FUNDAÇÃO DE ASSISTÊNCIA E EDUCAÇÃO
CENTRO UNIVERSITÁRIO ESPÍRITO-SANTENSE
CURSO SUPERIOR EM CIÊNCIA DA COMPUTAÇÃO

ARTHUR FERREIRA HENRIQUE
DANIEL JUNIOR DE FARIA ROCHA
GABRIELY BARBOSA DA SILVA AZEVEDO
JOSÉ LUIZ DOS SANTOS AZEREDO MENDES
SAMUEL LUCAS DE ABREU DOS SANTOS

CIBERSEGURANÇA

VITÓRIA
2024

ARTHUR FERREIRA HENRIQUE

DANIEL JUNIOR DE FARIA ROCHA

GABRIELY BARBOSA DA SILVA AZEVEDO

JOSÉ LUIZ DOS SANTOS AZEREDO MENDES

SAMUEL LUCAS DE ABREU DOS SANTOS

CIBERSEGURANÇA

TRABALHO APRESENTADO À DISCIPLINA DE UNIVERSO COMPUTACIONAL PARA OS CURSOS DE CIÊNCIA DA COMPUTAÇÃO, SOB A ORIENTAÇÃO DAS PROFESSORAS RENATA CRISTINA LARANJA LEITE E MARIA DE LOURDES FONSECA UYTENHOVE

VITÓRIA

2024

SUMÁRIO

1 INTRODUÇÃO

O mundo tem passado por uma gigantesca transformação nos últimos anos, na medida em que a revolução digital segue trabalhando intensamente. Dado que quase todos os aspectos de nossas vidas, desde a comunicação até as operações financeiras, foram virtualizados e integradas à vasta rede digital, novos desafios surgem. Como resultado, a cibersegurança tornou-se um assunto de extrema prioridade.

A cibersegurança é o termo geral para o conjunto de políticas, práticas e tecnologias projetadas para proteger contra-ataques cibernéticos da rede, os sistemas e os dados que contêm. Os ataques cibernéticos incrivelmente variam em gravidade e complexidade, desde tentativas simples de phishing e outras formas de fraude ou roubo de identidade até intrusões sofisticadas de jogadores maliciosos proeminentes. A cibersegurança é uma ameaça sempre presente para os indivíduos e organizações de todo o mundo.

Nesta introdução, vamos explorar os fundamentos da cibersegurança. O conhecimento dos conceitos básicos da cibersegurança nos permitirá fortalecer as defesas online e garantir um mundo digital mais seguro para todos.

2 CONTEXTUALIZAÇÃO HISTÓRICA

A cibersegurança teve suas raízes na época da Guerra Fria, quando a proteção de informações confidenciais e sistemas de comunicação se uma prioridade crucial para governos e organizações militares. Nesse período tenso, as potências mundiais investiram pesadamente em tecnologias de comunicação e computação para manter segredos importantes longe de olhares indesejados e ganhar vantagem competitiva. Isso levou ao desenvolvimento de protocolos de segurança e criptografia, fundamentais para o surgimento da cibersegurança moderna.

Essa base histórica é essencial para entender a grande importância da proteção cibernética na segurança nacional e empresarial. Como mencionado por Schmidt em uma entrevista ao programa '60 Minutes' da CBS em 2010, a cibersegurança é mais sobre procedimentos, educação e comportamento humano do que apenas tecnologia.

Esse ambiente de competição e sigilo durante a Guerra Fria estabeleceu os alicerces dos princípios básicos da cibersegurança, como confidencialidade, integridade e disponibilidade das informações. Com o avanço da tecnologia e a disseminação da conectividade digital, a importância da cibersegurança se expandiu para além das questões militares, abrangendo também aspectos comerciais, governamentais e pessoais.

Atualmente, a cibersegurança é uma preocupação global, com organizações e indivíduos enfrentando uma variedade de ameaças cibernéticas, desde ataques de hackers até o roubo de dados confidenciais. Isso transformou a cibersegurança em uma disciplina em constante evolução, que demanda a colaboração entre especialistas em tecnologia, jurídicos, políticos e sociais para assegurar um ambiente digital seguro e confiável.

3 TIPOS DE AMEAÇAS

Malware, abreviação de "software malicioso", é um termo genérico que se refere a qualquer tipo de software projetado para causar danos ou realizar operações indesejadas em um computador sem o consentimento do usuário.

Alguns exemplos de Malware são os *Worms,* um tipo de vírus auto replicador; os Cavalos de Troia, que roubam informações danificam sistemas e abrem portas para outros malwares; *Ransonware,* que criptografa arquivos e pode causar danos financeiros e interrupção dos negócios; *Spyware,* um tipo de software projetado para espionar atividades do usuário e monitora hábitos de navegação, senhas entre outras informações; *Adware,* que exibe anúncios invasivos, geralmente instalado sem o consentimento do usuário.

Ataques de *phishing* também são muito comuns, esses ataques são tentativas de enganar os usuários para que revelem informações confidenciais, como senhas, detalhes de cartão de crédito ou informações pessoais, geralmente por meio de e-mails, mensagens de texto ou sites falsos.

Já os ataques de negação de serviço (DoS - *Denial of Service*), são ataques de DoS que visam sobrecarregar servidores, redes ou serviços online, tornando-os inacessíveis para usuários legítimos. Os invasores geralmente usam uma rede de dispositivos comprometidos (*botnets*) para enviar um volume massivo de tráfego falso ou solicitações para o alvo, levando a uma interrupção do serviço.

O roubo de identidade também envolve o uso não autorizado das informações pessoais de uma pessoa para cometer fraudes, como abrir contas bancárias, obter crédito ou realizar compras em nome da vítima. Os invasores podem obter essas informações por meio de *malwares* ou brechas de segurança em bancos de dados.

Ataques de injeção de código (*SQL Iniection, XSS*) exploram falhas de segurança em aplicativos da web para inserir código malicioso nos sistemas. Visa manipular consultas de banco de dados, enquanto *Cross-Site Scripting* (X5S) injeta scripts maliciosos em páginas da web para atacar os usuários.

4 TIPOS DE CIBERSEGURANÇA

Assim como o crescimento do nosso desenvolvimento tecnológico resultou em um aumento concomitante do número de ameaças virtuais, muitas das nossas soluções também ofereceram caminhos sobrepujantes sobre as características inditosas e, entre os ir mais percorridos estão:

Segurança de rede: a segurança de rede protege redes de computadores contra invasão e acesso não autorizado. O firewall estabelece uma zona de segurança para os usuários fora dos quais os computadores e redes são acessíveis a todos e ao mesmo tempo protege o sistema de ataques.

Segurança de Endpoint: a segurança de ponto final protege o sistema do computador de tentativas de invasão ou entrada não autorizada. A segurança Endpoint foi recentemente definido como a prioridade máxima. É o processo de garantir que os elementos da tecnologia que um usuário pode acessar – como laptops, servidores e hardware – sejam segurados e protegidos contra ameaças perigosas.

Segurança de Aplicativos: é a proteção de aplicativos de software contra ameaças como falhas de segurança, explorações de vulnerabilidade e ataques de injeção de código. Testes de segurança de aplicativos, firewall de aplicativos da web (WAF) e práticas de desenvolvimento seguro são alguns exemplos.

Segurança de Nuvem: refere-se a como proteger dados, aplicativos e infraestrutura em nuvem de ameaças cibernéticas. Alguns métodos de Segurança de nuvem incluem criptografia, autenticação multifator e controle de acesso para manter os dados seguros.

Segurança de Dados: é o processo de manter os dados confidenciais e sensíveis em sigilo de acessos não autorizados, vazamento e roubo. Alguns componentes da segurança de dados incluem criptografia de dados, controle de acesso, backup regular e política de privacidade.

Segurança de Identidade e Acesso: Visa proteger identidades digitais e controlar o acesso a sistemas, redes e dados, garantindo que somente usuários autorizados tenham permissão para acessar recursos específicos. Autenticação forte, gerenciamento de identidades e acesso (IAM) e monitoramento de comportamento do usuário são algumas das medidas implementadas.

Segurança de Infraestrutura Crítica: Refere-se à proteção de sistemas e redes que prestam serviços essenciais como energia, transporte, saúde e serviços financeiros contra ameaças cibernéticas que pudessem ter impactos devastadores na sociedade.

Estes são apenas alguns dos principais tipos de cibersegurança, e é importante adotar uma abordagem ampla e em multiníveis para garantir proteção eficaz contra as crescentes ameaças cibernéticas.

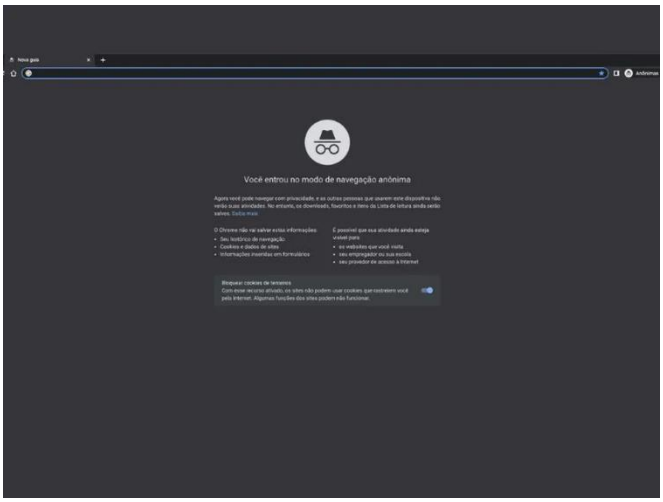
5 DICAS DE PROTEÇÃO

Principais orientações de Segurança Digital

1 A aba anônima e sua funcionalidade

> A navegação anônima não é capaz de “inviabilizar” nenhum usuário. No entanto, o recurso não salva cookies e nem registra históricos de navegação (Como é exemplificado na figura 1). Pode ser especialmente útil para acessar contas de redes sociais em computadores públicos, já que as informações de *login* não ficam salvas no navegador, e, assim, não há chances de que terceiros invadam o seu perfil.
>
> (SILVESTRE et al., 2023)

Figura 1 - Aba de navegação anônima

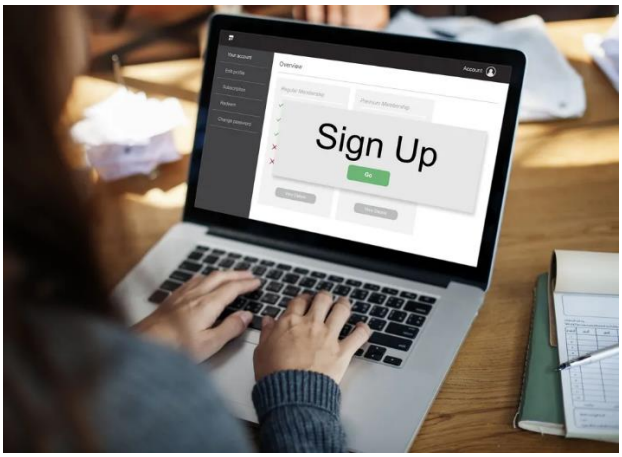


Fonte: TECHTUDO, 2023

2 Como evitar softwares indesejados

Um único clique descuidado pode expor seus dados pessoais ou infectar seu dispositivo com malwares diversos. Portanto, é crucial evitar determinados tipos de conteúdo *online*, como propagandas suspeitas, *links* de fontes não confiáveis, *e-mails* de *spam*, *clickbait* e anúncios não solicitados (Como exemplificado na figura 2). Para se proteger ainda mais, estar com o antivírus sempre atualizado (SILVESTRE et al., 2023)

Figura 2 – Anúncio não solicitado

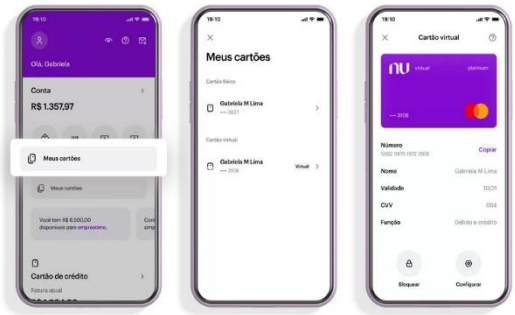


Fonte: FREEPIK

3 Segurança bancária

Não salvar informações de cartões nos navegadores e nem em lojas são recomendadas para evitar vazamentos de dados (como o uso do cartão virtual na figura 3) e, até mesmo, prevenir prejuízos financeiros. Geralmente, o procedimento é mais seguro quando a loja redireciona o usuário para provedores especializados em pagamentos, como PagSeguro, MercadoPago ou Paypal. (SILVESTRE et al., 2023)

Figura 4 – Cartão virtual



Fonte: NUBANK

4 A utilidade da *VPN*

Ao instalar uma VPN, é possível transformar uma rede pública em privada e ocultar seu endereço *IP*. As informações criptografadas são enviadas primeiro para o servidor VPN, que as descriptografa e as transmite para o destino desejado. O retorno das informações é realizado pelo mesmo canal, o que impede que sites, anunciantes e provedores de serviços de Internet rastreiem as atividades do usuário. (SILVESTRE et al., 2023)

5 Não acesse informações sensíveis via *Wi-Fi* público

Embora o uso de Wi-Fi público não seja seguro, ele é inevitável quando estamos sem dados móveis. Nesses casos, é importante evitar realizar transações financeiras, como serviços bancários online ou compras na *Internet*. (SILVESTRE et al., 2023)

6 ÉTICAS E LEIS DA CIBERSEGURANÇA

O compromisso moral é fundamental. A prática do "*hacking"* ético é guiada por normas éticas e legais que visam assegurar que as atividades sejam conduzidas de forma responsável, respeitando os direitos de privacidade e a segurança dos dados. Essas normas envolvem obter autorização antes de realizar qualquer teste de penetração, garantindo permissão do proprietário ou responsável pelo sistema a ser testado, para evitar acessos não autorizados, que são considerados ilegais.

Outro conjunto de diretrizes diz respeito à confidencialidade, em que o "*hacker"* ético deve preservar o sigilo do teste de penetração e não revelar informações confidenciais obtidas durante o processo. O respeito à privacidade é crucial, garantindo que os dados coletados durante o teste sejam tratados com confidencialidade e não sejam compartilhados sem autorização. (PIRES, 2024)

"A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n° 13.709, de 14/08/2018, foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo. A Lei versa sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado, englobando um amplo conjunto de operações que podem ocorrer em meios manuais ou digitais." (Brasil, 2018)

Há diversas formas de penalidades, e nem todas se traduzem em multas financeiras. Em certas situações em que a negligência é evidente, podem ocorrer advertências e orientações para assegurar o cumprimento da lei.

"A ANPD (Autoridade Nacional de Proteção de Dados) pode aplicar ainda, conforme as avaliações realizadas: Advertência, com indicação de prazo para resolver as questões pontuadas; comunicação pública da infração após devidamente apurada e confirmada a sua ocorrência; bloqueio dos dados pessoais a que se refere a infração até a sua regularização; eliminação dos dados pessoais a que se refere a infração; suspensão parcial do funcionamento do banco de dados a que se refere, até a regularização da atividade de tratamento pelo controlador; suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de seis meses, prorrogável por igual período; proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados." (flowti, 2023)

7 PROFISSÃO NA ÀREA

A cibersegurança é um campo multifacetado que abrange uma ampla gama de ocupações especializadas, cada uma desempenhando um papel crucial na proteção dos sistemas e dados contra ameaças cibernéticas. Como salientado por Bruce Schneier, renomado especialista em segurança, "A cibersegurança é sobre pessoas, processos e tecnologia. É uma abordagem holística para proteger os ativos digitais." Dentro desse contexto, as carreiras em cibersegurança vão muito além dos especialistas técnicos.

Entre as ocupações mais comuns estão os analistas de segurança, responsáveis por monitorar e avaliar as ameaças em potencial aos sistemas de informação, e os especialistas em resposta a incidentes, encarregados de identificar, conter e mitigar os impactos de incidentes de segurança. Além disso, os engenheiros de segurança projetam e implementam soluções técnicas para proteger sistemas contra ameaças, enquanto os consultores de políticas desenvolvem e implementam políticas de segurança cibernética para garantir a conformidade regulatória e mitigar riscos.

Outras ocupações importantes incluem os testadores de penetração, que avaliam a segurança de sistemas identificando e explorando vulnerabilidades, e os gerentes de segurança, que supervisionam e coordenam as atividades de segurança cibernética em uma organização. Com o aumento da conscientização sobre a importância da cibersegurança, essas profissões estão em alta demanda em uma variedade de setores, oferecendo oportunidades significativas de carreira para indivíduos com habilidades técnicas e conhecimento especializado em segurança cibernética.

REFERÊNCIAS

"Cybersecurity and Cyberwar: What Everyone Needs to Know" de P.W. Singer e Allan Friedman (2014)
DIGITAL SECURITY GUIDE, How to browse the internet safely both at work and at home, how-to-browse-the-internet-safely-both-at-work-and-at-home.html. Disponível em: <digitalsecurityguide.eset.com/en-us/how-to-browse-the-internet-safely-a-work-and-at-home>. Acesso em: 15 abr. 2024.

FREEPIK. Anúncio não solicitado. Disponível em: <www.techtudo.com.br/listas/2023/07/seguranca-digital-faca-essas-10-isas-para-se-manter-seguro-na-internet-edsoftwares.ghtml >. Acesso em: 15 abr. 2024.

GEEKSFORGEEKS, HOW TO BROWSE the Internet Safely?, how-to-browse-the-internet-safely.html, 2021. Disponível em: <www.geeeksforgeeks.org/how-to-browse-the-internet-safely/>. Acesso em: 15 abr. 2024.

https://flowti.com.br/blog/conheca-as-principais-sancoes-para-quem-descumpre-a-lgpd

https://www.gov.br/mds/pt-br/acesso-a-informacao/governanca/integridade/campanhas/lgpd

https://www.ibm.com/br-pt/products/ns1-connect/ddos-protection?mhsrc=ibmsearch_a&mhq=Ataques%20de%20nega%26ccedil%3B%26atilde%3Bo%20de%20servico%20%26lpar%3BDoS%20-%20Denial%20of%20Service%26rpar%3B

https://www.ibm.com/br-pt/topics/malware?mhsrc=ibmsearch_a&mhq=malware

https://www.ibm.com/brpt/topics/phishing?mhsrc=ibmsearch_a&mhq=Ataques%20de%20phishing

https://www.ibm.com/br-pt/topics/zero-day?mhsrc=ibmsearch_a&mhq=Ataques%20de%20dia%20zero

https://www.kaspersky.com.br/resource-center/definitions/what-is-a-cross-site-scripting-attack

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

KASPERSKY, Top 15 internet safety rules and what not to do online, top-10-preemptive-safety-rules-and-what-not-to-do-online.html. Disponível em: < www.kaspersky.com/resource-center/preemptive-safety/top-10-preemptive-safety-rules-and-what-not-to-do-online >. Acesso em: 15 abr. 2024.

NUBANK. Cartão virtual. Disponível em: < blog.nubank.com.br/cartao-virtual-nubank-tudo-sobre/ >. Acesso em: 15 abr. 2024.

OpenAI. (2021). *ChatGPT* (Versão 3.5) [Software]. Recuperado de https://openai.com/

SILVEIRA, C. Segurança digital: faça essas 10 coisas para se manter seguro na internet, segurança-digital-faca-essas-10-coisas-para-se-manter-seguro-na-internet-edsoftwares.ghtml, TechTudo, 2023. Dísponível em:

<www.techtudo.com.br/listas/2023/07/seguranca-digital-faca-essas-10-isas-para-se-manter-seguro-na-internet-edsoftwares.ghtml>. Acesso em: 15 abr. 2024.

SWISS CYBER INSTITUTE, How to Browse the Internet Safely: 10 Tips, 10-tips-on-how-to-browse-the-internet-safely.html. Disponível em: <swisscyberinstitute.com/blog/10-tips-on-how-to-browse-the-internet-safely/>. Acesso em: 15 abr. 2024.

TECHTUDO. Aba de navegação anônima. 2023. Disponivel em: < www.techtudo.com.br/listas/2023/07/seguranca-digital-faca-essas-10-isas-para-se-manter-seguro-na-internet-edsoftwares.ghtml >. Acesso em: 15 abr. 2024.

The State of Cybersecurity 2024. https://www.isc2.org/Research/Cybersecurity-Workforce-Study

"The Origins of Cybersecurity" de Jon Lindsay (2013)

TITANFILE, How to Browse the Internet Safely, how-to-browse-the-internet-safely.html. Disponível em: <www.titalfile.com/how-to-browse-the-internet-safety/>. Acesso em: 15 abr. 2024.

UNPLASH. Serviço de VPN. 2023. Disponível em < unsplash.com/pt-br/fotografias/pessoa-que-usa-o-computador-portatil-preto-NEtFkKuo7VY >. Acesso em: 15 abr. 2024