FEDERAÇÃO NACIONAL DOS ENGENHEIROS

60 ANOS 1964–2024

CRESCE BRASIL

+ENGENHARIA +DESENVOLVIMENTO

Cidades Inteligentes

Cibersegurança: um requisito para o desenvolvimento de cidades inteligentes

MARCOS A. SIMPLICIO JUNIOR

Cibersegurança: um requisito para o desenvolvimento de cidades inteligentes

Prof. Dr. Marcos Antonio Simplicio Junior

Escola Politécnica, Universidade de São Paulo

Entre as áreas de tecnologia consideradas relevantes para promover bem-estar e qualidade de vida para a população, o setor de cibersegurança vem ganhando cada vez mais notoriedade e importância. A razão é que, quanto maior a integração de soluções tecnológicas no cotidiano dos cidadãos (e.g., por meio das "cidades inteligentes") e em infraestruturas críticas (e.g., na chamada "Indústria 4.0"), maior a necessidade de prevenir o abuso dessas soluções para fins maliciosos, bem como as consequências decorrentes desses abusos: prejuízos financeiros e materiais, danos psicológicos, e até mesmo a perda de vidas humanas.

Muito dessa notoriedade da área de cibersegurança na atualidade é resultado direto do aumento persistente de ameaças a sistemas computacionais: conforme relatório da Check Point [CP2023], organizações ao redor do mundo observaram uma média de 1158 ataques por semana em 2023, superando em 1% os números observados em 2022. Os setores mais afetados foram os de Educação/Pesquisa, Governamental/Militar, Saúde e Comunicações.

Infelizmente, o Brasil não é uma exceção nessa tendência de crescimento no número de incidentes de segurança: pelo contrário, o país apresenta uma situação particularmente preocupante. Por exemplo, um relatório recente da Trend Micro [A23] mostra que o Brasil continua entre os principais alvos de ciberataques no mundo, contando com mais de 100 bilhões de registros de tentativas de ataque em 2023; o setor governamental está entre os alvos preferenciais dos atacantes, que também miram em áreas como educação, mercado financeiro, e varejo. Preocupações similares são apresentadas em outro relatório de 2023, publicado pelo SOCRadar [S23], que mostra um aumento expressivo nos últimos anos de incidentes de segurança tendo o Brasil como protagonista, incluindo casos de roubo e vazamento de dados, ataques de ransomware, e personificação de sites brasileiros via phishing.

Agravando essa expansão do número e variedade de ameaças, o mundo ainda apresenta um grave déficit de profissionais capacitados e treinados para construir sistemas computacionais mais resilientes, testar sua segurança de forma efetiva, e reagir rapidamente a eventuais ataques. Segundo estimativas do Consórcio Internacional de Certificações em Segurança da Sistemas de Informação (*International Information System Security Certification Consortium* - ISC2), em 2023 havia uma necessidade de quase dobrar a força de trabalho especializada em cibersegurança no mundo: embora o número atual de profissionais da área seja da ordem de 5.5 milhões, estima-se que seja necessário formar cerca 4 milhões adicionais para satisfazer as crescentes demandas do mercado [ISC23].

É nesse cenário que, ao se planejar o uso de tecnologia para melhorar a qualidade de vida nas cidades, deve-se pensar também em como promover a proteção dessa infraestrutura tecnológica, prevenindo a ação de agentes maliciosos e coibindo abusos. Esse é o papel de profissionais de diversas áreas do universo da Engenharia, como Engenharia da Computação, Engenharia de Controle e Automação, e Engenharia de Software: projetar, construir e operar

soluções que sejam efetivas e robustas contra invasões, aproveitem sinergias entre diferentes sistemas, e ao mesmo tempo protejam os direitos dos cidadãos.

Essa não é, entretanto, uma tarefa fácil: ela exige profissionais com experiência e conhecimento sólido, capazes de aplicar boas práticas e evitar erros comuns, além de inovar quando necessário. De fato, pode-se ilustrar o grau potencial de complexidade envolvido na concepção de sistemas robustos, por meio de um exemplo bastante discutido no contexto de tecnologias para a segurança pública: o uso de câmeras de vigilância inteligentes. A adoção desses sistemas tem crescido no mundo, com o uso de equipamentos capazes de identificar situações de interesse diversas, como sons indicativos de potencial disparo de arma de fogo, imagens faciais de investigados ou foragidos da justiça, e placas de veículos suspeitos de participação em ocorrências policiais ou trafegando em alta velocidade. Embora tais soluções de monitoramento sejam bastante promissoras, em particular quando integradas a sistemas de comunicação com autoridades policiais e de resposta a emergências, um risco inerente é que o abuso de suas funcionalidades pode levar a situações indesejadas e até mesmo perigosas. Exemplos incluem o monitoramento de alvos específicos (e.g., figuras políticas) sem a devida autorização legal, vigilância em massa, ou violação de privacidade dos cidadãos, situações cujo risco é potencializado caso membros do crime organizado consigam acesso indevido ao sistema. Um bom projeto deve, portanto, prever mecanismos que previnam ou ao menos dificultem/coíbam a ação de atacantes, sejam eles internos ou internos, incluindo boas práticas como: minimizar a quantidade de informações efetivamente enviadas para uma central de monitoramento (e.g., removendo faces de pessoas que porventura estejam na mesma imagem que uma pessoa de interesse); proteger os subsistemas de comunicação e armazenamento com mecanismos adequados de criptografia, prevenindo manipulação ou acesso indevidos aos dados; exigir a autorização de diferentes autoridades competentes para incluir uma pessoa ou veículo na base de alvos de monitoramento, impedindo que agentes o façam de forma individual (e.g., motivados por ciúme ou vingança); restringir o acesso ao sistema a entidades devidamente identificadas e autorizadas, implementando mecanismos de autenticação robustos; testar a segurança do sistema usando técnicas e ferramentas de invasão, identificando e eliminando eventuais brechas encontradas; incluir mecanismos de detecção automatizada de falhas em equipamentos, facilitando tarefas de manutenção e garantindo a operação contínua do sistema; empregar técnicas e tecnologias de redundância, de modo que o sistema não possa ser facilmente tirado do ar ao se explorar pontos únicos de falha; fazer o devido registro de uso das funcionalidades do sistema, para eventual auditoria posterior em caso de suspeita de invasão ou abuso. Identificar esses requisitos e conhecer ferramentas capazes de implementá-los corretamente é uma parte do papel de profissionais que trabalham com cibersegurança.

Assim, para fazer frente ao desafio de construir e operar sistemas tecnológicos resilientes a ataques, é recomendado que entidades governamentais, nas suas diferentes esferas, considerem em seus planos de trabalho a inclusão de equipes especializadas em cibersegurança. Isso pode ser feito de forma específica, criando grupos dedicados a uma região ou sistema alvo, ou de forma integrada, com a criação de equipes que possam prestar suporte a múltiplos sistemas e jurisdições. Em qualquer dos casos, o ideal é haver profissionais atuando nas diferentes fases de cada projeto tecnológico, incluindo (1) sua concepção, para permitir a construção de sistemas mais robustos, e (2) sua operação, para permitir melhoria contínua do sistema e uma resposta rápida a eventuais incidentes de segurança.

A implantação dessa ação pode se apoiar não apenas em parcerias público-privadas, envolvendo empresas do setor de cibersegurança, mas também em programas já existentes no Brasil para promover a formação de profissionais na área, como: o Programa Hackers do Bem, coordenado pela Softex e executado pela Rede Nacional de Ensino e Pesquisa (RNP) e pelo Senai-SP, que visa à capacitação profissional em larga escala e de forma contínua em cibersegurança, contemplando estudantes de ensino técnico, médio e superior, e profissionais que buscam uma especialização no tema [HB24]; e o referencial de formação para Cursos de Bacharelado em CiberSegurança lançado pela Sociedade Brasileira de Computação SBC), que tem por objetivo nortear e promover a criação de cursos de graduação voltados especificamente à área de cibersegurança [SBC23].

Cabe notar também que iniciativas dessa natureza estão alinhadas com as diretivas da Política Nacional de Cibersegurança (PNCiber), lançada pelo governo federal em 26 de dezembro de 2023, que tem como objetivos principais [EBC23]:

- Promover o desenvolvimento de produtos, serviços e tecnologias de caráter nacional destinados à segurança cibernética;
- Garantir a confidencialidade, a integridade, a autenticidade e a disponibilidade das soluções e dos dados utilizados para o processamento, o armazenamento e a transmissão eletrônica ou digital de informações;
- Fortalecer a atuação diligente no ciberespaço, especialmente das crianças, dos adolescentes e dos idosos;
- Contribuir para o combate aos crimes cibernéticos e às demais ações maliciosas no ciberespaço;
- Estimular a adoção de medidas de proteção cibernética e de gestão de riscos para prevenir, evitar, mitigar, diminuir e neutralizar vulnerabilidades, incidentes e ataques cibernéticos, e seus impactos;
- Incrementar a resiliência das organizações públicas e privadas a incidentes e ataques cibernéticos;
- Desenvolver a educação e a capacitação técnico-profissional em segurança cibernética na sociedade;
- Fomentar as atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionadas à segurança cibernética;
- Incrementar a atuação coordenada e o intercâmbio de informações de segurança cibernética entre:a União, os Estados, o Distrito Federal e os Municípios; os Poderes Executivo, Legislativo e Judiciário; o setor privado; e a sociedade em geral;
- Desenvolver mecanismos de regulação, fiscalização e controle destinados a aprimorar a segurança e a resiliência cibernéticas nacionais; e
- Implementar estratégias de colaboração para desenvolver a cooperação internacional em segurança cibernética.

Em conclusão, ao integrar cibersegurança na construção de suas políticas públicas que dependem de tecnologia de informação e comunicação, gestores estarão dando um passo importante em uma direção que não apenas é relevante na prática, mas que também será cada vez mais cobrada de suas administrações.

[A23] ABES (2023) “Brasil permanece na lista dos países mais atacados por malware, aponta Trend Micro”. Associação Brasileira das Empresas de Software. URL: https://abes.com.br/brasil-permanece-na-lista-dos-paises-mais-atacados-por-malware-aponta-trend-micro/

[CP2023] Check Point (2023) Check Point Research: 2023 – The year of Mega Ransomware attacks with unprecedented impact on global organizations. URL: https://blog.checkpoint.com/research/check-point-research-2023-the-year-of-mega-ransomware-attacks-with-unprecedented-impact-on-global-organizations/

[EBC23] P. Peduzzi (2023) "Política Nacional de Cibersegurança já está vigorando no Brasil". Agência Brasil, Empresa Brasil de Comunicação (EBC). URL: https://agenciabrasil.ebc.com.br/geral/noticia/2023-12/politica-nacional-de-ciberseguranca-ja-esta-vigorando-no-brasil

[HB24] Programa Hackers do Bem. URL: https://conteudo.hackersdobem.org.br

[ISC23] ISC2 (2023) "How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce". International Information System Security Certification Consortium, Cybersecurity Workforce Study. URL: https://www.isc2.org/Research

[S23] SOCRadar (2023) “Brazil Threat Landscape Report - Unmasking Stealer Malware Dominance in Brazil”. URL: https://socradar.io/wp-content/uploads/2023/06/Brazil-Threat-Landscape-Report.pdf

[SBC23] SBC (2023) “SBC apresenta Referenciais de Formação para os Cursos de Bacharelado em CiberSegurança”. Sociedade Brasileira de Computação. URL: https://www.sbc.org.br/noticias/2508-sbc-apresenta-referenciais-de-formacao-para-os-cursos-de-bacharelado-em-ciberseguranca

Sindicatos filiados

Sindicato dos Engenheiros no Estado do Acre

Sindicato dos Engenheiros no Estado de Alagoas

Sindicato dos Engenheiros no Estado do Amapá

Sindicato dos Engenheiros no Estado do Amazonas

Sindicato dos Engenheiros no Estado do Ceará

Sindicato dos Engenheiros no Distrito Federal

Sindicato dos Engenheiros no Estado de Goiás

Sindicato dos Engenheiros no Estado do Maranhão

Sindicato dos Engenheiros no Estado de Mato Grosso

Sindicato dos Engenheiros no Estado de Mato Grosso do Sul

Sindicato dos Engenheiros no Estado do Pará

Sindicato dos Engenheiros no Estado do Piauí

Sindicato dos Engenheiros no Estado do Rio Grande do Norte

Sindicato dos Engenheiros no Estado do Rio Grande do Sul

Sindicato dos Engenheiros no Estado de Roraima

Sindicato dos Engenheiros de Santa Catarina

Sindicato dos Engenheiros no Estado de São Paulo

Sindicato dos Engenheiros, Arquitetos e Geólogos no Estado do Tocantins

FNE
FEDERAÇÃO NACIONAL DOS ENGENHEIROS

60 ANOS
1964–2024

SDS Edifício Eldorado, salas 106/109
CEP 70392-901 – Brasília/DF
Tel.: (61) 3225-2288 – secretaria@fne.org.br
www.fne.org.br

/FNEngenheiros /fnengenheiros /FNESind