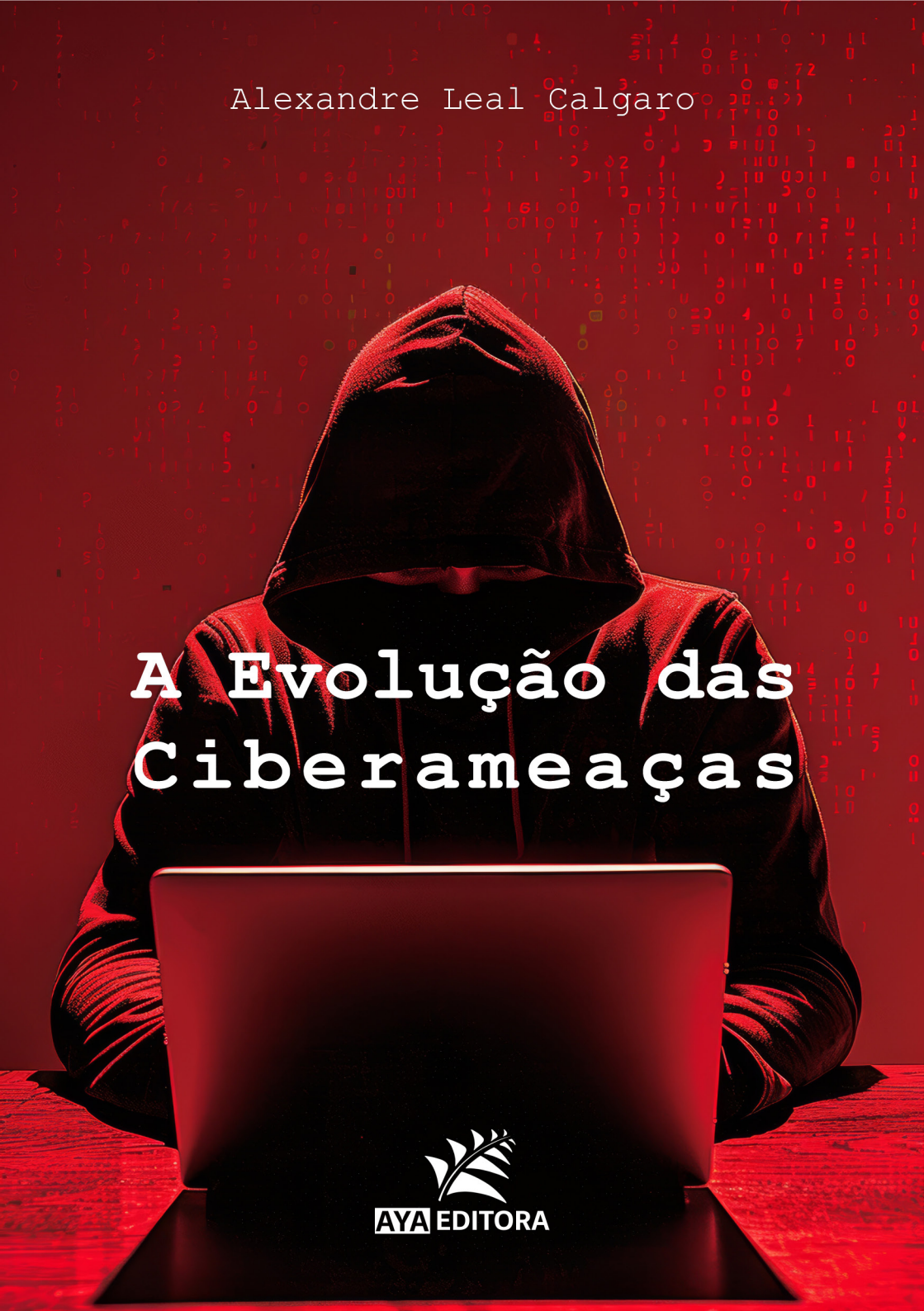
Alexandre Leal Calgaro

A Evolução das Ciberameaças



AYA EDITORA

A Evolução das Ciberameaças

Alexandre Leal Calgaro

A Evolução das Ciberameaças

AYA EDITORA

Direção Editorial
Prof.° Dr. Adriano Mesquita Soares
Autor
Alexandre Leal Calgaro
Capa
AYA Editora©
Revisão
Priscilla Teodora Gonçalves de Moura

Executiva de Negócios
Ana Lucia Ribeiro Soares

Produção Editorial
AYA Editora©
Imagens de Capa
br.freepik.com

Área do Conhecimento
Ciências Sociais Aplicadas

Conselho Editorial

C151 Calgaro, Alexandre Leal

A evolução das ciberameaças [recurso eletrônico]. / Alexandre Leal Calgaro. -- Ponta Grossa: Aya, 2024. 34 p.

Inclui biografia
Inclui índice
ISBN: 978-65-5379-599-0
DOI: 10.47573/aya.5379.1.306

1. Cibernética. 2. Computadores - Medidas de segurança. 3. Redes de computadores - Medidas de segurança. I. Título

CDD: 003.5

Ficha catalográfica elaborada pela bibliotecária Bruna Cristina Bonini - CRB 9/1347

International Scientific Journals Publicações de Periódicos e Editora LTDA

AYA Editora©
CNPJ: 36.140.631/0001-53
Fone: +55 42 3086-3131
WhatsApp: +55 42 99906-0630
E-mail: contato@ayaeditora.com.br
Site: https://ayaeditora.com.br
Endereço: Rua João Rabello Coutinho, 557
Ponta Grossa - Paraná - Brasil
84.071-150

SUMÁRIO

APRESENTAÇÃO

Este livro aborda de forma clara e direta as ciberameaças que se tornaram um dos principais desafios da era digital. Com uma análise atualizada, os autores exploram os tipos mais comuns de ataques, como malware, ransomware e phishing, e discutem estratégias de defesa, destacando a importância da ciberhigiene e da educação em segurança digital.

Os leitores encontrarão explicações acessíveis sobre os riscos da segurança cibernética e exemplos práticos que ilustram os impactos dessas ameaças. É uma leitura essencial para profissionais de TI, gestores, estudantes e todos que buscam entender melhor os desafios da segurança digital nos dias de hoje.

"Ciberameaças: Desafios e Estratégias no Século XXI" é um guia indispensável para enfrentar os riscos do mundo conectado, oferecendo conhecimento para proteger sistemas e informações.

Boa leitura!

INTRODUÇÃO

À medida que se avança o século XXI, a *internet* e as tecnologias digitais tornaram-se fundamentais em todos os aspectos da vida humana. Desde comunicações pessoais e transações comerciais até infraestrutura crítica e segurança nacional, a dependência da tecnologia digital continua crescendo. No entanto, com essa crescente dependência, surgem também uma variedade de vulnerabilidades que podem ser exploradas por atores mal-intencionados. Essas explorações são conhecidas como ciberameaças, que se manifestam de diversas formas e têm potencial para causar danos significativos.

As Ciberameaças variam desde *malwares*, que podem infectar e tomar controle de dispositivos individuais, até ataques de negação de serviço distribuído (DDoS) que podem derrubar redes inteiras. Além disso, a exploração de vulnerabilidades em *software* e *hard*ware continua a ser um campo fértil para ataques, exigindo vigilância e atualizações constantes de segurança por parte de usuários e administradores de sistema.

Este livro explora a natureza multifacetada das ciberameaças, destacando os tipos de ameaças mais prevalentes. Os ataques podem ser motivados por ganhos

financeiros, como no caso de *ransomware*, ou podem ter objetivos mais destrutivos, como o vandalismo digital ou a espionagem corporativa e estatal.

A prevenção e a defesa contra ciberameaças requerem uma abordagem que envolve tanto tecnologia quanto comportamento humano. A conscientização e a educação em cibersegurança são fundamentais para fortalecer a primeira linha de defesa: os usuários e deve ser realizadas, desde práticas básicas de higiene digital, como manter *software* atualizado e utilizar medidas de segurança robustas, até estratégias mais complexas de defesa cibernética implementadas por organizações, todos os aspectos são cruciais para uma proteção efetiva.

Através de uma análise das tendências atuais e emergentes em ciberameaças, visa-se oferecer uma compreensão profunda e prática das dinâmicas de cibersegurança, bem como das estratégias necessárias para enfrentar esses desafios crescentes. Com uma abordagem baseada em evidências e melhores práticas, busca-se inspirar e informar aqueles que estão na linha de frente da defesa cibernética, desde indivíduos até grandes corporações e entidades governamentais.

A HISTÓRIA DA INTERNET

A “Internet” é definida como uma rede global de computadores que conecta dispositivos pessoais, entidades de pesquisa, instituições culturais e militares, bibliotecas e empresas de diversos tamanhos, possibilitando a troca virtual de informações e comunicações.

Em 1957, a União Soviética lançou o Sputnik, seu primeiro satélite, levando o então presidente dos Estados Unidos, John Kennedy, a prometer não apenas enviar um americano à lua, mas também desenvolver um sistema de defesa invulnerável. Para apoiar esse objetivo e impulsionar o avanço tecnológico do país, foi estabelecida a Agência de Projetos de Pesquisa Avançada (ARPA) (Wendt; Jorge, 2012).

Com a formação da Administração Nacional da Aeronáutica e Espaço (NASA) em 1958, a ARPA teve que redefinir seu foco de pesquisa. Anos mais tarde, a ARPA visava construir uma rede que permitisse a comunicação de dados entre computadores distantes, resultando na criação da ARPANET em 1969. Esta rede utilizava uma tecnologia de troca de pacotes que se tornaria a base da Internet moderna (Wendt; Jorge, 2013).

A ARPANET inicialmente conectou várias universidades na Califórnia e em Utah e em 1972, a primeira demonstração pública da rede demonstrou funcionalidades como login remoto e e-mail. Em 1973, ocorreu a primeira conexão internacional, ligando a Inglaterra e a Noruega. No final dos anos 70, o protocolo de comunicação de pacotes foi alterado de *Network Control Protocol* (NCP) para *Transmission Control Protocol/Internet Protocol* (TCP/IP), facilitando a interconexão de redes independentes. (Guisso, 2017, p. 14).

Um marco importante ocorreu no final dos anos 80 com a criação da *World Wide Web* (WWW) por *Tim Berners-Lee*, que também desenvolveu o protocolo HTTP e a linguagem HTML. Em 1984, a Fundação Nacional de Ciências (NSF) estabeleceu a NSFNET, focando na segurança da rede. Com o declínio da ARPANET em 1990, a NSFNET tentou comercializar sua tecnologia, apoiando fabricantes de computadores nos EUA, mas foi desativada em 1995 devido à prevalência do acesso à Internet, levando ao surgimento De Redes Privadas Operadas Por Diversos Provedores (Guisso, 2017, p. 15).

CIBERAMEAÇAS

Recentemente, tem-se intensificado o debate sobre as ciberameaças. Nações têm adotado posturas e elaborado estratégias para antecipar essas ameaças e para salvaguardar e instruir o público sobre os perigos potenciais.

As ciberameaças são comumente ligadas ao cibercrime, definido como, **um termo que descreve a violência abaixo do nível de um conflito armado entre estados, envolvendo atores não estatais e podendo incluir interrupções em infraestruturas críticas ou atividades de desestabilização política.**

Um usuário típico da *internet* pode encontrar três principais tipos de riscos de segurança da informação. O primeiro é o furto de dados, que pode expor informações pessoais ou estratégicas (Amoroso, 2011).

O segundo risco é a utilização indevida de credenciais, que pode resultar na destruição ou modificação de dados pessoais. O terceiro risco é a apropriação de recursos, como o controle das finanças de um indivíduo (Lewis, 2014).

Para identificar as ameaças específicas abordadas e analisadas nesta dissertação, foi utilizado o Relatório de Ciberameaças da Agência Europeia para a Segurança das Redes e da Informação (ENISA). Este relatório detalha as 15 principais ciberameaças que impactaram os usuários da *internet* entre 2015 e 2016, fornecendo um panorama das ameaças mais frequentes e suas tendências, além de uma breve descrição de cada uma delas. É importante entender que essas ameaças frequentemente não ocorrem isoladamente, mas podem ser catalisadoras para outras ameaças.

As 15 principais ciberameaças são:

Malware - Representa *softwares* prejudiciais que podem se espalhar pela rede, atuar como um vírus e orientar as vítimas sobre ações pós-infecção. O malware pode causar perda de dados e disfunções nos dispositivos.

Ataques baseados na Web - Exploram falhas em componentes e extensões web, usando-os como entradas para comprometer servidores ou *sites*. Usuários podem ser alvo em *sites* comprometidos ou alterados, com alguns grupos sendo mais visados.

Ataques a Aplicações Web - Relacionam-se com ataques baseados na web, mas originam-se principalmente de aplicações web ou móveis. Aplicações públicas são alvos comuns, e ameaças nesse ambiente continuam a proliferar e compartilhar vulnerabilidades.

Ataques de Negação de Serviço (DoS) - Miram em servidores web ou outros componentes conectados à *internet*. Utilizando múltiplos computadores, os atacantes sobrecarregam a conexão da vítima, inundando-a com excesso de dados e desativando o sistema.

Botnets - Conhecidos como “computadores zumbis”, assumem o controle dos dispositivos de usuários, muitas vezes sem que estes percebam que seus dispositivos estão ou estiveram envolvidos em botnets. Botnets facilitam outros crimes cibernéticos, inclusive enganando controles de segurança como filtros de spam.

Phishing - Uma das técnicas mais refinadas de engenharia social, utiliza e-mails que parecem ser de fontes confiáveis. Os e-mails não são danosos por si só, mas induzem à abertura de páginas maliciosas, inserção de credenciais ou transferência de fundos.

Spam - Embora não seja imediatamente danoso, o spam é um método comum para disseminar malware. Pode induzir as vítimas a abrir anexos suspeitos ou clicar em URLs prejudiciais, comprometendo sua segurança.

Ransomware - Um tipo específico de malware que visa extorquir dinheiro ao bloquear dispositivos ou criptografar dados das vítimas. As opções são pagar o resgate, geralmente em criptomoeda, ou tentar descriptografar os dados.

Ameaças Internas - Podem ser acidentais ou intencionais. Ameaças internas acidentais podem incluir manipulação inadequada de dados ou uso de *hard*ware não autorizado. As ameaças internas intencionais são frequentemente motivadas por ganhos financeiros.

Manipulação Física - Embora não diretamente ligada à segurança da informação, a perda, roubo ou dano de dispositivos pode ter consequências graves como vazamento de informações ou violação de dados. Fraudes com cartões de crédito são um exemplo comum de manipulação física.

Kits de Exploração - Visam identificar vulnerabilidades ou falhas de segurança para espalhar malware. Oferecem "*crimeware-as-a-service"* (CaaS), permitindo que indivíduos paguem para disseminar malware em *sites* específicos.

Violações de Dados - Geralmente resultam do roubo de credenciais, podendo desencadear um efeito cascata de violações. Credenciais comprometidas são frequentemente vendidas a baixo custo no mercado negro e usadas para disseminar phishing e spam.

Roubo de Identidade - Um caso especial de violação de dados, ocorre quando cibercriminosos se apoderam de credenciais importantes, como informações financeiras ou de saúde, causando danos significativos às vítimas.

Fugas de Informação - Acesso não autorizado a dados e informações confidenciais, seja por acidente ou intencionalmente. Fugas intencionais são geralmente mais prejudiciais em termos de impacto.

Ciberespionagem - Predominantemente realizada entre Estados, utiliza outros tipos de crimes cibernéticos como meio. Caracteriza-se pela criação estratégica de vantagens e desvantagens entre atores estatais.

Infecção por Malware

Os códigos maliciosos, conhecidos como malware, são programas projetados especificamente para realizar atividades prejudiciais em dispositivos computacionais, como desktops, servidores, *smartphones* e tablets. A cartilha do Centro de Estudos, Resposta e Tratamentos de Incidentes de Segurança no Brasil (CERT.br) detalha várias maneiras pelas quais o malware pode infectar ou comprometer um computador:

- Explorando vulnerabilidades em *softwares* instalados;
- Ativando-se automaticamente a partir de mídias removíveis infectadas, como pen-drives;
- Acessando páginas da web mal-intencionadas com navegadores vulneráveis;
- Por meio de atacantes que, após invadir o computador, inserem arquivos com códigos

maliciosos;

- Executando arquivos que já estavam infectados, obtidos por anexos de e-mails, através de mídias removíveis, em páginas da web ou diretamente de outros computadores via compartilhamento de recursos.

Uma vez instalado, o malware pode acessar e manipular dados armazenados no dispositivo, executando ações em nome do usuário conforme as permissões concedidas, operando em benefício do cibercriminoso. As principais motivações por trás desses ataques incluem ganhos financeiros, roubo de informações confidenciais, vandalismo e autoproclamação, selecionando seus alvos baseados nessas motivações.

Ataques de Ransomware

O ransomware é um tipo de malware que utiliza criptografia para bloquear sistemas ou arquivos em um dispositivo, exigindo um resgate, geralmente em criptomoedas como Bitcoin, para liberar o acesso ao usuário. De acordo com a cartilha do CERT.br, os métodos mais comuns de propagação deste malware incluem:

- E-mails que contêm o código malicioso em anexo ou que levam o usuário a clicar em um link;
- Exploração de falhas em sistemas que não

estão devidamente atualizados em termos de segurança.

A cartilha CERT.br distingue dois tipos de ransomware:

- Ransomware Locker: bloqueia o acesso ao dispositivo infectado;
- Ransomware Crypto: bloqueia o acesso aos dados armazenados no dispositivo, geralmente através de criptografia.

Além de infectar o dispositivo inicial, o ransomware frequentemente busca criptografar outros dispositivos conectados, tanto locais quanto em rede. Enquanto qualquer empresa pode ser alvo de um ataque de ransomware, certas organizações são mais suscetíveis devido à atratividade de seus dados para os cibercriminosos, a importância crítica de restaurar rapidamente o acesso aos dados, a vulnerabilidade de suas seguranças e a eficácia do treinamento de seus funcionários contra ataques de phishing, entre outros fatores (Martin, 2017).

Ataques de DDoS

Ataques de DDoS (*Distributed Denial of Service),* ou Negação de Serviço Distribuída, exploram limitações na capacidade de recursos de rede ao coordenar um conjunto de dispositivos distribuídos para tirar de operação um serviço, computador ou rede conectada à Internet.

Diferentemente de um ataque por malware, cuja motivação pode incluir roubo de dados ou dano direto aos sistemas, o objetivo de um ataque DDoS é meramente esgotar recursos e causar indisponibilidade, impedindo que o alvo acesse ou execute operações necessárias. De acordo com a cartilha do CERT.BR, os ataques de negação de serviço podem ocorrer de diversas maneiras:

- Enviando uma grande quantidade de requisições para um serviço, consumindo recursos essenciais como processamento, número de conexões simultâneas, memória e espaço em disco, o que impede que requisições de outros usuários sejam processadas;
- Gerando um volume massivo de tráfego de dados para uma rede, ocupando toda a banda disponível e tornando inacessíveis computadores ou serviços nessa rede;
- Explorando vulnerabilidades em programas que podem resultar na inacessibilidade de um serviço específico.
- Em casos onde há saturação de recursos, se um serviço não foi adequadamente dimensionado, ele pode se tornar inoperante mesmo ao tentar processar solicitações legítimas (Zillion, 2018).

A SEGURANÇA EM RELAÇÃO A CIBERAMEAÇA

A cibersegurança está sujeita a um ambiente dinâmico e em constante evolução, é crucial reconhecer que novas ameaças surgem continuamente, impulsionadas pelo progresso tecnológico, mudanças nas táticas dos cibercriminosos e as complexidades das relações internacionais (Kello, 2013).

À medida que organizações e indivíduos se empenham em proteger seus sistemas e informações, torna-se essencial manter-se informado sobre as tendências e avanços em cibersegurança. A natureza em constante mudança das ameaças demanda uma abordagem proativa, adaptável e colaborativa para enfrentar os desafios presentes e futuros.

Ademais, é importante reconhecer a crescente interconectividade dos sistemas e a dependência da tecnologia em nossas vidas diárias. A segurança digital agora é uma questão central nas relações internacionais, com os estados buscando fortalecer suas capacidades defensivas e colaborar em esforços conjuntos contra as ameaças cibernéticas transnacionais.

É relevante destacar que, quando as ciberameaças resultam em vítimas, elas se transformam em crimes. Portanto, os termos ciberameaças e cibercrimes serão usados de forma intercambiável aqui, considerando que um é a causa e o outro, o resultado de uma execução bem-sucedida de uma ameaça (Buchanan, 2014).

Como Buchanan mencionou, todas as inovações digitais, como qualquer outra invenção na história, foram possíveis graças a grandes visionários. Infelizmente, nem todas as descobertas no domínio digital são benignas, e indivíduos com avançados conhecimentos de computação podem descobrir vulnerabilidades tecnológicas que podem ser exploradas para fins mal-intencionados.

Os riscos e ameaças cibernéticas estão em constante transformação; o que hoje pode parecer surpreendente, amanhã pode se tornar comum. Como os usuários da *internet* não são esperados para identificar todos os riscos e ameaças por conta própria, aumentar a conscientização sobre essas ameaças e adotar práticas mais seguras *online* é fundamental. A ciberhigiene deve ser mantida no mundo digital, assim como práticas de higiene pública são essenciais nos cuidados de saúde para prevenir a propagação de doenças (Kello, 2013).

Ciberhigiene

A ciberhigiene é um conceito que busca promover, sustentar e garantir a segurança e saúde digital. Para al-

cançar esses objetivos, ações como promover a ciberhigiene através de conscientização e educação sobre riscos computacionais e divulgar boas práticas de cibersegurança são cruciais (Ware, 2013). Isso é realizado por meio de campanhas, treinamentos, seminários e programas educacionais, com o objetivo de disseminar conhecimento e encorajar comportamentos seguros *online*.

A sustentação da ciberhigiene é alcançada pela implementação de estratégias e diretrizes de segurança digital em organizações e instituições, que estabelecem padrões e práticas de segurança a serem seguidos por todos os usuários (Ware, 2013).

Além disso, a atualização regular de sistemas, aplicações e programas, o uso de senhas fortes e a proteção adequada de dispositivos móveis são fundamentais para manter a ciberhigiene. A garantia da ciberhigiene é obtida através da adoção de soluções de segurança digital, como antivírus, firewalls e ferramentas de detecção de malware, que ajudam a proteger contra ciberameaças e asseguram a segurança dos sistemas e dados (Buchanan, 2014).

A realização regular de backups dos dados e a implementação de medidas de privacidade e proteção de dados também são essenciais para garantir a ciberhigiene.

Com o aumento da conscientização sobre a esfera digital, espera-se uma melhor ciberhigiene e, consequen-

temente, um aumento no nível de conhecimento sobre as ciberameaças e as medidas de prevenção e proteção necessárias (Buchanan, 2014).

CONSIDERAÇÕES FINAIS

Ao concluir este livro, ressalta-se a importância cada vez maior da cibersegurança em nossa sociedade profundamente conectada digitalmente. Nesta obra, foram explorados diversos tipos de ameaças cibernéticas, desde malwares e ransomwares até ataques de negação de serviço (DDoS), todos pintando um quadro do ambiente dinâmico e perigoso da *internet*. Esses riscos transcendem os desafios técnicos, abarcando também questões cruciais de conscientização e educação.

A implementação de programas contínuos de treinamento, campanhas de conscientização e o cultivo de uma cultura robusta de segurança são essenciais para equipar tanto indivíduos quanto organizações contra ataques cibernéticos sofisticados. Educando sobre práticas recomendadas, é possível mitigar muitas das vulnerabilidades exploradas por cibercriminosos.

Ademais, a promoção de ciberhigiene, que inclui manter *softwares* atualizados, utilizar autenticação multifatorial e realizar backups regulares, oferece uma proteção comparável à higiene pessoal contra doenças. Este livro também abordou a necessidade de uma abordagem colaborativa em cibersegurança, destacando a importân-

cia da cooperação entre países, empresas e indivíduos para fortalecer a segurança cibernética global.

Porém, apesar dos esforços em educação e colaboração, os desafios em cibersegurança continuarão a evoluir com as tecnologias. Investimentos contínuos em pesquisa e desenvolvimento, especialmente em tecnologias emergentes como inteligência artificial e aprendizado de máquina, são vitais para se antecipar a ataques cibernéticos. O papel dos governos é igualmente crucial, não apenas em proteger infraestruturas críticas, mas também em estabelecer políticas e agências reguladoras que promovam práticas seguras e aumentem a resiliência nacional e internacional.

À medida que quase todos os aspectos de nossas vidas tornam-se interconectados, a cibersegurança não é só uma questão de proteger informações, mas também de salvaguardar nosso modo de vida. Assim, enquanto navegamos por este mundo avançado digitalmente, devemos permanecer vigilantes e proativos na luta contra as ciberameaças. Este livro não apenas visa informar, mas também inspirar mudança e ação, encorajando todos a engajar-se ativamente na defesa do ciberespaço, um elemento cada vez mais crítico em nossas vidas no século XXI.

REFERÊNCIAS

AMOROSO, E. G. (2011). **Cyber Attacks**: Protecting National Infrastructure. Burlington: Butterworth-Heinemann.

BUCHANAN, B. (2017). **The Cybersecurity Dilemma**: Hacking, Trust, and Fear Between Nations. New York: Oxford University Press.

CERT.BR. **Materiais de Apoio para Grupos de Resposta a Incidentes de Segurança em Computadores (CSIRTs)**. 2018. Disponível em: https://www.cert.br/csirts/. Acesso em: 04 maio 2020. CERT.BR. Ransomware. 2018. Disponível em: https://cartilha.cert.br/ransomware/. Acesso em: 06 Ago 2024.

GUISSO, Leonardo. **Segurança Digital**: Avaliação Do Nível De Conhecimento DaPopulação Sobre Os Riscos De Segurança Atrelados Ao Uso DaInternet Na Região De Bento Gonçalves. 2017. 84 p. Relatório de Conclusão (Bacharelado em Sistemas de Informação) - Universidade De Caxias Do Sul, Rio Grande do Sul, 2017.

KELLO, L. (2013). **The Meaning of the Cyber Revolution**: Perils to Theory and Statecraft (Vol. 38).The MIT Press.

LEWIS, J. A. (2014). **National Perceptions of Cyber Threats**. Strategic Analysis, (Vol. 38). Strategic Analysis.

MARTIN, James A.. **Who is a target for ransomware attacks**? 2017. Disponível em: https://www.csoonline.com/article/3208111/who-is-a-target-for-ransomwareattacks.html. Acesso em: 07 Ago. 2024.

WENDT, Emerson; JORGE, Higor Vinicius Nogueria. **Crimes Cibernéticos**: Ameaças e Procedimentos de Investigação. 2. ed. Rio de Janeiro: Brasport, 2013. Disponível em: Acesso em: 07 Ago. 2024.

ZILLION CYBERSECURITY. **Conheça o que é e como funciona o ataque DDoS**. 2018. Disponível em: https://www.zillion.com.br/?s=conhe%C3%A7a+como+%C3%A9+e+como+funciona+ataques+ddos. Acesso em: 07 Ago. 2024.

SOBRE O AUTOR

Alexandre Leal Calgaro é um líder proeminente em Tecnologia da Informação, atuando como CEO e Managing Partner na Vega Consultoria em Tecnologia da Informação LTDA. Sua carreira é marcada pela integração exemplar entre inovação tecnológica e estratégia de negócios. Liderou projetos significativos, como a implementação de infraestruturas de segurança e migração para a nuvem, gerenciando orçamentos substanciais e impulsionando a eficiência operacional. Antes disso, atuou como Analista de Suporte Sênior na Sony Brasil, responsável pela administração de redes e datacenters e pela implementação de sistemas complexos como SAP. Alexandre possui formações e certificações em áreas cruciais como virtualização, segurança da informação e soluções de armazenamento da IBM. Fluente em Português, Inglês e Espanhol, dedica-se à promoção da segurança cibernética e ao fortalecimento das competências de TI. Com este livro, Alexandre compartilha seu vasto conhecimento, oferecendo insights valiosos sobre como as organizações podem se proteger contra as crescentes ciberameaças, fomentando uma cultura de segurança robusta em um mundo digital interconectado.

ÍNDICE REMISSIVO

A

C

D

E

F

G

I

M

P

R

S

T

U

V


AYA EDITORA