

Envie perguntas ou comentários para globalperspectives@theiia.org.

Sobre o The IIA

The Institute of Internal Auditors (IIA) é uma associação profissional internacional sem fins lucrativos que atende mais de 255.000 membros globais e concedeu mais de 200.000 certificações *Certified Internal Auditor*® (CIA®) no mundo todo. Fundado em 1941, o The IIA é reconhecido globalmente como líder da profissão de auditoria interna em normas, certificações, educação, pesquisa e orientação técnica. Para mais informações, visite theiia.org.

Isenção de Responsabilidade

The IIA publica este documento para fins informativos e educacionais. Este material não se destina a fornecer respostas definitivas a circunstâncias individuais específicas e, como tal, destina-se apenas a ser usado como guia. The IIA recomenda buscar assessoria especializada independente relacionada diretamente a qualquer situação específica. The IIA não aceita qualquer responsabilidade por qualquer pessoa que confie exclusivamente neste material.

Copyright

Copyright © 2025 The Institute of Internal Auditors, Inc. Todos os direitos reservados. Para permissão para reprodução, entre em contato com copyright@theiia.org.

Janeiro de 2025

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101