Mauro Sammarco
Presidente da Associação Comercial de Santos (ACS)

Proteção cibernética

Os incidentes cibernéticos entraram para o novo rol de preocupações das pessoas e das empresas. Segundo o Instituto Brasileiro de Cibersegurança, a cada 39 segundos ocorre um novo ataque cibernético no mundo.

Esses ataques são cada vez mais sofisticados e os criminosos se adaptaram ao uso de IA (Inteligência Artificial). Um levantamento global analisou 22.052 incidentes refletindo tanto o aumento das tentativas quanto a maior visibilidade dos incidentes por meio de investigação e reporte. Entre as tendências mais preocupantes está a presença dominante de um tipo de software mal-intencionado, que criminosos cibernéticos usam para bloquear o acesso, destruir ou publicar dados críticos de uma vítima, sequestrando assim uma organização e objetivando que um resgate seja pago.

Outro tipo de ataque crescente é a exploração de vulnerabilidades de segurança, visando principalmente o roubo de credenciais de usuários da organização. Houve um aumento muito expressivo em ataques de negação aos serviços digitais das organizações, pela criação de fluxos elevados de tráfego nas conexões e acesso na presença digital da organização, impedindo-a de usar seus serviços na internet.

As relações com terceiros — fornecedores de hardware, software, serviços na nuvem e até os parceiros comerciais — também emergiram como fator crítico, ou seja, o envolvimento de terceiros em incidentes analisados nas organizações dobrou, alcançando cerca de 30%.

A inteligência artificial já aparece no radar pelo seu uso em sofisticados ataques cibernéticos: e-mails maliciosos (de fraudes ou phishing) dobrou nos últimos dois anos, e evidências apontam para uso crescente dessas ferramentas automatizadas por agentes maliciosos.

No Brasil, entre os top 5 no uso de internet e redes sociais, os indicadores também preocupam. A Autoridade Nacional de Proteção de Dados (ANPD) formalizou regras sobre a comunicação de incidentes relacionados com a privacidade, elevando as exigências de reporte e a responsabilização das organizações que tratam dados pessoais.

Especialistas dizem que o Brasil enfrenta um momento de transição entre maior maturidade regulatória e ferramentas nacionais e lacunas em controles básicos e na proteção cibernética com pequenas e médias empresas mais vulneráveis. Infelizmente já se vê organizações sofrendo impactos significativos que vão desde prejuízos em sua imagem e marca até o encerramento de seus negócios.

Isso reforça a ideia de que a segurança deixou de ser apenas uma responsabilidade interna das organizações, mas também deve incluir todo o ecossistema de negócios, além de sua própria operação.

Analistas apontam prioridades desde reduzir o tempo de correção de vulnerabilidades críticas até treinar seus colaboradores para reconhecerem ataques de engenharia social e o uso malicioso de IA.

Recentemente a Associação Comercial de Santos (ACS) firmou uma parceria estratégica para ampliar sua própria proteção interna e a de seus membros. A solução utiliza inteligência artificial, monitoramento em tempo real e resposta automatizada a incidentes. Além disso, a ACS promove regularmente eventos e discussões sobre o tema, incluindo encontros com especialistas para debater a segurança digital em corporações e na administração pública.

AGENDA ACS

DIA 25/11, 8H30
Fórum Invest Retroporto (parceria com ABTTC)
Inscrições: bit.ly/invest-retroporto
DIA 26/11, 16 HORAS
Palestra: Os efeitos colaterais da reforma tributária nos negócios, com Lucas Ribeiro, fundador e CEO da ROIT
Inscrições: bit.ly/eventosReforma Tributária
DIA 27/11, 9 hORAS
1º Painel Setorial do Ipem-SP: Infraestrutura da Qualidade e Competitividade Portuária: Do Debate à Ação
Inscrições: bit.ly/ipemsp
DIA 27/11, 17 hORAS
ACS DAY - Happy Hour exclusivo para associados