E-Book Colaborativo

Introdução à Cibersegurança

Sumário

Capítulo 1

Introdução à Cibersegurança

A Cibersegurança é uma das principais áreas da computação atualmente, e será cada vez mais, que abrange todas as áreas e aspectos da sociedade contemporânea, uma sociedade hiperconectada. Empresas, Governos, Cidadãos e todos os agentes da sociedade devem ter preocupações com a segurança no meio digital que possui como principal característica a alteração dinâmica e constante. Nas mídias sociais, não é raro saber que algum "influencer" teve sua conta invadida, ou até mesmo, pessoas próximas que tiveram contas invadidas ou o "whatsapp clonado", o que evidencia a importância da difusão do tema e boas práticas de segurança no cotidiano de todos, não somente para empresas, órgãos estatais ou profissionais de 'TI'. Muitos ataques e golpes que são propagados pelo meio digital são atualizações de golpes já conhecidos que eram realizados por outros meios, sendo esses os que utilizam principalmente a Engenharia Social, como o Phishing que geralmente chega às vítimas por meio de emails, ou mensagens, como propaganda, ou, e como pessoal, sistemas, conhecidos das vítimas, se passando por eles para extrair informações ou direcionar a outros ambientes menos protegidos. Mas há também ataques e golpes específicos do meio virtual, como é o caso dos ataques de DDoS, que visa causar instabilidade, ou até inviabilizar o acesso, de sistemas online,

principalmente sites.

Há muitos aspectos da Cibersegurança a serem abordados por profissionais de tecnologia, usuários e organizações privadas e públicas para manterem seus sistemas, redes e dados seguros no ambiente virtual.

Capítulo 2

Princípios Básicos de Segurança Digital

A Cibersegurança possui alguns princípios básicos e fundamentais para todo e qualquer agente na sociedade digital, sendo os 4 principais: Confidencialidade, Integridade, Disponibilidade e Autenticidade.

A Confidencialidade: é a proteção da informação contra acesso não autorizado, garantir que apenas pessoas ou sistemas autorizados possam visualizar ou manipular informações sensíveis. Este princípio é crucial para preservar a privacidade e proteger dados confidenciais, seja de indivíduos, empresas ou governos. Os meios de se garantir a confidencialidade das informações é por meio de 'Autenticação', verificação da identidade do utilizador, 'Criptografia', codificação das informações, 'Controle de Acesso', meios para restringir o acesso a informações com base em políticas e permissões, e 'Políticas de Privacidade', definição clara de como proteger e quem pode acessar os dados.

A Integridade: é a garantia de que as informações serão mantidas inalteradas, precisas, assegurando que os dados permaneçam consistentes ao longo do tempo e que as alterações sejam feitas de forma controlada. Algumas formas de garantir a integridade dos dados são o 'Hash e Somatórios de Verificação', funções e algoritmos matemáticos que ao final resultam em um número único para cada conjunto de dados, 'Controles de Versão', histórico de mudanças per-

mitindo a restauração de versões anteriores, 'Assinaturas Digitais', aplicação de criptografia para verificar a origem e a integridade de mensagens ou documentos eletrônicos, 'Auditorias e Logs', monitoramento e registro de atividades de sistema para detectar e investigar alterações não autorizadas.

A disponibilidade é a garantia de que a informação e os sistemas estão acessíveis e utilizáveis quando necessário, princípio fundamental, pois mesmo dados protegidos e precisos são inúteis se não estiverem disponíveis para uso no momento certo. As principais formas de garantir a disponibilidade são a 'Redundância', equipamentos e sistemas duplicados para evitar falhas de software ou hardware, 'Backup e Recuperação', realização de cópias regulares de dados que podem ser restauradas em caso de perda ou corrupção, 'Planos de Continuidade de Negócios', estratégias para manter operações críticas durante e após uma crise, 'Proteção contra Ataques DDoS', medidas para mitigar ataques.

A Autenticidade: assegura que as informações e comunicações sejam genuínas e provenientes de fontes confiáveis por meio de verificação da identidade de usuários, dispositivos e dados, garantindo que as partes envolvidas são quem dizem ser. As formas de se garantir a autenticidade são por 'Certificados Digitais', utilização de certificados emitidos por autoridades confiáveis para validar a identidade de

usuários e sistemas, ‘Assinaturas Digitais’, garantia de que um documento ou mensagem é autêntico e não foi alterado após sua assinatura, ‘Autenticação Multifator’, implementação de múltiplos métodos de verificação para confirmar a identidade do usuário, ‘Protocolos Seguros’, uso de protocolos de comunicação segura, como ‘https’, para garantir a autenticidade dos dados transmitidos.

Cada um desses fundamentos é essencial para garantir que as informações estejam seguras e utilizáveis quando necessário. Compreender e aplicar esses princípios é crucial para proteger os dados e a eficiência das operações em um ambiente digital cada vez mais complexo.

Capítulo 3

Ameaças Cibernéticas: uma visão geral detalhada

As ameaças cibernéticas evoluem com a tecnologia e afetam o comportamento humano e os sistemas. Elas variam em magnitude e gravidade, desde ameaças simples até perdas financeiras e de reputação adversas. Neste contexto, apresentamos a seguir as ameaças cibernéticas mais habituais, seus métodos, exemplos, e medidas para mitigação das ameaças.

Malware: abrange toda uma gama de programas maliciosos, como vírus, worms, cavalos de troia, spyware, adware, rootkits, entre outros. Pode ser desenvolvido para danificar sistemas, armazenar dados ou obter acesso aos dispositivos de forma escusa. Os meios de dispersão de malware ocorre por meio de downloads de arquivos infectados, anexos de e-mails maliciosos, links maliciosos ou dispositivos USB infectados. Um malware de grande impacto é o Ransomware, pois criptografa todo o sistema e discos conectados solicitando um 'resgate' para reaver o sistema, um sequestro dos dados, sendo muitas vezes o resgate é solicitado em criptomoedas, por serem meios não rastreáveis de pagamento. Um exemplo desse tipo de ataque ocorreu com a Oleoduto Colonial, em 2021, impactando diretamente o fornecimento de petróleo nos Estados Unidos.

Ataque de negação de serviço (DDoS): São ataques que enviam inúmeras requisições a um sistema, visando

causar instabilidades, ou até mesmo deixar fora de funcionamento um sistema, geralmente sites são os principais alvos para esses ataques, porém podem ocorrer com qualquer sistema online. Um exemplo de ataque DDoS ocorreu em novembro de 2021, onde a Azure sofreu o ataque que teve origem de 10 mil dispositivos de 10 países diferentes, causando instabilidades no serviço.

Spyware e keyloggers: Spyware e Keyloggers são geralmente utilizados em conjuntos, pois ambos espionam a vítima, o spyware observa as atividades, os keyloggers fazem o registro das teclas digitadas no dispositivo com o intuito de obter informações das vítimas. Podem tanto registrar localmente essas informações e depois enviar para o hacker, tanto quando podem transmitir em tempo real, permitindo que o atacante envie comandos pelo keylogger para o dispositivo infectado. Raramente são identificados, pois se passam por softwares legítimos, ou até mesmo encorpados em softwares legítimos, que a vítima instala em seu computador por meio de fontes não confiáveis, como no caso de softwares 'crackeados' onde se remove a solicitação licenças e chaves de ativação.

Esses são alguns dos ataques que ocorrem diariamente e impactam diretamente empresas, organizações governamentais e usuários, há vários outros tipos de ataques e combinações de métodos para esse fim.

Capítulo 4

Boas Práticas para Proteção Digital

Ter boas práticas de segurança digital reduz significativamente as chances de sofrer algum tipo de ataque virtual é indispensável para todos, indivíduos ou organizações. Há inúmeras práticas de segurança que podem ser tomadas, mas algumas sempre surgem como as principais e mais adotadas, que são:

Senhas: fáceis, previsíveis, ou até mesmo padrões, como ‘12345’, ‘admin admin’ ou datas de aniversários não são eficazes e em muitos casos são o principal meio de obtenção acesso não autorizado, por isso criar senha mais complexas, com uma maior quantidade de caracteres são melhores, misturar letras, números e caracteres especiais na senha a tornam mais segura. Outra forma criar senha seguras é por meio de frases, mas deve-se tomar cuidado com essa forma de criar senhas, pois não se deve colocar uma frase óbvia como senha. Reutilizar senhas em vários locais e contas na internet também não é uma boa, pois caso descubram sua senha, descobriram de todas as suas contas, então sempre crie senhas únicas para cada.

Atualizações: devem ser feitas cotidianamente, pois essas atualizações em sua maioria corrigem bugs, falhas e até mesmo problemas de segurança dos sistemas, que afetam diretamente o usuário final dos sistemas. Por mais que algumas atualizações sejam demoras de realizar, são de

vital importância pois elas garantem que os sistemas não sofram ataques de vulnerabilidades já conhecidas e consertadas, assim reduzindo a chances de um ataque ocorrer por essas falhas. Em muitos dispositivos e sistemas há a opção de atualizações automáticas, mas ainda há alguns que não oferecem essa opção, então sempre verifique se há atualizações para eles. Não ignore nenhum aviso de atualização dos seus sistemas, pois elas são de extrema importância para a segurança digital.

Desconfie: de emails, mensagens que você não conheça a fonte, ou que contenham textos fora do habitual, pois isso é um grande indício de Phishing, onde os criminosos usam de engenharia social para adquirir informações que possam lhe serem úteis. Atualmente o dominio "@gmail.com" é o mais utilizado por pessoas e empresas e geralmente são confiáveis, porém grandes empresas não o utilizam e sim possuem um domínio próprio.

Desconfie também de propagandas em sites, pop-ups e ofertas improváveis, sempre acesse os sites oficiais de comércios e serviços.

Antivírus: é um sistema que verifica constantemente processos, arquivos e outros componentes do sistema do dispositivo em busca de possíveis ameaças de segurança, uma busca ativa, além de verificar todo novo arquivo e programa adicionados ao sistema, impedindo a execução em caso de ameaças. Por esses motivos, utilizar um bom

antivírus é importante para garantir uma maior segurança digital.

Capítulo 5

Noções Básicas de Segurança para Profissionais de TI

Profissionais da TI estão em um ponto central na questão de segurança, são os principais responsáveis por manter ambientes organizacionais e sistemas seguros.

No ambiente organizacional, o profissional de TI visa principalmente pela segurança dos dados da organização, a rede interna e o que os usuários podem ou não acessar na internet. Garantindo maior controle das vulnerabilidades. A proteção da rede de uma organização é extremamente importante, pois é a primeira e principal medida de proteção. Algumas boas práticas para essa segurança de rede são:

Gerenciamento de Identidade e Acesso (IAM): é forma de gerir acesso aos usuários apenas aos itens que têm permissão e bloqueia o acesso aos que não tem permissão para acessar, assim evitando que os usuários vejam documentos, informações confidenciais ou que não deveriam ter acesso, assim evitando vazamentos de informações.

Redes Privadas Virtuais (VPNs): são serviços de segurança que criptografam as comunicações na internet, permitindo a criação de 'canais exclusivos' para indivíduos, ou no caso para organizações. Fornecem um grande grau de anonimato, o que permite que funcionários fisicamente fora da rede da organização acessem arquivos, sistemas e

outras funcionalidades internas da organização como se estivesse fisicamente na empresa, permitindo assim acessos externos de forma segura dentro e fora da empresa.

Firewalls: é um sistema que monitora e gerencia o tráfego de redes com base em regras de segurança definidas pelos profissionais de TI, geralmente os firewalls ficam entre a rede interna da organização e a internet, permitindo ou não o tráfego de dados de fora para dentro e dentro para fora da organização, barrando o tráfego sempre que alguma regra de segurança não for atendida.

Gestão de Vulnerabilidades: é a prática contínua de identificação, avaliação e correção de falhas de segurança, sendo um processo importante para evitar ataques por meio dessas vulnerabilidades conhecidas.

Além das redes organizacionais, há também profissionais de TI que trabalham no desenvolvimento de sistemas que devem seguir práticas para terem segurança em seus sistemas. Alguma dessas práticas são:

Capítulo 6

Conclusão

A importância da cibersegurança é extensa e essencial para todos, os pontos apresentados neste livro são apenas uma breve introdução ao tema, mesmo que de grande valor. Há muito conteúdo e cursos disponíveis, formações de nível superior e com vagas no mercado de trabalho.

Deixamos abaixo as referências usadas na formulação desse livro, para maior aprofundamento no tema.

Capítulo 7

Referências

SYMCANTEC CORPORATION. Internet Security Threat Report. Mountain View: Symantec, 2022. Disponível em: <https://www.symantec.com>. Acesso em: 16 nov. 2024.

KASPERSKY LAB. Relatório de Inteligência de Ameaças. Moscou: Kaspersky, 2023. Disponível em: <https://www.kaspersky.com>. Acesso em: 16 nov. 2024.

Ataque cibernético provoca fechamento de um dos principais oleodutos dos EUA. Disponível em: <https://www.cnnbrasil.com.br/internacional/ataque-cibernetico-provoca-fechamento-de-um-dos-principais-oleodutos-dos-eua/>. Acesso em: 16 nov. 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Framework for Improving Critical Infrastructure Cybersecurity. Gaithersburg: NIST, 2018. Disponível em: <https://www.nist.gov>. Acesso em: 16 nov. 2024.

OWASP FOUNDATION. Top 10 Security Risks. Los Angeles: OWASP, 2023. Disponível em: <https://owasp.org>. Acesso em: 16 nov. 2024.

VARITUS BRASIL. Quais são os 4 Princípios da Segurança da Informação? - Varitus Brasil. Disponível em: <https://www.varitus.com.br/v-tech/quais-sao-os-4-principios-da-seguranca-da-informacao/2306/>. Acesso em: 16 nov. 2024.

ataques DDoS famosos | Maiores ataques DDoS. Disponível em: <https://www.cloudflare.com/pt-br/learning/ddos/famous-ddos-attacks/>. Acesso em: 22 nov. 2024.

O que é segurança de rede? | Segurança de rede corporativa? Disponível em: <https://www.cloudflare.com/pt-br/learning/network-layer/network-security/>. Acesso em: 22 nov. 2024.

O que é IAM | Gerenciamento de identidade e acesso. Disponível em: <https://www.cloudflare.com/pt-br/learning/access-management/what-is-identity-and-access-management/>. Acesso em: 22 nov. 2024.

O que é uma VPN? Disponível em: <https://www.cloudflare.com/pt-br/learning/access-management/what-is-a-vpn/>. Acesso em: 22 nov. 2024.

O que é firewall | Firewall de rede. Disponível em: <https://www.cloudflare.com/pt-br/learning/security/what-is-a-firewall/>. Acesso em: 22 nov. 2024.

O que é gerenciamento de vulnerabilidades? | IBM. Disponível em: <https://www.ibm.com/br-pt/topics/vulnerability-management>. Acesso em: 22 nov. 2024.

O que é gerenciamento de vulnerabilidades? Disponível em: <https://www.redhat.com/pt-br/topics/security/what-is-vulnerability-management>. Acesso em: 22 nov. 2024.

VINICIUS. Boas práticas de Desenvolvimento de Software e Segurança | D3 Works. Disponível em: <https://d3.works/boas-praticas-de-desenvolvimento-de-software-e-seguranca/>. Acesso em: 22 nov. 2024.

ADMIN. Desenvolvimento de software seguro: o que é e como auxilia na proteção da sua empresa - Secureway. Disponível em: <https://secureway.com.br/desenvolvimento-de-software-seguro-o-que-e-e-como-auxilia-na-protecao-da-sua-empresa/>. Acesso em: 22 nov. 2024.

TEAM, C. 6 dicas de segurança no desenvolvimento de softwares. Disponível em: <https://blog.convisoappsec.com/seguranca-no-desenvolvimento-de-softwares/>. Acesso em: 22 nov. 2024.