Framework do NIST, que traz as diretrizes mais importantes do mundo em segurança da informação, padronizando sua aplicação, foi atualizado no fim de fevereiro, com o reconhecimento da governança como um dos seis elementos fundamentais

As empresas precisam de uma **governança em segurança cibernética** para que possam se proteger das ameaças cada vez mais frequentes. No fim de fevereiro, o NIST (National Institute of Standards and Technology) publicou o **Cybersecurity Framework 2.0**, nova versão do framework ou da estrutura de segurança cibernética que se aplica a todas as organizações, independentemente do seu tamanho, setor ou maturidade tecnológica, com a principal novidade de incluir a governança como elemento imprescindível para o sucesso desses esforços em cibersegurança.

“O NIST fornece as diretrizes mais importantes do mundo em termos de segurança da informação. Ao definir uma taxonomia, um comportamento padrão para todo o mundo, ele fortalece a prevenção e o combate às ameaças cibernéticas por parte das organizações e dos governos. Essa padronização envolve conceitos, prioridades e a forma de organizar a companhia para fazer um trabalho bem-sucedido nessa área”, diz Demetrio Carrión, sócio-líder de cibersegurança da EY para LAS & Brasil.

Entre os principais desafios para as empresas está o **excesso de superfícies de ataque cibernético em potencial**, de acordo com 52% dos CISOs (Chief Information Security Officers) entrevistados pelo estudo Global Cybersecurity Leadership Insights, produzido pela EY. Ao considerar somente a amostra brasileira, essa resposta foi escolhida por 54% dos entrevistados. Nuvem em escala, Internet das Coisas (IoT, na sigla em inglês) e inteligência artificial/machine learning fazem parte das tecnologias que representam os **maiores riscos à cibersegurança das empresas** nos próximos cinco anos. “A nova versão do NIST começa a trabalhar taxonomia também para os incidentes cibernéticos provenientes de IA preditiva e regenerativa”, destaca Demetrio.

Bilhões de ameaças cibernéticas

O Brasil está entre os países mais vulneráveis a ataques cibernéticos, atrás apenas dos Estados Unidos, de acordo com relatório da Trend Micro referente ao primeiro semestre do ano passado. Apenas nos primeiros seis meses de 2023, a empresa bloqueou 85,6 bilhões de ameaças em todo o mundo. Como esses riscos estão em franco crescimento, a gestão deles deve ser uma tarefa contínua, segundo o NIST. Esse raciocínio se aplica para as empresas que estão começando a lidar com os desafios de cibersegurança e para aquelas ativas há muitos anos com uma equipe sofisticada voltada para esses esforços. O NIST fez da governança o sexto elemento fundamental, que deve ser aplicado em conjunto com identificação; proteção; detecção; resposta; e recuperação.

Por meio de uma governança estabelecida, as empresas mantêm ativas e atualizadas suas estratégias de cibersegurança, bem como as expectativas e a política de gestão de riscos. Além disso, têm capacidade de manter os colaboradores informados sobre as melhores práticas de segurança da informação, podendo monitorar adequadamente os riscos nos diferentes pontos de contato da empresa com o ambiente externo.

Cibersegurança como prioridade dos C-Levels

A governança envolve, ainda, a compreensão do contexto organizacional; a criação de um framework de cibersegurança; o gerenciamento do risco à segurança da informação por parte dos fornecedores da cadeia de suprimentos; a delegação de funções e responsabilidades; o estabelecimento de políticas internas; e a supervisão da estratégia de segurança cibernética. “As ameaças cibernéticas representam um dos maiores riscos corporativos, devendo receber atenção dos C-Levels, já que elas podem trazer danos financeiros e reputacionais irreversíveis”, observa Demetrio.

Veja abaixo os outros cinco elementos indispensáveis para os esforços de segurança cibernética, de acordo com a versão 2.0 do framework do NIST.

Identificação: É a compreensão dos riscos atuais de segurança cibernética da empresa. Isso significa mapear e entender o funcionamento dos ativos da organização (como dados, hardware, software, sistemas, instalações e serviços), assim como os fornecedores e os riscos de segurança cibernética relacionados, para priorizar esforços em uma estratégia de gestão de risco e de cumprimento dos objetivos traçados.

Proteção: É o uso de dispositivos para gerenciar os riscos de segurança cibernética da organização. A proteção envolve reduzir a probabilidade e os impactos dos ataques.

Detecção: Esses esforços permitem identificar e analisar ataques e comprometimentos à segurança da informação. Isso é feito por meio da descoberta de anomalias nos sistemas, indicadores de comprometimento e outros eventos adversos que podem indicar que ataques e incidentes cibernéticos estejam ocorrendo. Essa etapa permite respostas bem-sucedidas a incidentes e dá ensejo a atividades de recuperação.

Resposta: São as ações tomadas para conter os efeitos do incidente de segurança cibernética, como gerenciamento desse evento, análise, mitigação, relatórios e comunicação adequada.

Recuperação: É a restauração de ativos e operações afetados por um incidente de segurança. O objetivo é restaurar a normalidade o mais rápido possível para reduzir os efeitos do incidente, evitando que a operação da empresa seja interrompida.

As ações de governança, identificação, proteção e detecção devem ocorrer continuamente. Já as de resposta e recuperação precisam estar engatilhadas para que sejam adotadas imediatamente nos casos de incidentes de segurança cibernética. Essa metodologia do NIST se aplica a todos os tipos de ambiente tecnológico, incluindo nuvem, dispositivos móveis e **sistemas de inteligência artificial**.

Fonte: Agência EY, em 20.03.2024.