Fundação Universidade de Blumenau

Legislação em Informática

Profº Alejandro Knaesel Arrabal

Aluno: Luiz Henrique Martendal

**A Cibersegurança e o Anonimato na era digital**

A cibersegurança é um termo que se refere à proteção de sistemas, redes e dados digitais contra os ataques cibernéticos. Com o aumento da dependência da tecnologia em nossas vidas, a cibersegurança tornou-se uma preocupação cada vez mais importante. Hackers e outras pessoas mal-intencionadas estão constantemente procurando maneiras de obter acesso a informações privadas e sensíveis, e é crucial que as empresas e indivíduos protejam seus dados.

A importância de proteger dados é evidente em vários setores, incluindo finanças, saúde e governo. Hackers podem roubar informações pessoais, como números de cartão de crédito ou contas bancárias, e usá-las para fins fraudulentos. Eles também podem acessar dados confidenciais, como informações de pacientes em hospitais ou segredos de negócios em empresas. Em alguns casos, os hackers podem até causar danos físicos, como interromper sistemas de energia ou transporte.

Os hackers agem de várias maneiras, incluindo phishing, engenharia social e exploração de vulnerabilidades em sistemas de segurança. O phishing é uma técnica em que os hackers enviam e-mails fraudulentos que parecem legítimos, na tentativa de enganar as pessoas a clicarem em links maliciosos ou fornecerem informações pessoais. A engenharia social é uma técnica em que os hackers manipulam as pessoas para obter acesso a informações confidenciais. A exploração de vulnerabilidades em sistemas de segurança envolve encontrar falhas em sistemas de segurança e usá-las para obter acesso a informações.

Hoje em dia o termo hacker para muitas pessoas leva a imagem de alguém que age no anonimato, onde seu objetivo é buscar vulnerabilidades e conseguir ter acesso de forma maliciosa aos dados de outras pessoas. Bem, em parte, pode-se dizer que a afirmação está correta. Isso porque não há somente um “tipo” de hacker, atualmente temos vários, e com isso eu decidi por interesse próprio perguntar ao Chatgpt quais eram esses “tipos” e um pequeno resumo sobre:

Resposta do Chatgpt

“

*Existem diferentes tipos de hackers, classificados com base em suas intenções e motivações. Aqui estão alguns dos principais tipos.*

*Hacker ético (White Hat Hacker): Esses hackers são especialistas em segurança cibernética contratados para proteger sistemas e redes. Eles usam suas habilidades para identificar vulnerabilidades em sistemas e fornecer soluções para fortalecer a segurança. Os hackers éticos geralmente trabalham em empresas de consultoria em segurança ou fazem parte das equipes de segurança internas das organizações.*

*Hacker malicioso (Black Hat Hacker): Esses hackers têm intenções maliciosas e usam suas habilidades para explorar vulnerabilidades em sistemas, redes ou aplicativos para obter acesso não autorizado, roubar informações valiosas, realizar fraudes ou causar danos. Eles estão envolvidos em atividades ilegais e são responsáveis por ataques cibernéticos, como roubo de dados, ataques de ransomware e invasões de sistemas.*

*Hacker cinza (Gray Hat Hacker): Esses hackers não têm intenções estritamente maliciosas, mas também não têm permissão legal para acessar sistemas ou redes. Eles podem encontrar vulnerabilidades e explorá-las sem autorização, mas, em alguns casos, notificam os proprietários dos sistemas sobre as falhas de segurança, fornecendo informações para que possam ser corrigidas. Embora suas intenções não sejam puramente maliciosas, suas ações são ilegais.*

*Hacker ativista (Hacktivist): Os hackers ativistas são motivados por causas políticas, sociais ou ideológicas. Eles usam suas habilidades em hacking para divulgar mensagens, realizar ataques de negação de serviço (DDoS) ou invadir sistemas de organizações ou governos que consideram contrários aos seus ideais. Grupos como Anonymous são exemplos de hacktivistas.*

*Script Kiddie: Esse termo é usado para descrever pessoas inexperientes em hacking que usam ferramentas ou scripts criados por outros para realizar ataques cibernéticos. Eles geralmente não têm um profundo conhecimento técnico e dependem de métodos prontos para uso, em vez de desenvolver suas próprias habilidades.*

*É importante lembrar que o termo "hacker" pode ter conotações diferentes dependendo do contexto em que é usado. Nem todos os hackers estão envolvidos em atividades ilegais, e alguns podem até ser considerados heróis da segurança cibernética, trabalhando para proteger sistemas e redes contra ameaças.*

“

Nos dias atuais, podemos ver claramente que os grupos de hackers que mais repercutem na mídia atual são os Black Hat Hackers e os Hacktivist. Isso se leva ao fato de seus atos atacarem principalmente empresas grandes, governos ou pessoas com “alta importância” na sociedade. Com isso, trago um acontecimento de 2017 sobre o caso WannaCry, um ransomware que se aproveitou de uma vulnerabilidade no sistema Windows da Microsoft onde os arquivos dos usuários eram mantidos como reféns e, para que fossem devolvidos, era exigido um resgate em bitcoins. E uma das formas que esse ransomware invadiu máquinas no mundo todo foi através do phishing, uma prática citada no início do texto.

Se não fosse o uso contínuo de sistemas de computador desatualizados e o pouco conhecimento sobre a necessidade de atualizar o software, os danos causados por esse ataque poderiam ter sido evitados.

Abaixo, eu trago um trecho do site Kaspersky (o site do antivírus Kaspersky) que fala sobre o impacto do ransomware:

“

*O ataque do ransomware WannaCry atingiu cerca de 230 mil computadores em todo o mundo.*

*Uma das primeiras organizações afetadas foi a empresa espanhola de telefonia móvel, a Telefónica. Em 12 de maio, milhares de consultórios e hospitais do NHS foram afetados em todo o Reino Unido.*

*Um terço das fundações hospitalares do NHS foram afetadas pelo ataque. Outro acontecimento assustador foi que as ambulâncias mudaram de rota e deixaram de atender pessoas que precisavam de cuidados urgentes. O custo estimado para o NHS foi de esmagadores £ 92 milhões após 19 mil consultas terem sido canceladas como resultado do ataque.*

*À medida que o ransomware se disseminou para fora da Europa, os sistemas de computadores em 150 países ficaram paralisados. O ataque do ransomware WannaCry teve um impacto financeiro considerável em todo o mundo. Estima-se que as perdas causadas por esse crime cibernético tenham somado US$ 4 bilhões em todo o mundo.*

*O WannaCry se espalhou usando uma exploração de vulnerabilidade chamada "EternalBlue". A Agência de Segurança Nacional dos Estados Unidos (NSA) desenvolveu essa exploração, presumivelmente para uso próprio, mas ela foi roubada e lançada ao público por um grupo chamado Shadow Brokers depois que a própria NSA foi comprometida. O EternalBlue só funcionava em versões mais antigas e sem patch do Microsoft Windows, mas havia um número de máquinas mais do que o suficiente executando tais versões para permitir a rápida disseminação do WannaCry.*

“

O grupo responsável pelo ataque nunca foi bem comprovado, já que todos os grupos agem no anonimato. Mas, muitos indícios apontam ao grupo Shadow Brokers um grupo de invasores que começaram a vazar ferramentas de malware e explorações de dia zero para o público em 2016. Eles são suspeitos de terem adquirido várias explorações desenvolvidas pela NSA, possivelmente devido a um ataque interno na agência. Em 14 de abril de 2017, os Shadow Brokers vazaram a exploração Eternal Blue que o WannaCry acabaria por usar.

E como esses hackers “vivem no anonimato”, que seria uma ferramenta que os hackers usam para esconder sua identidade e evitar serem rastreados. Acabamos enxergando melhor os prós e contras para o anonimato na internet. Por um lado, o anonimato pode permitir que pessoas expressem opiniões livremente e denunciem injustiças sem medo de retaliação. Por outro lado, o anonimato pode permitir que os hackers cometam crimes sem serem responsabilizados por suas ações.

Existem várias ferramentas de proteção de dados disponíveis para empresas e indivíduos. As ferramentas incluem firewalls, antivírus, criptografia e autenticação de dois fatores. Os firewalls são barreiras que impedem o acesso não autorizado a redes e sistemas. Os antivírus são programas que detectam e removem vírus e malware de computadores e dispositivos móveis. A criptografia é uma técnica que codifica informações para que só possam ser lidas por pessoas autorizadas. A autenticação de dois fatores é um processo em que os usuários precisam fornecer duas formas de identificação para acessar uma conta

Em resumo, a cibersegurança é uma preocupação cada vez mais importante em nossas vidas digitais. É crucial que empresas e indivíduos protejam seus dados contra hackers e outras pessoas mal-intencionadas. Existem várias ferramentas de proteção de dados disponíveis, e é importante usar essas ferramentas para garantir a segurança dos dados. O anonimato pode ter prós e contras, e é importante considerar cuidadosamente as implicações do anonimato na internet.

**Referências**

O que é o ransomware WannaCry; Kaspersky; Acesso em: 04/06/2023; Disponível em: <https://www.kaspersky.com.br/resource-center/threats/ransomware-wannacry>;