2 de outubro de 2019

Cel Arthur Pereira Sabbat
Diretor do Departamento de Segurança da Informação e Comunicação (DSIC)
Gabinete de Segurança Institucional da Presidência da República

Re: Comentários sobre a proposta de Estratégia Nacional de Segurança Cibernética

Prezado Cel Arthur Pereira Sabbat

A BSA| The Software Alliance (BSA)[1] agradece a oportunidade de oferecer comentários à proposta de Estratégia Nacional de Segurança Cibernética (E-Ciber). Os membros da BSA têm um compromisso profundo e de longa data em proteger os dados de seus clientes através de tecnologias e modelos de negócios. Portanto, parabenizamos o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) por seus esforços para fortalecer a segurança cibernética no Brasil.

A estratégia proposta contém muitos elementos positivos. Parabenizamos particularmente a GSI por seu foco no fortalecimento da colaboração entre as partes interessadas em toda a sociedade, de maneira a promover a inovação, a flexibilidade e o envolvimento internacional. Além disso, oferecemos algumas recomendações gerais aplicáveis em toda a Estratégia, bem como algumas recomendações específicas para ações estratégicas individuais, que acreditamos serem importantes para garantir políticas robustas e eficazes de segurança cibernética em vigor no Brasil. A BSA e seus membros têm uma vasta experiência trabalhando com governos e outras partes interessadas em todo o mundo em políticas que promovem políticas fortes de segurança cibernética e compartilhamos as opiniões abaixo para ajudar a GSI em seus esforços para alcançar esse objetivo.

---

[1]A BSA| The Software Alliance (www.bsa.org) é a principal defensora da indústria global de software junto aos governos e no mercado internacional. Seus membros estão entre as empresas mais inovadoras do mundo, criando soluções de software que estimulam a economia e melhoram a vida moderna. Com sede em Washington, DC, e operações em mais de 60 países, a BSA é pioneira em programas de conformidade que promovem o uso legal de software e defende políticas públicas que promovam a inovação tecnológica e impulsionam o crescimento da economia digital.

São membros da BSA: Adobe, Akamai, Apple, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens PLM Software, Sitecore, Slack, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

Rua Samuel Morse, 134 Conjunto 62
São Paulo – SP, CEP 04576-060

F (11) 4420-3070
W bsa.org

Recomendações Gerais:

A BSA recomenda que a Estratégia proposta esclareça que as futuras políticas de segurança cibernética sejam baseadas nos seis princípios gerais a seguir:

1 - As políticas devem estar alinhadas com as normas técnicas internacionalmente reconhecidas.

Os padrões técnicos reconhecidos internacionalmente fornecem estruturas amplamente avaliadas e baseadas em consenso para definir e implementar abordagens eficazes para a segurança cibernética e facilitar abordagens comuns para desafios comuns, possibilitando colaboração e interoperabilidade. Esse alinhamento é particularmente importante no que diz respeito à priorização da estratégia de proteção de infraestruturas críticas nacionais; as normas e orientações técnicas internacionalmente reconhecidas, conforme descritas no Relatório Técnico da Organização Internacional de Padronização (ISO)/Relatório Técnico 27103 da Comissão Eletrotécnica Internacional (IEC), podem garantir que as infraestruturas críticas nacionais do Brasil adotem abordagens comprovadas de defesa cibernética e que o Brasil esteja disposto a cooperar com a comunidade internacional no enfrentamento de ameaças transnacionais. Da mesma forma, quaisquer certificações de segurança cibernética contempladas na Ação Estratégica 1 devem ser alinhadas com os padrões técnicos reconhecidos internacionalmente por razões semelhantes.

2 - As políticas devem ser baseadas em risco, focadas em resultados e neutras em tecnologia.

A atividade maliciosa de segurança cibernética acarreta riscos diferentes para sistemas diferentes. Geralmente, existem várias abordagens para se defender contra o mesmo tipo de ataque cibernético e várias abordagens para melhorar a segurança e a resiliência do sistema em geral. As políticas devem refletir essas variáveis, priorizando abordagens que abordem diferentes níveis de risco e permitam aos proprietários e operadores de redes e sistemas defender sua infraestrutura com as tecnologias e abordagens que considerem melhores para atingir o nível de segurança desejado. A BSA recomenda que a Estratégia proposta avalie uma abordagem baseada em risco, focada em resultados e neutra em termos de tecnologia em toda a Estratégia.

3 - As políticas devem se basear em mecanismos orientados pelo mercado, sempre que possível.

A tecnologia da informação está em constante evolução e as ameaças à segurança cibernética evoluem com ela. Nem as tecnologias nem as ameaças são limitadas pelas fronteiras nacionais, o que significa que é improvável que o excesso de confiança nas estruturas governamentais ou na fiscalização regulatória atinja os resultados desejados. As políticas que alavancam as forças do mercado para impulsionar a segurança cibernética provavelmente serão mais bem-sucedidas em acompanhar o ambiente de segurança em mudança e alcançar o efeito mais amplo.

4 - As políticas devem ser orientadas para proteger a privacidade.

Nenhuma abordagem à segurança cibernética deve comprometer a integridade dos dados que ela procura defender contra atividades cibernéticas maliciosas; as políticas de segurança cibernética devem ser cuidadosamente sintonizadas com as considerações de privacidade. As principais considerações incluem garantir a liderança civil, incentivar fortes proteções de dados, proteger informações pessoais nos mecanismos de compartilhamento de informações e evitar políticas que comprometam o uso de tecnologias de aprimoramento da privacidade.

Recomendações específicas sobre ações estratégicas definidas na estratégia proposta:

Além de confiar nos princípios descritos acima, oferecemos as seguintes recomendações com relação a entradas específicas na Seção de Ações Estratégicas da Estratégia proposta.

Ação estratégica 1 - Fortalecer a governança de segurança cibernética

- A BSA concorda que o estabelecimento de requisitos mínimos de segurança cibernética em compras públicas pode servir como uma ferramenta poderosa para aprimorar a segurança cibernética do setor público e incentivar uma segurança mais forte em todo o mercado. Ao estabelecer esses requisitos, é importante garantir que as aquisições permaneçam neutras em termos de tecnologia, evite os requisitos de preferências domésticas, garanta que quaisquer esquemas de certificação exigidos sejam voluntários, orientados pelo o mercado, de base ampla e alinhados internacionalmente, e sejam consistentes com os padrões internacionalmente reconhecidos.

Da mesma forma, as certificações de segurança cibernética podem incentivar a conscientização sobre segurança cibernética e permitir que os consumidores priorizem a segurança ao comparar produtos ou serviços concorrentes. Assim como os padrões de compras, as certificações devem ser neutras em termos de tecnologia, voluntárias, orientadas pelo mercado e alinhadas com padrões reconhecidos internacionalmente.

Além disso, como os países do mundo todo consideram os esquemas de certificação de segurança cibernética, o Governo deve tomar medidas para garantir que todos os esquemas de certificação estabelecidos no Brasil sejam interoperáveis e recíprocos com certificações semelhantes em mercados estrangeiros. Isso permitirá que as empresas brasileiras concorram com mais eficiência no mercado externo, contribuindo para uma linha de base comum de segurança.

Ação estratégica 5 - Elevar o nível de proteção da infraestrutura crítica nacional

A BSA concorda que a proteção crítica da infraestrutura é fundamental para uma estratégia robusta de segurança cibernética. Essa ação estratégica pode ser melhorada ainda mais, fornecendo orientações para a criação e manutenção de um Plano Nacional de Resposta a Incidentes de Segurança Cibernética atualizado para infraestrutura

crítica. Além disso, para garantir uma forte política de segurança cibernética para proteger a infraestrutura crítica, a Estratégia proposta deve:

- Focar nos resultados de segurança;
- Usar estrutura flexível e baseada em risco;
- Evite a definição excessiva de infraestrutura crítica;
- Alinhar a segurança crítica da infraestrutura com os padrões internacionalmente reconhecidos, particularmente conforme descrito no Relatório Técnico ISO / IEC 27103;
- Evitar padrões de segurança locais;
- Garantir que quaisquer regimes de certificação sejam equilibrados, transparentes e baseados internacionalmente;
- Rejeitar os requisitos para divulgar o código fonte e outras propriedades intelectuais.

Ação estratégica 6 - Melhorar o quadro jurídico de segurança cibernética

A BSA elogia a GSI por promover uma estrutura legal mais forte de segurança cibernética, que é uma base importante para a dissuasão, prevenção e repressão de crimes cibernéticos. A Convenção de Budapeste sobre criminalidade cibernética estabelece um padrão internacional para um quadro legal nacional cibernético eficaz e justo; A BSA insta o Brasil a direcionar seus esforços no âmbito da Ação Estratégica 6 para alinhar sua estrutura legal com a Convenção de Budapeste. Além disso, este quadro jurídico deve:

- Ativar fluxos de dados transfronteiriços para fins comerciais;

- Evitar requisitos de localização de dados;

- Manter um ambiente político que permita tecnologias emergentes; e

- Garantir treinamento técnico adequado e apoio à aplicação da lei.

Ação estratégica 8 - Aumentar a cooperação internacional em segurança cibernética

Como a Estratégia proposta reconhece, a cooperação internacional em segurança cibernética é essencial. Os esforços multilaterais em andamento no momento têm como objetivo criar os padrões que guiarão a segurança em tecnologias emergentes, como redes de comunicações 5G e Internet das Coisas, bem como em áreas de preocupação emergentes, como segurança da cadeia de suprimentos. Na busca do engajamento internacional descrito na Ação Estratégica 8, é essencial que o Brasil participe dessas iniciativas de estruturação futura. Além disso, à medida que esses padrões tomam forma, a BSA insta o Brasil a trabalhar para influenciar e adotar esses padrões internacionais, em vez de buscar soluções específicas do Brasil para os que são claramente desafios transnacionais.

Ação estratégica 10 - Elevar o nível de maturidade da segurança cibernética

A Ação Estratégica 10 identifica a necessidade de promover a capacitação na área de segurança cibernética; essa ação deve ser esclarecida, estabelecendo a importância de identificar/mapear as habilidades necessárias e as lacunas existentes como o primeiro passo para alcançar esse objetivo.

Também é importante incluir referência a iniciativas para promover o desenvolvimento de habilidades em segurança cibernética. A abordagem da escassez de trabalhadores com habilidades em segurança cibernética deve incluir ações que visem todo o espectro da força de trabalho.

A Estratégia proposta deve incentivar iniciativas para aumentar o interesse e o acesso à educação em ciências da computação para estudantes do ensino básico ("alunos no ensino fundamental"), com foco na expansão de parcerias público-privadas, repensando a educação profissional e treinando mais professores qualificados.

Também é importante se concentrar em programas de reciclagem no meio da carreira para fornecer aos trabalhadores habilidades de alta segurança em segurança cibernética. Isso deve incluir iniciativas para permitir que os funcionários das agências federais aproveitem a experiência do setor privado para treinar uma variedade de habilidades e melhores práticas de segurança cibernética.

Estrutura BSA para software Seguro

Por fim, a BSA reconhece que o software desempenhará um papel vital no sucesso de todas as ações estratégicas identificadas na Estratégia proposta. A sociedade moderna é construída com base em software - o software fornece tecnologias pessoais, infraestrutura crítica, indústrias em todos os setores e tecnologias emergentes, como 5G e Inteligência Artificial. À medida que comunidades e empresas se tornam cada vez mais dependentes do software, a segurança desse software se torna fundamental.

A BSA está comprometida em elevar o nível de segurança de software em todo o ecossistema digital. No início deste ano, a BSA lançou o BSA Framework for Secure Software, um *benchmark* pioneiro em segurança de software que é específico, mensurável e aplicável a todos os tipos de software. O objetivo é permitir uma avaliação significativa da segurança dos produtos e serviços de software e informar as discussões entre os principais interessados - desenvolvedores, fornecedores, consumidores, formuladores de políticas e outros - a fim de elevar a segurança desses produtos e serviços e permitir informações informadas sobre segurança. decisões no mercado.

Oferecemos BSA Framework for Secure Software como um recurso ao governo brasileiro, na medida em que desenvolve iniciativas para aumentar a segurança cibernética e esperamos oportunidades de colaborar com o governo para tratar da segurança do software. Gostaríamos de ter a oportunidade de fornecer mais informações sobre o Framework, conforme apropriado.

Mais uma vez, gostaríamos de agradecer a oportunidade de oferecer esse conjunto inicial de comentários que esperamos contribuir para criar uma estrutura robusta de segurança cibernética no Brasil. Esperamos continuar participando dessa importante discussão e estaremos prontos para responder a quaisquer perguntas que você possa ter.

Atenciosamente,

Antonio Eduardo Mendes da Silva
Country Manager – Brazil
BSA | The Software Alliance