Segurança da Informação como vetor da defesa cibernética

Cap Inf Filipe Ramos Gajo*

Introdução

Em 2007, a Estônia enfrentou o primeiro grande ataque cibernético conhecido. Depois de uma disputa sobre a remoção de um memorial da Segunda Guerra Mundial entre os governos estoniano e russo, a Estônia foi alvo de ataques cibernéticos em massa destinados ao governo, bancos e imprensa. O governo estoniano desativou o acesso externo de IP e, como resultado, levou meses para retornar à normalidade (Araújo, 2022). Esse ataque teve repercussões em todo o mundo e marcou o início da implementação de políticas e estratégias de segurança cibernética e defesa cibernética (Cassiani, 2023, p. 5).

O ataque cibernético é definido como uma invasão não autorizada a um sistema para causar danos ou obter dados e informações sigilosas através de meios fraudulentos (Klusaitè, 2023). A segurança da informação, por outro lado, é fundamental para prevenir e mitigar os efeitos dos ataques cibernéticos, garantindo a confidencialidade, integridade e disponibilidade das informações (Brasil, 2022).

Com a crescente conectividade e transformação digital, o número de ataques cibernéticos tem aumentado exponencialmente. De janeiro a junho de 2022, o Brasil sofreu 31,5 bilhões de tentativas de ataques cibernéticos, um aumento de 94% em relação ao mesmo período do ano anterior. Isso colocou o Brasil na segunda posição entre os países da América Latina que mais sofreram ataques cibernéticos (Fortinet, 2022).

Diante desse cenário preocupante, o Estado brasileiro tem tomado medidas para fortalecer a segurança da informação. Em 2018, foi instituída a Política Nacional de Segurança da Informação (PNSI), que tem como princípios garantir o sigilo das informações essenciais à segurança da sociedade e do Estado e promover a educação como base para incentivar a cultura de segurança da informação (Brasil, 2018).

Em relação às Forças Armadas, a importância da segurança da informação se dá diante da necessidade de manter o país preparado para responder a cenários adversos de defesa (Brasil, 2014). Em 2008, a Estratégia Nacional de Defesa (END) estabeleceu como prioridade três setores estratégicos: nuclear, cibernético e espacial (Brasil, 2008). Dessa forma, com o objetivo de cumprir a END nos setores estratégicos de defesa, o Ministério da Defesa atribuiu ao Exército a responsabilidade pela coordenação e integração do setor cibernético (Brasil, 2009).

Dessa forma, com a crescente digitalização, torna-se imperativa a confluência entre segurança da informação e defesa cibernética. Sendo assim, de que maneira é possível utilizar a segurança da informação como um elemento-chave na estratégia de defesa cibernética?

* Cap Inf (AMAN/2011, EsAO/2021). Pós-graduado em Ciências Militares. Atualmente é instrutor da Escola de Aperfeiçoamento de Oficiais.

Ataque x defesa

Com a aprovação da END em 2008, os campos da segurança cibernética e defesa cibernética passaram a ser reconhecidos. O primeiro ficou a cargo da Presidência da República, já a defesa cibernética, a cargo do Ministério da Defesa. Conforme o nível decisório – nível político, estratégico, operacional e tático – as ações cibernéticas receberam as denominações descritas na **figura 1** (Brasil, 2014, p. 17).

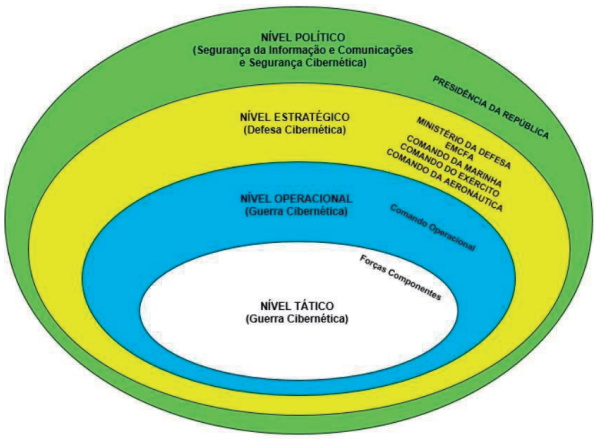

Figura 1 – Figura ilustrativa dos níveis decisórios das ações cibernéticas
Fonte: Brasil, 2014, p. 17

Ataque

De acordo com Brasil (2014) a defesa cibernética é composta por ações ofensivas, defensivas e exploratórias realizadas no ambiente virtual, coordenadas pelo Ministério da Defesa em um planejamento nacional estratégico. Seus objetivos são proteger os sistemas de informação relevantes para a defesa nacional, obter informações para a produção de inteligência e comprometer os sistemas de informação do oponente.

Conceitualmente, ataque cibernético engloba ações que visam interromper, negar, degradar, corromper ou destruir informações e sistemas armazenados em dispositivos e redes computacionais e de comunicação (Brasil, 2014, p. 23). Dessa forma, é fundamental destacar a importância da prevenção em setores críticos, uma vez que os ataques cibernéticos podem ter consequências graves para a segurança do país.

Dentre as características da defesa cibernética, destaca-se a insegurança latente e a vulnerabilidade das fronteiras geográficas. O primeiro afirma que nenhum sistema computacional é totalmente seguro, uma vez que seus ativos de informação sempre serão alvos por meio de ameaças cibernéticas. Já o segundo reforça que os agentes podem atuar de qualquer lugar e realizar suas ações em qualquer lugar (Brasil, 2014, p. 23).

No atual conflito envolvendo Rússia e Ucrânia, uma situação em particular chamou a atenção. O Ministro da Defesa russo afirmou que o uso de celulares por militares ucranianos permitiu o rastreamento e a determinação das coordenadas das localizações dos soldados ucranianos para o ataque, ocorrido no dia de ano novo (CNN, 2023),

Defesa

A segurança da informação pode ser caracterizada como o conjunto de medidas que visam proteger dados de empresas e indivíduos, bem como o valor associado a eles, em qualquer ambiente, seja físico ou virtual. A segurança da informação atua para que os dados estejam seguros a vazamentos (Andrade, 2023).

Nesse contexto, a segurança da informação possui como pilares: confidencialidade, integridade e disponibilidade. A confidencialidade faz referência à segurança das informações, que não devem ser acessadas por pessoas não autorizadas. A integridade possui relação direta com a informação armazenada, devendo ser garantida que nenhuma alteração ocorrerá em seu conteúdo. Já a disponibilidade requer que as informações estejam sempre disponíveis, sempre que necessário (Batistella, 2023).

Embora a tecnologia seja essencial na defesa cibernética, a velha máxima de que "os seres humanos são o elo mais fraco" em qualquer programa de segurança parece ser mais verdadeira do que nunca. Uma pesquisa conduzida pela empresa de segurança cibernética Tessian descobriu que 88% das ocorrências de violação de dados envolveram erro humano (SHRM, 2023).

Tendo em mente que os ataques cibernéticos podem assumir diversas formas – cavalos de troia, *backdoors, botnets, spywares, phishing, spear phishing* e outros (Da Silva; Nogueira, 2019) – aliados ao fato de que novas formas de ataques surgem constantemente (FBI 2018), um tipo de técnica específica merece destaque: a engenharia social, uma vez que tem o foco principal no usuário dos mais diversos serviços (Kaspersky, 2023a).

Com o intuito de manipular as pessoas para que compartilhem informações confidenciais, visitem *sites* que não deveriam, façam *downloads* de programas maliciosos ou até mesmo enviem dinheiro para criminosos, a engenharia social explora as fraquezas humanas, deixando de lado as falhas técnicas (IBM, 2023).

Grande parte de todos os tipos de ataques cibernéticos contém alguma forma de engenharia social. Alguns exemplos incluem *e-mails* de *phishing* e golpes com vírus, que são repletos de insinuações sociais para convencer os usuários de que são de fontes legítimas e obter dados pessoais ou corporativos (Kaspersky, 2023a).

Segundo Kaspersky (2023b), o ataque denominado como *phishing* é uma forma de fraude eletrônica que visa enganar um indivíduo, organização ou empresa específica por intermédio de *e-mails* ou outras formas de comunicação eletrônica. Embora o principal objetivo seja roubar dados pessoais ou corporativos, os criminosos cibernéticos também podem tentar instalar *software* malicioso no dispositivo do usuário. Frequentemente as informações e dados confidenciais roubados são revendidos para governos e empresas privadas.

Os ataques de *phishing* representam um desafio, pois são altamente personalizados e, portanto, difíceis de detectar. Uma única falha por parte de uma pessoa pode ter consequências graves, afetando empresas, governos e organizações sem fins lucrativos. Esses ataques podem levar à divulgação de informações confidenciais, manipulação de preços de ações e atividades de espionagem (Kaspersky, 2023b).

Seja no Brasil ou pelo mundo, o vazamento de dados é cada vez mais frequente, corroborando com a ideia de que o usuário é o elo mais fraco na segurança. Em 2022, pesquisadores compraram cartões de memórias com informações pessoais de mais de 2.600 militares (Soldateli, 2023). Já em 2023, um militar de baixa patente conseguiu acesso a documentos ultrassecretos dos EUA e os divulgou em uma plataforma *online* de bate-papo (Debusmann, 2023). No Brasil, em janeiro de 2021, os dados de 223 milhões de pessoas foram vazados, incluindo informações sobre CPF, nome, sexo, dados de veículos, entre outros (G1, 2023). Sendo assim, à medida que informações confidenciais são expostas, mais precisas e efetivas se tornam as tentativas de uso de engenharia social.

A fim de proteger os usuários contra a engenharia social, parte vital se torna a educação e treinamento. Funcionários devem ser ensinados a não clicar em *links* suspeitos e a proteger suas credenciais de *login*, tanto no trabalho quanto em casa. É importante que os usuários conheçam os sinais de um ataque de *phishing*, incluindo *e-mails* não solicitados, erros de ortografia e gramática e mensagens que solicitam informações confidenciais. Além disso, as empresas devem implementar políticas de senha forte e autenticação em dois fatores para proteger as credenciais de *login* dos usuários (Kaspersky, 2023a).

Conclusão

O investimento em educação por parte dos usuários, no contexto da segurança da informação, pode ser considerado o primeiro passo na busca pela confidencialidade, integridade e disponibilidade das informações sensíveis. O vazamento de dados de milhões de pessoas no Brasil, incluindo informações confidenciais, ressalta a necessidade de conscientização e capacitação dos usuários para lidar com ameaças como a engenharia social.

Diante do cenário atual em que os ataques cibernéticos estão cada vez mais frequentes e sofisticados, investir em educação e conscientização dos usuários, portanto, é essencial para fortalecer a segurança cibernética. A identificação precoce das possíveis ameaças é crucial para evitá-las. Com a implementação de medidas de proteção, como políticas de senha forte e autenticação em dois fatores, as organizações podem reduzir significativamente os riscos de violações de dados e proteger suas informações confidenciais. A educação dos usuários se torna, portanto, um componente vital no contexto da segurança da informação.

Referências

ANDRADE, Juliana. **Cibersegurança:** entenda os perigos do ambiente digital. Disponível em: https://forbes.com.br/forbes-tech/2020/11/ciberseguranca-entenda-os-perigos-do-ambiente-digital/. Acesso em: 22 jun 2023.

ARAÚJO LISBOA, Cícero; ZIEBELL DE OLIVEIRA, Guilherme. **O Conceito de dissuasão cibernética:** relevância e possibilidades. Oasis n° 35, p. 53-78, maio 2022.

BATISTELLA, Carla. **Confidencialidade, Integridade e Disponibilidade (CID)**. Disponível em: <Confidencialidade Integridade e Disponibilidade (CID) – (certifiquei.com.br)>. Acesso em: 23 jun 2023.

BRASIL. **Cartilha de gestão de segurança da informação**. Gabinete de Segurança Institucional, Brasília, DF, 21 dez 2022.

BRASIL. **Decreto nº 6.703, de 18 de dezembro de 2008.** Aprova a Estratégia Nacional de Defesa, e dá outras providências. Diário Oficial da União, Brasília, DF, 19 dez 2008. Seção 1, p. 4.

BRASIL. **Decreto nº 9.637 de 26 de dezembro de 2018**. Institui a Política Nacional de Segurança da Informação. Diário Oficial da União, Brasília, DF, 27 dez 2018.

BRASIL. **Diretriz Ministerial nº 0014, de 9 de novembro de 2009**. Dispõe sobre a integração e coordenação dos setores estratégicos da defesa. Ministério da Defesa, Brasília, DF, 9 nov 2009.

BRASIL. Ministério da Defesa. **MD31-M-08: Doutrina Militar de Defesa Cibernética**. 1. ed. Brasília, DF, 2014.

CASSIANI, Arthur Gonçalves *et al.* **O Papel da Defesa Nacional em Casos de Ataques Cibernéticos**: Uma Análise sobre a Necessidade de Protocolo(s) de Prevenção e Atuação. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/artigos/xvi_cadn/oa_papela_daa_defesaa_nacionala_ema_casosa_dea_ataquesa_ciberneticosa_umaa_analisea_sobrea_aa_necessidadea_dea_protocolos.pdf>Acesso em: 20 jun 2023.

CNN. **Uso de celulares revelou localização para ataque que matou dezenas de soldados russos**. Disponível em: <Uso de celulares revelou localização para ataque que matou dezenas de soldados russos (cnnbrasil.com.br)>. Acesso em: 22 jun 2023.

DA SILVA, Washington Rodrigues; NOGUEIRA, Jorge Madeira. Ataques cibernéticos e medidas governamentais para combatê-los. **Revista O Comunicante**. Brasília, v. 9, nº 1, p. 43-57, 2019.

DEBUSMANN, Bernd. **Como um militar de baixa patente de 21 anos conseguiu acesso a documentos 'ultrassecretos' dos EUA**. Disponível em: <Como um militar de baixa patente de 21 anos conseguiu acesso a documentos 'ultrassecretos' dos EUA- BBC News Brasil>. Acesso em: 24 jun 2023.

FEDERAL BUREAU OF INVESTIGATION (FBI). What we investigate: Cyber Crime. U.S. Government, U.S. Departament of Justice. 2018. Disponível em:<https://www.fbi.gov/investigate/cyber>. Acesso em: 24 jun 2023.

FORTINET. **Brasil é o segundo país que mais sofre ataques cibernéticos na América Latina**. Disponível em: < Brasil é o segundo país que mais sofre ataques cibernéticos na América Latina | Fortinet> Acesso em: 22 jun 2023.

G1. **Megavazamento de dados de 223 milhões de brasileiros**: o que se sabe e o que falta saber. Disponível em: <Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber | Tecnologia | G1 (globo.com)>. Acesso em: 24 jun 2023.

IBM. **O que é engenharia social?**. Disponível em: <https://www.ibm.com/br- pt/topics/social-engineering> Acesso em: 23 jun 2023.

KASPERSKY. **Engenharia social – definição.** Disponível em: < https://www.kaspersky.com.br/resource-center/definitions/what-is-social-engineering> Acesso em: 23 jun 2023a.

KASPERSKY. **O que é spear phishing?**. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/spear-phishing> Acesso em: 23 jun 2023b.

KLUSAITÈ, Laura. **O que é um ataque cibernético?** Disponível em: <https://nordvpn.com/pt-br/blog/o-que-e-ataque-cibernetico/> Acesso em: 22 jun 2023.

SINGER, Peter Warren; FRIEDMAN, Allan. **Cybersecurity and cyberwar:** what everyone needs to know. 2014. Segurança e Guerra cibernéticas: o que todos precisam saber. Tradutor Geraldo Alves Portilho Junior. Rio de Janeiro: Biblioteca do Exército Editora, 2017.

SHRM. **The Weakest Link in Cybersecurity**. Disponível em: <The Weakest Link in Cybersecurity (shrm.org)>. Acesso em 23 jun 2023.

SOLDATELI, Fernanda Lopes. **Não é vazamento! Dados militares são esquecidos em dispositivos**. Disponível em: https://olhardigital.com.br/2022/12/27/seguranca/nao-e-vazamento-dados-militares-sao-esquecidos-em-dispositivos/. Acesso em: 23 jun 2023.