ARTIGO

FORMANDO PROFISSIONAIS SOB A PERSPECTIVA DA EVOLUÇÃO NA ADOÇÃO DE SISTEMAS EM NUVEM

POR

Luiz Fernando Rust da Costa Carmo e Ewerton Longoni Madruga

Instituto Nacional de Metrologia, Qualidade e Tecnologia (Inmetro)

lfrust@inmetro.gov.br, elmadruga@inmetro.gov.br

Um sistema de software é como uma grande residência: possui diferentes compartimentos, como quartos e salas, construídos com lotes de tijolos de origem distinta. Ou seja, é importante lembrar que um sistema utiliza inúmeros componentes de diferentes fornecedores. E estes componentes de software têm diferentes níveis de maturidade no seu desenvolvimento, o que afeta a possibilidade de introdução de vulnerabilidades ao sistema como um todo. O eixo de Segurança de Sistemas trata dos aspectos dos sistemas compostos por componentes e conexões, e os softwares em uso [SBC 2023].

Os sistemas tradicionais já trazem consigo os seus próprios desafios. Eles executam dentro da empresa, em um computador, conectados à Internet, em uma sala climatizada e com configuração e operação monitoradas localmente. A cibersegurança deste tipo de sistema já vem sendo estudada há décadas e é razoavelmente bem entendida. Seus principais aspectos já são ensinados nos cursos superiores de computação no país, num processo que deve manter-se evolutivo de forma natu-

ral. Entretanto, no momento em que este artigo é escrito, uma explosão de demanda por Inteligência Artificial (IA) Generativa [WIZ 2024] faz com que a computação em nuvem e o crescimento na sua adoção provoque um deslocamento no eixo das discussões a respeito dos aspectos de segurança em sistemas.

Há pouco mais de um ano, a inteligência artificial generativa viu um crescimento explosivo tanto entre os usuários finais quanto nas empresas. Enquanto a IA e a aprendizagem de máquina tradicionais têm sido integradas tanto em empreendimentos científicos quanto comerciais há muitos anos, a IA generativa e os grandes modelos de linguagem (LLMs, na sigla em inglês) em particular tornaram essa tecnologia conhecida por todos. O poder da inteligência artificial generativa é potencialmente transformador. A tendência começou com os lançamentos de serviços de geração de imagens, incluindo *Midjourney e DALL-E 2 (OpenAI)*, em paralelo com modelos como o *Stable Diffusion da Stability.ai* [Roose 2022]. E esta tendência tomou proporções ainda maiores com o lançamento de serviços de geração de texto, e, especialmente, do ChatGPT (também OpenAI), logo a seguir.

Assim, olhando para o longo prazo, o potencial de crescimento da utilização da computação em nuvem dentro das empresas é muito grande [WIZ 2024], especialmente com a chegada das ondas de transformação que tecnologia de IA podem ainda vir a trazer dentro de empresas nos próximos anos. Entretanto, a computação em nuvem não é um assunto que seja refletido na realidade dos cursos de nível superior com a importância que está adquirindo. Gostaríamos de discutir o tema e acrescentar aspectos a serem considerados na hora da montagem do programa de cibersegurança dentro das universidades no país.

Modelos de Serviço

Existem diferentes modelos de serviço em *cloud computing*, que oferecem diferentes níveis de controle e responsabilidade para os usuários: IaaS, PaaS e SaaS. As principais diferenças entre eles são:

1. **Infrastructure as a Service (IaaS):** Nesse modelo, os provedores de serviços em nuvem fornecem infraestrutura básica de TI, como servidores virtuais, gerência de chaves criptográficas, armazenamento e redes. Os usuários têm controle total sobre o sistema operacional, aplicativos e dados, sendo responsáveis por instalar, configurar e gerenciar o software necessário. Exemplos de provedores de IaaS incluem Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform (GCP).
2. **Platform as a Service (PaaS):** Aqui os provedores de nuvem oferecem plataformas de desenvolvimento e execução de aplicativos, incluindo ferramentas de desenvolvimento, infraestrutura de execução, banco de dados e componentes de middleware. Os usuários desenvolvem

e implantam seus aplicativos na plataforma fornecida, sem se preocupar com a infraestrutura subjacente.

3. **Software as a Service (SaaS):** Nesse modelo, os usuários acessam aplicativos baseados na nuvem através da Internet, em vez de instalá-los localmente em seus dispositivos. Os provedores de serviços em nuvem são responsáveis por toda a infraestrutura, manutenção e atualizações do software. Exemplos de aplicativos SaaS incluem o Zoom, plataforma de videoconferência, e o Microsoft 365, plataforma com editor de texto, planilha e editor de apresentações.

Existem obstáculos em criar um ambiente de ensino de cibersegurança no contexto *cloud computing* em laboratório. Conside-se aqui um modelo de IaaS, por exemplo, que oferece uma conjunto grande de componentes (gerência de chaves, computação virtualizada, banco de dados, repositório de arquivos, orquestração de contêineres, execução de programas sem servidor, etc.) que podem ser interligados de maneiras diversas através de uma interface-console. Construir um protótipo válido na escola ou encontrar uma plataforma de baixo custo que replique em laboratório a experiência de um analista de segurança que audita um ambiente em produção dentro de um provedor de serviços de *cloud computing* não é um processo simples. Um pouco mais adiante, discutimos este problema na seção "Desafios Acadêmicos" e apresentamos possíveis soluções que atendam às instituições de ensino superior no país.

Referência Normativa

Para seguirmos a discussão, é importante contextualizar as normas de mais ampla aplicação que regem qualquer atividade de gestão corporativa com vistas à cibersegurança, utilizando computação em nuvem ou não. Existe uma enorme coleção de normas nesta área, mas, para simplificar a composição de novos planos pedagógicos, é possível estabelecer uma fundamentação regulatória mais básica com três padrões: a) ISO 27001, b) NIST CSF, e c) ISO/IEC 15408. A ISO 27001 [ISO 2022] é um padrão internacional que estabelece os requisitos para um sistema de gestão de segurança da informação (SGSI). Seu principal objetivo é garantir a confidencialidade, integridade e disponibilidade das informações em uma organização, além de minimizar os riscos de segurança da informação.

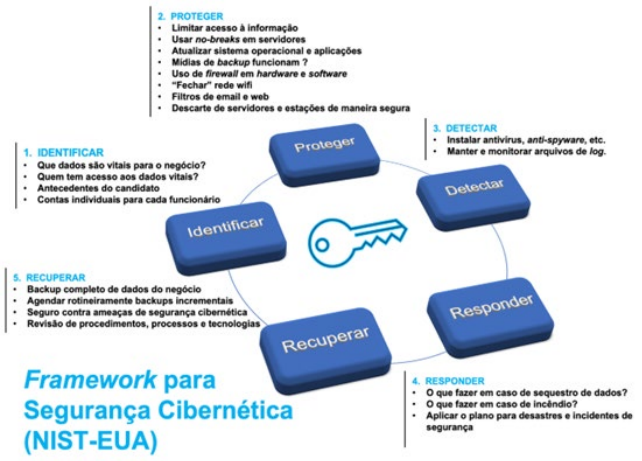

FIG. 01 | **O CYBERSECURITY FRAMEWORK (CSF), DO NIST**

Já o NIST *Cybersecurity Framework* (CSF) [NIST 2024] é um conjunto de diretrizes, melhores práticas e padrões destinados a ajudar as organizações a melhorarem sua postura de segurança cibernética. Como ilustra a Figura 1, este importante arcabouço concentra-se em cinco áreas principais: identificar, proteger, detectar, responder e recuperar, sendo focado em fornecer orientações práticas e acionáveis para a implementação de medidas de segurança cibernética.

Embora tanto o NIST CSF quanto o ISO 27001 possam ser utilizados em qualquer momento da jornada de segurança de uma organização, cada um tem um estágio de maturidade ideal em que são mais úteis. O NIST CSF é projetado para organizações em estágios iniciais de desenvolvimento de sua cibersegurança. Isso ocorre porque ele serve como um guia para ajudar uma empresa a construir uma estratégia de segurança da informação e estabelecer uma postura de segurança básica. O ISO 27001 é mais adequado para organizações mais maduras e com um risco de segurança aumentado. Ao buscar a certificação ISO 27001, a organização provavelmente já possui um programa geral de cibersegurança em vigor, mas precisa de práticas mais intensivas para fortalecer sua postura e aderir aos padrões do cliente. Possivelmente, porque empresas que compram serviços, para resguardar seu investimento, estabelecem a certificação de um fornecedor como um requisito técnico no processo de compra.

O padrão ISO/IEC 15408 diz respeito ao *Common Criteria for Information Technology Security Evaluation* (Critérios Comuns para Avaliação de Segurança de Tecnologia da Informação) [ISO 2009] é um padrão internacional utilizado para avaliar a segurança e a confiança de produtos e sistemas de tecnologia da informação. Os principais objetivos do *Common Criteria* são estabelecer critérios para avaliação de segurança de produtos e sistemas de TI, fornecer uma estrutura para a avaliação independente de segurança, permitir a comparação entre produtos de segurança, e promover a confiança no uso de produtos de TI.

Durante a pandemia, a distância forçada entre as pessoas trouxe uma explosão do uso de videoconferência para a comunicação em geral,não apenas para reuniões corporativas, mas também para comunicação pessoal, de cunho familiar. O software Zoom tornou-se um grande nome neste setor, tendo investido em computação em nuvem para atender esta demanda explosiva [Bourne 2020].

O serviço da empresa Zoom é um exemplo clássico de um SaaS, que baseia a oferta de serviços na computação em nuvem, e precisa do *Common Criteria* para expandir seu mercado. Numa decisão estratégica para se distanciar dos problemas que teve neste período de crescimento astronômico, e também aproximar-se de clientes corporativos de maior envergadura, a empresa obteve a certificação Common Criteria v3.1 rev 5. [Zoom 2021] para o seu Zoom Client. A familiaridade com este e com os demais padrões discutidos acima é importante e o estudo destes padrões traz um exemplo sobre o que os egressos de um curso de cibersegurança podem encontrar no mercado de trabalho.

Responsabilidade Compartilhada

Os principais provedores de serviços em nuvem (ou, no inglês, *Cloud Service Providers* - CSPs) operam sob um modelo de responsabilidade compartilhada. Isso significa que uma parcela das obrigações de segurança reside com a equipe de segurança da empresa cliente, que contrata o serviço. Transferir operações para uma plataforma de nuvem não significa que uma organização esteja livre de todas as responsabilidades de cibersegurança. O que toca a cada um depende do modelo de serviço empregado.

Por exemplo, no caso do modelo IaaS, os CSPs são responsáveis pela infraestrutura básica da nuvem, incluindo a segurança física das instalações que abrigam os equipamentos. Em outras palavras, os CSPs não são responsáveis pela segurança dos sistemas operacionais ou das pilhas de software necessárias para executar aplicativos ou armazenar dados.

No caso do modelo PaaS, este modelo requer que o provedor assuma maior responsabilidade adicional pelos aplicativos e sistemas operacionais. Não raro, a gerência não técnica de sistemas de computação em nuvem, erroneamente, posiciona-se no sentido de que a segurança da sua aplicação em nuvem é garantida integralmente pelo CSP. Ao contrário, a realidade é que existe este modelo de responsabilidade compartilhada, que significa que o CSP e seus clientes trabalham juntos para garantir a segurança dos dados e das aplicações na nuvem, cada um desempenhando um papel específico na proteção dos recursos.

Catálogos de Vulnerabilidades

Existem diferentes bases que são fundamentais para que a comunidade de profissionais de cibersegurança consiga acompanhar as centenas de vulnerabilidades que surgem diariamente. Quem usa software não deseja estar vulnerável, ou seja, não quer seus dados pessoais ou de clientes roubados por terceiros, por exemplo. Quem fabrica software que é oferecido como produto precisa acompanhar todos os problemas de segurança que surgem ao longo do ciclo de vida do produto. Detalhe – o acompanhamento não é apenas do seu produto, assim também como os componentes de software de terceiros que ele utiliza. Existe, portanto, uma teia de responsabilidades que deve ser bem compreendida para que a qualidade de um produto de software atenda às necessidades mínimas de segurança do cliente.

Por esta razão, existem várias bases de dados que auxiliam os profissionais responsáveis por administrar a segurança tanto de usuários como de produtos de fabricantes. Dois destes catálogos gerenciam não apenas vulnerabilidades de pacotes de software específicos, assim como potenciais classes de vulnerabilidades ('*weaknesses*') de pacotes de software. Uma classe de vulnerabilidades pode ser por exemplo uma que descreva em alto nível o que é um ataque de 'Cross-site Scripting' (XSS). Uma vulnerabilidade desta classe seria listada em outro catálogo com um grau numérico de severidade, e associado a um pacote de software específico.

O catálogo *Common Weakness Enumeration (CWE)*[1] é uma lista de diferentes tipos de falhas de segurança e vulnerabilidades comuns encontradas em software e hardware. Mantido pelo MITRE Corporation, o CWE fornece uma linguagem comum e padronizada para descrever e categorizar falhas de segurança, facilitando a identificação, compreensão e mitigação dessas vulnerabilidades. O CWE é utilizado por organizações de segurança, desenvolvedores de software e profissionais de segurança da informação para melhorar a segurança dos sistemas, ajudando a identificar e corrigir vulnerabilidades conhecidas e a evitar a introdução de outras durante o processo de desenvolvimento de software.

Já o catálogo de *Common Vulnerabilities and Exposures (CVE)*[2] é uma lista pública de informações sobre vulnerabilidades de segurança conhecidas em software e hardware específicos. Mantido pela organização MITRE Corporation, o CVE fornece identificadores únicos (CVE IDs) para cada vulnerabilidade, juntamente com informações detalhadas sobre a vulnerabilidade, sua gravidade e as maneiras de mitigá-la. O objetivo principal do CVE é fornecer uma referência comum para identificar e compartilhar informações sobre vulnerabilidades de segurança, facilitando a colaboração entre os pesquisadores de segurança, fabricantes de produtos e usuários finais para proteger sistemas e dados de contra-ataques maliciosos.

1 https://cwe.mitre.org/

2 https://www.cve.org/

Com muita frequência, surgem vulnerabilidades associadas aos provedores de serviço de nuvem. Como por exemplo, o CVE-2024-28823, que diz respeito a um módulo em *javascript* para acesso a repositórios de arquivos em nuvem através do protocolo HTTPS. A vulnerabilidade é da classe definida por CWE-79, conhecida como '*Cross-Site Scripting (XSS)*'. Este é um dos serviços de nuvem mais básicos e esta vulnerabilidade permite a injeção de código *javascript* não autorizado e potencial vazamento de informação. É desejável que casos como este sejam estudados em sala de aula no contexto de segurança em serviço de nuvem.

Desafio Acadêmico

No currículo de um curso de cibersegurança [SBC 2023], o eixo de formação em segurança de sistemas tem desafios importantes no desenvolvimento de competências quando o contexto é nuvem. Existem aspectos da tecnologia de computação em nuvem em que a reprodução em laboratório é mais simples. Por exemplo, a competência C.2.7 fala da necessidade da utilização de técnicas de resiliência. A replicação de várias instâncias de máquinas virtuais para simular tolerância a falhas de um sistema é algo razoavelmente simples de explicar em sala de aula e montar em laboratório usando Linux, KVM, e QEMU. [FONSECA 2017]

Entretanto, existem também obstáculos. Em primeiro lugar, existe a necessidade de acompanhar a contabilidade de uso dos componentes em nuvem. Alunos devem ser doutrinados a monitorar

muito de perto o custo da atividade sendo realizada. Caso a atividade envolva, por exemplo, o uso de aceleradores de cálculo matemático (GPUs, TPUs, etc.) para treinamento de um modelo em Deep Learning, a conta diária pode ser muito alta. Simular esta contabilização no uso de componentes de serviço em nuvem na escola não é uma tarefa fácil.

Em segundo lugar, os CSPs em geral mantêm disponível uma extensa *Application Programming Interface* (API) para controle de toda sua longa lista de serviços. Autenticação e autorização passam por dar acesso correto aos diversos usuários que controlam o uso da nuvem corporativa. E, ficando apenas neste exemplo, o teste para autorização a esta lista de serviços disponibilizados por CSPs, mesmo considerando os mais básicos, é difícil de ser replicado apenas com Linux, KVM e QEMU.

Os maiores provedores de serviço de nuvem mantêm um programa de certificação de profissionais[3][4]. Na esteira da preparação para esta certificação, estes provedores mantêm também portais educacionais aos quais instituições de ensino no país podem ter acesso sem custo. Esta é uma ótima alternativa que exige apenas o contato da instituição com as academias de cada um dos grandes provedores. É uma solução completa para os dois obstáculos listados acima.

Como alternativa, existem soluções de código aberto que podem ser utilizadas em laboratório. Uma destas alternativas é o OpenStack[5], que é um conjunto de módulos para a criação e gerenciamento de nuvens computacionais públicas e privadas. Ele fornece uma plataforma para a virtualização de recursos de computação, armazenamento e rede, permitindo que os usuários criem e gerenciem nuvens de forma flexível e escalável.

O OpenStack é composto por vários projetos inter-relacionados, cada um sendo associado a uma parte específica da funcionalidade da nuvem, como computação virtual (Nova), armazenamento em bloco (Cinder), armazenamento de objetos (Swift), rede (Neutron) e gerenciamento de identidade (Keystone), entre outros.

Mensagem Final

Conforme explicado no início do artigo, com o surgimento de tecnologias inovadoras como a Inteligência Artificial, existe uma tendência de crescimento na adoção de serviços de *cloud computing* pelas empresas. Daí segue a necessidade de estruturar unidades curriculares que se ocupem em ensinar os diversos aspectos relevantes sobre a segurança de sistemas em contexto de computação em nuvem. Além de padrões internacionais de segurança e bases globais de vulnerabilidades relevantes, discutimos alternativas para que instituições de ensino no país possam superar as dificuldades de trazer uma experiência mais mão na massa em sala de aula ou em laboratórios. Esta experiência nos bancos escolares torna-se crucial

3 https://aws.amazon.com/pt/training/awsacademy/

4 https://learn.microsoft.com/pt-br/training/educator-center/

5 https://www.openstack.org/

na formação de profissionais com perfil tão carente no mercado de trabalho.

Referências

1. SOCIEDADE BRASILEIRA DE COMPUTAÇÃO. Referenciais de formação para o curso de Bacharelado em CiberSegurança. Porto Alegre: Sociedade Brasileira de Computação (SBC), 2023. 40p. DOI 10.5753/sbc.ref.2023.125.
2. Wiz Inc. State of AI in the Cloud, 2024. Obtido em: https://www.wiz.io/blog/key-findings-from-the-state-of-ai-in-the-cloud-report-2024
3. International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO/IEC Padrão número 27001:2022). Obtido em https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-3:v1:en
4. International Organization for Standardization. (2009). Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model (ISO/IEC Padrão número 15408). Obtido em https://www.iso.org/obp/ui/#iso:std:iso-iec:15408:-1:ed-3:v2:en
5. National Institute of Standards and Technology (2024). The NIST Cybersecurity Framework (CSF) 2.0. Obtido em https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
6. ROOSE, K. AI-Generated Art Is Already Transforming Creative Work. New York Times, Outubro 2022.
7. BOURNE, J. Zoom makes Amazon Web Services its preferred cloud provider, Dezembro 2020. Obtido em https://www.cloudcomputing-news.net/news/2020/dec/04/zoom-makes-amazon-web-services-its-preferred-cloud-provider
8. ZOOM, Inc. Common Criteria, Dezembro 2021. Obtido em https://www.zoom.com/en/trust/legal-compliance/common-criteria/
9. FONSECA, N. Networking for Big Data: Lab Exercise. UNICAMP, 2017. Obtido em: https://www.ic.unicamp.br/~nfonseca/comsoc-school/2017/lab-exercise.html

EWERTON LONGONI MADRUGA é pesquisador-tecnologista do Instituto Nacional de Metrologia, Qualidade e Tecnologia (INMETRO). Tem Bacharelado e Mestrado em Ciências de Computação pela Universidade Federal do Rio Grande do Sul (UFRGS), assim como Doutorado em Engenharia de Computação pela Universidade da California, Santa Cruz. Foi desenvolvedor de sistemas e protocolos de rede na Nokia Networks, em Mountain View, CA, até 2003. Atualmente é pesquisador-tecnologista e coordenador do Curso Técnico em Segurança Cibernética (INMETRO/IFF). Suas áreas de interesse são segurança da informação, sistemas móveis, computação em nuvem e aprendizado de máquina aplicado à técnicas de segurança ofensiva.

LUIZ F RUST C CARMO é formou-se em Engenharia Eletrônica em 1984, obteve o título de M.Sc. em Ciência da Computação em 1988, ambos pela Universidade Federal do Rio de Janeiro (UFRJ), e Ph.D. em Ciência da Computação em 1994, pelo Laboratório de Arquitetura e Análise de Sistemas da Organização Nacional Francesa de Pesquisa Científica (LAAS/CNRS) em Toulouse - França. Desde 2008 é Especialista Sênior do Instituto Nacional de Metrologia, Qualidade e Tecnologia (INMETRO) e, atualmente, atua como Diretor de Metrologia Científica, Industrial e Tecnologia. É professor ativo nos programas de doutorado em Ciência da Computação na UFRJ (PPGI) e em Metrologia (PPGMT) no Inmetro. Seus interesses de pesquisa incluem segurança da informação, validação de software para sistemas embarcados e transformação digital em metrologia.