CIBERSEGURANÇA[1] UMA QUESTÃO PARA A LIDERANÇA ESTRATÉGICA ?

Wilson Mendes Lauria

"I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."

Robert S. Miller III
Director FBI 2001 – 2013

CONSIDERAÇÕES INICIAIS

Em 1986, no momento em que a Internet começava a se tornar popular, hackers alemães invadiram os computadores do *Lawrence Berkeley National Laboratory* e de outras instituições norte-americanas para acessar, de forma ilegal, dados sensíveis sobre projetos estratégicos de defesa. Aquele incidente ficou conhecido como o *Cuckoo's Egg*[2] e foi percebido como a primeira ação – realizada no domínio cibernético [3] – com a intenção de se obter informações classificadas.

A caixa de pandora digital foi aberta em 2007, quando uma série de ataques cibernéticos inviabilizou operacionalmente o governo da Estônia. A partir de então, eventos como o Stuxnet (2010), o WannaCry (2013) e o NotPetya (2017) demonstraram as vulnerabilidades de uma sociedade completamente conectada e dependente de seus ativos digitais[4].

Imagem: AdobeStock.com

Em 2020, a pandemia do COVID – 19 ampliou os holofotes sobre o tema cibersegurança. O aumento da exposição digital de pessoas e instituições resultou em consequências inesperadas e indesejadas. Em 01 de Abril de 2020, o FBI emitiu o alerta I-040120-PSA[5] informando que atores cibernéticos estavam aproveitando aquela situação para perpetrar crimes.

De acordo com a TrendMicro, no 1º quadrimestre de 2020, foram detectados mais de 900.000 emails spams, 703 arquivos *malware* e 48.000 URLs maliciosos relacionados ao tema COVID – 19. Já no 3º quadrimestre do mesmo ano, foram identificados 3.818.307 emails spams, 15.513 arquivos malware e 1.025.301 URLs maliciosos vinculados à pandemia , apontando para outra pandemia[6], desta vez digital, concomitante à sanitária.

Face à crescente dependência que temos dos meios digitais, e ao inerente crescimento do risco de incidentes digitais, o que o líder de uma instituição, independente de sua expertise profissional, necessita conhecer sobre cibersegurança?

Esta é a questão-chave que será endereçada neste trabalho.

CIBERSEGURANÇA – UMA QUESTÃO DE RESILIÊNCIA

Segundo a Estratégia de Cibersegurança da Finlândia, "Segurança cibernética é o estado final desejado no qual o domínio cibernético é confiável e tem o seu funcionamento assegurado". Para a *ISO*, segurança cibernética é definida como "a preservação da confidencialidade, da integridade e da disponibilidade da informação no espaço cibernético"[7] .

Integrando aquelas duas abordagens, pode-se definir, para este trabalho, cibersegurança como o estado final desejado no qual o ecossistema digital tem o seu funcionamento assegurado e a confidencialidade, a integridade e a disponibilidade do dado digital está preservada.

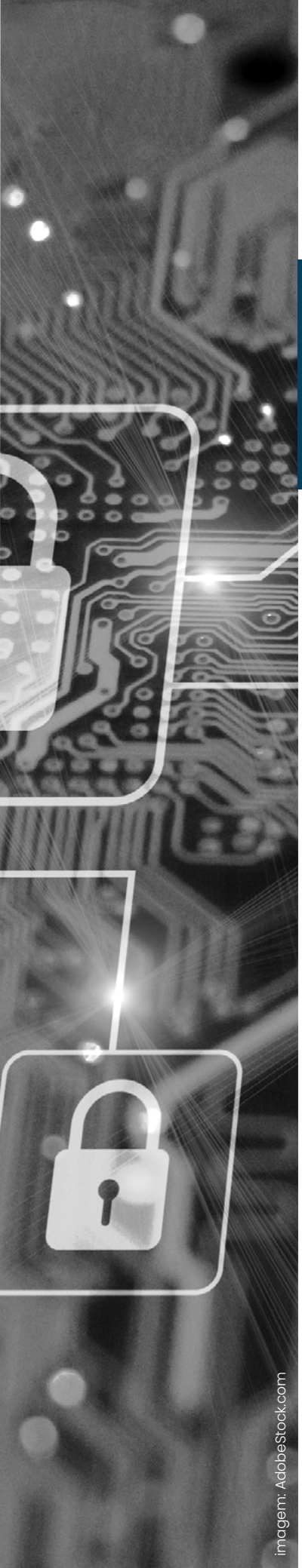


imagem: AdobeStock.com

De acordo com o entendimento de Rothrock (2018)[8] , a cibersegurança possui duas camadas – a defesa e a resiliência digital – que, em uma visão esquemática, podem ser representadas como dois círculos concêntricos.

A defesa digital compreende um conjunto de táticas, técnicas e procedimentos que tentarão impedir um acesso não autorizado ao ecossistema em questão constituindo, assim, a sua primeira linha de defesa.

Aceitando o pressuposto de que não existe sistema defensivo inexpugnável, o propósito real da defesa digital é iludir, testar e desgastar o agressor levando-o, se possível antes de concretizar a intrusão, a ultrapassar o ponto culminante do ataque [9] obrigando-o a rever a sua intenção ofensiva.

Incidentes cibernéticos são inevitáveis, e, portanto, uma solução de segurança - não equilibrada - que priorize em sua concepção a defesa digital não apresentará, em campo, uma resposta que assegure um retorno sobre o investimento (ROI) vantajoso para o seu patrocinador.

Independente da sua natureza, um sistema para ser resiliente tem que ter condições de assegurar tanto a continuidade da sua operação em condições degradadas como a sua recuperação plena após a contenção daquele evento desfavorável.

A *IBM* indica que um vazamento de dados demora, em média, 207 dias para ser identificado e 73 dias para ser contido[10] . A capacidade de manter a continuidade da operação nesse ambiente de ameaça persistente é vital para a sobrevivência do negócio.

Sobre a recuperação do sistema, é relevante ressaltar que recuperar não significa retornar exatamente ao *status quo ante bellum*. O estado final desejado pós-incidente é uma situação evolutiva na qual os ensinamentos colhidos tenham sido aproveitados.

Em *Develop Your Cyber Resilience Plan*[11] , há um modelo pragmático com vários insights para a inserção da resiliência nas estratégias de segurança cibernética corporativas.

Somente a sinergia entre a defesa digital e a resiliência digital proporcionará uma resposta vencedora para o desafio que é prover segurança no volátil, incerto, complexo e ambíguo ecossistema digital do século XXI.

Embora dissuasão cibernética seja um tema bastante controverso, como efeito de segunda ordem, um aparato defensivo robusto pode, inclusive, dissuadir[12] o agressor a agir.

Utilizando a metodologia *Cyber Kill Chain*[13] , desenvolvida em 2014 por um grupo de cientistas da *Lockheed Martin*, fica fácil entender a relação defesa – resiliência.

A *Cyber Kill Chain* apresenta o racional de um ataque cibernético. A sua utilidade está amparada pelo argumento que fez a glória dos grandes Capitães: antever os passos de seu oponente.

De acordo com aquele modelo, uma ação cibernética ofensiva tem sete fases distintas que são:

1ª Fase Reconhecimento (Identificação de Vulnerabilidades);

2ª Fase Obtenção do Artefato (Aquisição ou Desenvolvimento);

3ª Fase Entrega do Artefato (Intrusão);

4ª Fase Exploração da Vulnerabilidade do Ecossistema Alvo;

5ª Fase Instalação do Artefato no Ecossistema Alvo (Desdobramento);

6ª Fase Abertura de Canal de Comando e Controle Remoto Artefato – Atacante; e

7ª Fase Ação no Objetivo.

Analisando a *Cyber Kill Chain* com a lente proposta por Rothrock (2018) observa-se que:

- as ações de defesa digital ocorrem entre a **1ª Fase** – Reconhecimento e **4ª Fase** – Exploração da Vulnerabilidade do Ecossistema Alvo;
- as atividades que conferem Resiliência Digital são desencadeadas, prioritariamente, entre a **4ª Fase** – Exploração da Vulnerabilidade do Ecossistema Alvo e a **7ª Fase** – Ação no Objetivo; e
- na **4ª Fase** da *Cyber Kill Chain* a sobreposição entre as camadas defesa e resiliência confere uma vantagem competitiva ao defensor.

Em face da situação apresentada, pode-se inferir que na **4ª Fase**, a superioridade da defesa sobre o ataque – conceito clausewitziano[14] ratificado para o domínio digital por Clarke e Knake (2019)[15] – pode levar o agressor, que já vem com algum "desgaste", a ultrapassar o ponto culminante do ataque compelindo-o a desistir. Esse entendimento teórico da dinâmica ataque - defesa, não pode ser ignorado pelos arquitetos dos sistemas de segurança cibernética.

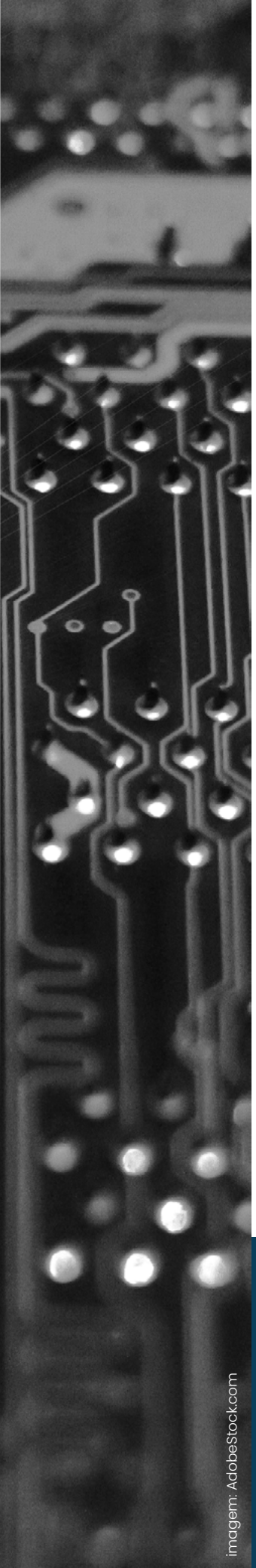


imagem: AdobeStock.com

O ECOSSISTEMA DIGITAL E A CULTURA DE SEGURANÇA

Em seu último livro, Klaus Schwab[16] apresentou uma atualização do modelo econômico, de sua autoria, denominado *Stakeholder Capitalism*.

Na primeira versão, publicada em 1971, em livro *Modern Company Management in Mechanical Engineering*, as Empresas ocupavam o núcleo do ecossistema.

Hoje, Schwab o redesenha com as Pessoas (indivíduos que ocupam aquele espaço) e o Planeta (ambiente em que vivemos) como core ao redor do qual orbitam *stakeholders* (Empresas, Países, ONGs e outros), com seus diferentes e diversos objetivos, mas com o compromisso comum de assegurar a sustentabilidade e a governança daquela construção (Figura 1).

Figura 1 – Ecossistema Econômico do Século XXI

Fonte: Adaptado, por este autor, de Schwab e Vanham (2021)

Tendo Schwab e Vanham (2021) como *benchmark* correlato, exercitamos uma modelagem do ecossistema digital do Século XXI.

Assim, imaginamos os dois ecossistemas como sendo bastante semelhantes. O que muda é o ambiente onde os *stakeholders* se relacionam. A alteração se dá no núcleo, onde o planeta – ambiente físico em que vivemos, convivemos e temos os nossos conflitos – é substituído por uma arena de interação virtual que é o espaço cibernético.

Nunca é demais lembrar que o espaço cibernético é uma construção tecnológica, feita pelo homem, no contexto das 3ª e 4ª Revoluções Industriais.

Como pode ser depreendido da Figura 2, o ecossistema digital é composto pelas dimensões Humana (Pessoas), Tecnológica (Espaço Cibernético) e Governança (*Stakeholders*). Para a segurança cibernética, aquelas são pilares estruturais que orientarão a concepção de políticas, táticas e estratégias.

Figura 2 – Organização do Ecossistema Digital do Século XXI

Fonte: Adaptado, por este autor, de Schwab e Vanham (2021)

Em seu artigo *Social Engineering Explained: The Human Element in Cyberattacks*[17], Lillian Ablon sugere que o ser humano é o fator mais imprevisível e vulnerável do ecossistema digital. Para aquela autora, a engenharia social é o caminho mais comum para a obtenção de acesso, não autorizado, às redes e aos dados privados.

O argumento de Ablon (2015) é ratificado por Rothrock (2018) que afirma ser o indivíduo por trás de um monitor ou operando um *smartphone* a maior vulnerabilidade de uma rede digital.

Em tempos de COVID-19, com as pessoas realizando as suas atividades profissionais de forma remota e a indesejada prática do uso corrente de equipamentos de caráter pessoal, sem os devidos protocolos de controle, em atividades institucionais, agravou exponencialmente a realidade de risco.

A maneira de se trabalhar a fragilidade do elo humano no ecossistema digital, e ter como resultado a edificação de um "*firewall* humano", é por intermédio do desenvolvimento de uma cultura de segurança[18].

Mudança cultural é um empreendimento de longo prazo que pressupõe a desconstrução do *status quo* e a implantação de novas práticas comportamentais. Desafio de tal monta, impõe o engajamento da alta hierarquia institucional. Naquele universo, um Líder com perfil transformador, que catalise e influencie os demais colaboradores rumo a condutas mais maduras e

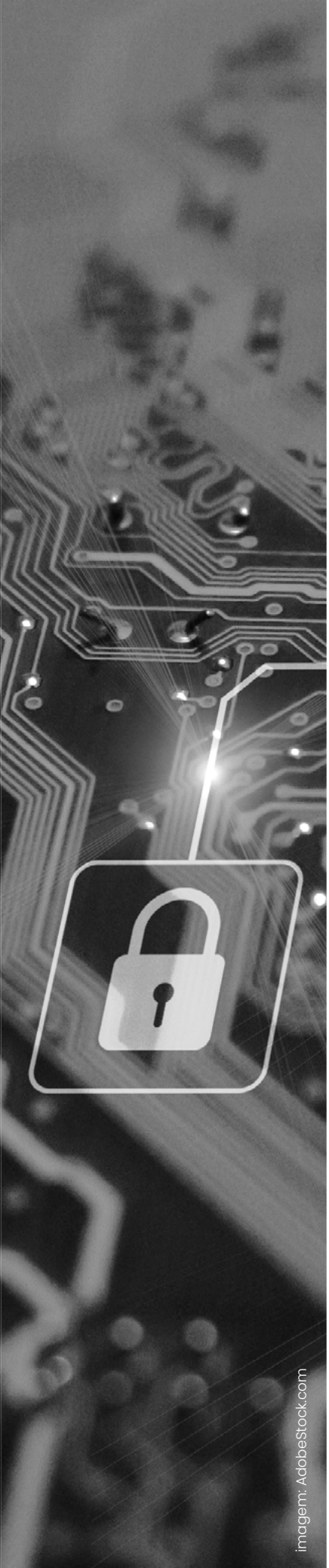


imagem: AdobeStock.com

propósitos consequentes é fator crítico de sucesso. Para John Kotter, gerentes fazem sistemas funcionar enquanto líderes constroem sistemas novos ou transformam os antigos.

COMO FAZER ISSO?

Em *The Unadressed Gap in Cybersecurity: Human Performance*[19], Stephen Wilson reconhece os limites da tecnologia e propõe o modelo denominado *High-Reliability Cybersecurity Operations* (HRCO)[20], para aquele fim.

Também, na camada operacional, há ações de capacitação (treinamentos) com impacto muito rápido e de excelente custo benefício como nos demonstra o resultado da aplicação de um treinamento *anti-phishing* publicado no *Phishing by Industry 2020 Benchmarking Report*[21]. Segundo o que foi apurado, inicialmente, sem qualquer tipo de treinamento específico 37,9 % do universo pesquisado clicou em um *link* ou respondeu a uma solicitação maliciosa. Após um treinamento de 90 dias, aquele número percentual reduziu para 14,1%. Ao término de um ciclo de capacitação de 12 meses, apenas 4,7% caiu naquela abordagem fraudulenta. Em números percentuais, ocorreu uma melhoria de 87% no desempenho daquele grupo.

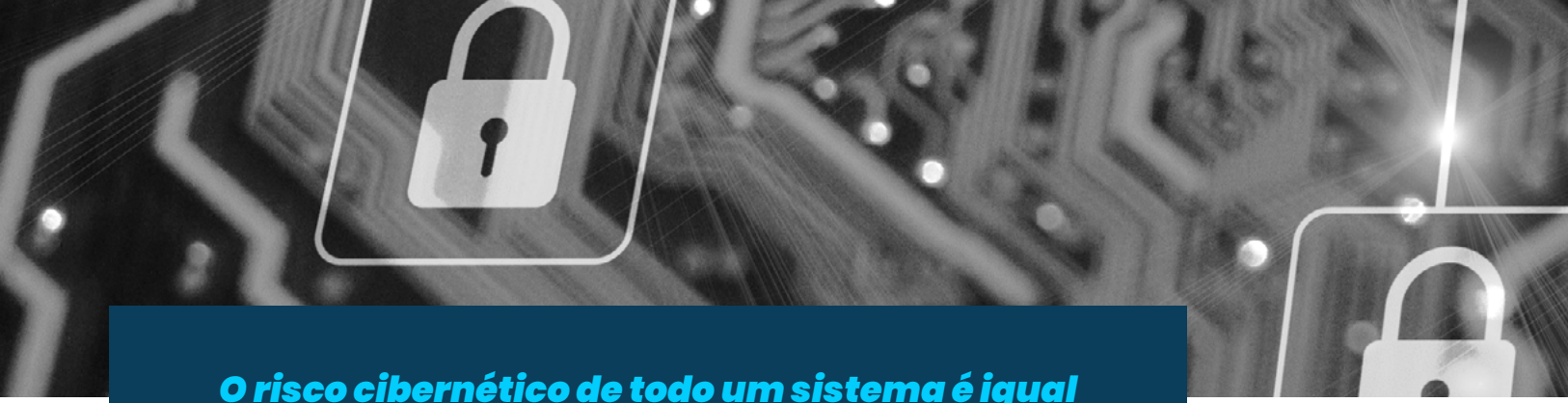
Considerando que, segundo o *Microsoft Digital Defense Report*[22], 90% dos ataques cibernéticos têm o seu início com a aplicação da técnica de *phishing*, o impacto positivo de um treinamento específico sobre a cultura de segurança é inquestionável.

TAKEAWAYS – UMA LISTA NÃO-EXAUSTIVA

O que o líder de uma instituição, independente de sua *expertise* profissional, necessita conhecer sobre cibersegurança?

Antes de qualquer coisa, ter um conceito objetivo, para compartilhar com os seus colaboradores, para o termo cibersegurança.
Definir o que está sendo tratado é o ponto origem para qualquer empreendimento de sucesso, principalmente, quando se trata sobre algo recente sobre o qual não há uma definição consensual como é o tema em comento.

Cibersegurança é um empreendimento de caráter público-privado que envolve todos os stakeholders do ecossistema digital. Resiliência é o seu core e *Develop Your Cyber Resilience Plan*[23] apresenta um modelo pragmático para a sua construção.



O risco cibernético de todo um sistema é igual ao da sua parte mais vulnerável.

O incidente na gigante do varejo americano *Target* – onde o acesso à base de dados da empresa foi efetivado por intermédio de uma ação de *phishing* sobre um de seus prestadores de serviço – demostrou aquela verdade.

Neste aspecto, apenas como um exemplo, a partir de 2020, a fim de elevar o grau de segurança de sua cadeia de suprimento, o U.S. Department of Defense (DoD) tem exigido de seus fornecedores de bens e serviços a conformidade em relação ao Cybersecurity Maturity Model Certification (CMMC)[24] .

Não há uma solução única ou específica que possa garantir risco cibernético zero. Em uma realidade onde os ativos digitais, segundo a Forbes constituem 85% do valor de uma empresa[25], aquele paradigma de segurança passa a ser um desafio de gestão de risco sistêmico, pois, além de ser inevitável, um incidente cibernético pode comprometer a sobrevivência da instituição, portanto um tema afeto aos conselhos empresariais. Como esse tema é percebido no Brasil?[26]

Não existe prontidão sem treinamento. Ter um plano de contingência não é suficiente, os procedimentos ali descritos devem ser treinados e, principalmente, avaliados. As pessoas tem que saber, exatamente, o que fazer. Quem é o comandante na cena? Quem fala com a mídia? Qual a mensagem que deve ser transmitida aos acionistas? Em caso de crise, não pode existir esse tipo de dúvida.

James Cummings e Paul Mee[27] destacam a utilidade de exercícios cibernéticos, os chamados jogos de guerra em jargão militar, para identificar e mitigar vulnerabilidades operacionais. Jogos são ferramentas de baixo custo que, de acordo com o cenário elaborado, podem trabalhar questões políticas, estratégicas e táticas. Hoje, o uso desse tipo de ferramenta tem sido uma prática cada vez mais comum no ambiente corporativo.

Como último insight, afirmo que programas e ações orientadas para o desenvolvimento/aperfeiçoamento de uma cultura de segurança cibernética trazem impacto rápido, são perenes e apresentam um excelente retorno sobre o investimento realizado.

O principal objetivo desse artigo é despertar o interesse do leitor sobre o tema. Poucos questionarão a sua contemporaneidade e relevância. Se isso é verdade, porque incidentes cibernéticos continuam ocorrendo?

Wilson Mendes Lauria
General do Exército Brasileiro

Oficial General (R1) do Exército Brasileiro, com mais de 37 anos de serviço, desenvolveu atividades nos domínios da política, tática e estratégia. Na área de Inteligência, chefiou a Seção de Acompanhamento da Conjuntura Internacional do Centro de Inteligência do Exército. Foi Adido de Defesa, Naval e do Exército Brasileiro na República da Guiana. Integrou o Estado-Maior do Exército, chefiando a Seção de Assuntos Internacionais onde desenvolveu projetos de cooperação com Exércitos de mais de 50 países. Comandou a 2ª Brigada de Cavalaria Mecanizada e, como última comissão, dirigiu o Campus Brasília da Escola Superior de Guerra. Graduou-se nos cursos militares regulares brasileiros, bem como no Canadian Forces College, no United States Army War College e na Escola Superior de Guerra.

Imagem: AdobeStock.com

NOTAS E REFERÊNCIAS

1 Neste texto, os termos Cibersegurança e Segurança Cibernética serão utilizados como sinônimos.

2 Para informações mais detalhadas sobre aquele incidente consultar Stoll, Cliford. *The cuckoo's egg: tracking a spy through the maze of computer espionage.* New York, NY: Doubleday, 1989.

3 Domínio Cibernético é o ambiente construído pelo homem, sem fronteiras físicas, constituído por ativos digitais – tanto físicos (hardwares, redes e outros) quanto não-físicos (*softwares*, dados e outros) – onde ocorre a interação entre seus usuários. No presente texto, os termos Domínio Cibernético e Espaço Cibernético serão utilizados como sinônimos.

4 Para um detalhamento sobre os incidentes cibernéticos que ocorreram entre 2008 e 2018 consultar Sanger, David. *The perfect weapon: war, sabotage, and fear in the cyber age.* Broadway Books, 2019.

5 https://www.ic3.gov/Media/Y2020/PSA200401

6 https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

7 Dados obtidos na publicação *Compilation of Existing Cybersecurity and Information Security Related Definitions*, disponível em https://www.newamerica.org/cybersecurity-initiative/policy-papers/compilation-of-existing-cybersecurity-and-information-security-related-definitions/

8 Rothrock, Ray. *Digital resilience: is your company ready for the next cyber threat?* Amacom, 2018.

9 Segundo Clausewitz, o Ponto Culminante do Ataque é o momento em que o atacante, já desgastado, não tem mais condições para prosseguir na ofensiva. Para maiores detalhes sobre aquele conceito consultar o Capítulo 5. O Ponto Culminante do Ataque, do Livro VII. O Ataque de On War.

10 Dado extraído do documento *Cost of Data Breach Report 2020* disponível em https://www.ibm.com/security/data-breach

11 Disponível em https://sloanreview.mit.edu/article/develop-your-cyber-resilience-plan/

12 A dissuasão aqui tratada é o que Joseph Nye, em seu artigo *Deterrence and Dissuasion in Cyberspace*, define como deterrence by denial onde o agressor não age, pois a sua expectativa de sucesso é muito baixa. Disponível em https://www.belfercenter.org/publication/deterrence-and-dissuasion-cyberspace

13 Para informações mais detalhadas sobre essa metodologia consultar *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains*, disponível em https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

14 Para uma melhor explicação sobre esse conceito, favor consultar o item 2. Vantagens da Defesa, do Capítulo 1. Ataque e Defesa, do Livro VI. Defesa de On War.

15 Clarke, Richard; Knake, Robert. *The fifth domain: defending our country, our companies and ourselves in the age of cyber threats*. Penguin Press, 2019.

16 Schwab, Klaus; Vanham, Peter. *Stakeholder capitalism: a global economy that works for progress, people and planet*. WEF, 2021.

17 Disponível em https://www.rand.org/blog/2015/10/social-engineering-explained-the-human-element-in-cyberattacks

18 De acordo com *The 7 Dimensions of Security Culture*, Cultura de Segurança deve ser entendida como um conjunto de ideias, costumes e procedimentos de uma pessoa ou de um grupo que os livre de perigos ou ameaças. Disponível em https://get.clt.re/seven-dimensions-security-culture/

19 Disponível em https://sloanreview.mit.edu/article/the-unaddressed-gap-in-cybersecurity-human-performance/

20 O *High-Reliability Cybersecurity Operations* (HRCO) é a adaptação do conceito de *High-Realibility Organization* (HRO), que teve a sua origem no *United States' Naval Nuclear Propulsion Program*, para o tema cibersegurança. HRO são organizações que realizam atividade de alto risco e se submetem a protocolos operacionais muitos restritos para assegurar um pequeno número de falhas. Em síntese, são organizações que cultivam a mentalidade de Zero Erro.

21 Disponível em https://info.knowbe4.com/phishing-by-industry-benchmarking-report

22 Disponível em https://www.microsoft.com/en-us/download/details.aspx?id=101738

23 Disponível em https://sloanreview.mit.edu/article/develop-your-cyber-resilience-plan/

24 Disponível em https://www.acq.osd.mil/cmmc/

25 Disponível em https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/?sh=38cb74f64947

26 Na pesquisa realizada para a redação deste texto, não identifiquei nos programas para formação/ treinamento de Conselheiros disponíveis no mercado doméstico qualquer menção sobre o tema Cibersegurança.

27 Disponível em https://sloanreview.mit.edu/article/is-your-company-ready-for-a--cyberattack/

LEITURA RECOMENDADA

CLARKE, Richard; KNAKE, Robert. *The fifth domain*: *defending our country, our companies and ourselves in the age of cyber threats.* Penguin Press, 2019.

ROTHROCK, Ray. *Digital resilience*: *is your company ready for the next cyber threat?* Amacom, 2018.

SANGER, David. *The perfect weapon*: *war, sabotage, and fear in the cyber age*. Broadway Books, 2019.