7º MoEduCiTec
Mostra Interativa da Produção Estudantil em Educação Científica e Tecnológica
1º Mostra de Extensão Unijuí
O Protagonismo Estudantil em Foco
27 de outubro de 2023 - Unijuí - Campus Ijuí

CIBERSEGURANÇA: SISTEMAS ESSENCIAIS E INFORMAÇÕES SENSÍVEIS

Gustavo Legunde Ristow[1]
Nicolas De Almeida Dos Santos[2]
Rosana Souza de Vargas[3]

Instituição: Escola Técnica Estadual 25 de Julho

Modalidade: Relato de Pesquisa

Eixo Temático: Tecnologias da Informação e Comunicação

Introdução

Neste trabalho, pretendemos compreender tudo sobre a cibersegurança. Segundo o site Softsell, o principal objetivo da cibersegurança é reforçar os servidores e redes, além de garantir a proteção dos equipamentos, como computadores e dispositivos móveis, e também dos dados armazenados nestes locais, sejam físicos ou em nuvens.

Alem disso, um grande problema que coincide na cibersegurança é o desconhecimento sobre a área (principalmente das pessoas mais velhas). Segundo o site Security Report, o Brasil sofreu mais de 103 bilhões de ataques cibernéticos no ano passado, mais atingido da América Latina e com um aumento de 16% em relação a 2021. Várias pessoas são atacadas virtualmente, podendo ocasionar em dinheiro roubado, máquinas estragadas e danos morais.

Segundo o site Security Report, um estudo Alemão da Consultora Roland Berger, o Brasil foi o 5º país que mais sofreu crimes cibernéticos no ano passado, com 9,1 milhões de ocorrências, somente no primeiro trimestre – mais que o ano inteiro de 2020. Por isso, acreditamos que seja importante debater sobre esse assunto.

Caminho metodológico

A forma de pesquisa que utilizamos é a abordagem qualitativa (que, segundo o site Projeto Acadêmico, realiza uma análise muito mais aprofundada sobre o tema pesquisado).

[1] Estudante do 2º do Ensino Médio da Escola Técnica Estadual 25 de Julho: gustavo-ristow@educar.rs.gov.br
[2] Estudante do 2º do Ensino Médio da Escola Técnica Estadual 25 de Julho: nicolas-dadsantos@educar.rs.gov.br
[3] Professora da disciplina de Iniciação Científica da Escola Técnica Estadual 25 de julho: rosana-vargas@educar.rs.gov.br.

Além de escrever e aprofundar conhecimento teórico sobre o tema em uma pesquisa bibliográfica em artigos científicos e sites da internet.

Esta é uma pesquisa de natureza aplicada, pois iremos desenvolver um guia informativo, que será apresentado no dia da Mostra, de fácil acesso e grande circulação, para ajudar na busca pela solução para o problema da falta de cuidado na internet em relação aos vírus, ataques, senhas fracas, roubos de dados e informações, compartilhamento de senhas, etc.

Resultados e discussão

CIBERSEGURANÇA

O Termo Cibersegurança ou Cibersecurity surgiu em 1990 para se referir a segurança do ciberespaço, tendo como finalidade abranger um novo conjunto de ameaças e atores. ele é a prática proteger ativos de informação tais sistemas, computadores e servidores entre outros contra ameaças cibernéticas ou ataques maliciosos.

O motivo pelo qual a cibersegurança é importante e que sem ela inúmeros usuários poderiam facilmente cair em golpes e até mesmo baixar malwares perigosos em suas máquinas. É graças a coisas como a cibersegurança, antivírus, antispyware, defenders e afins que a internet consegue ser um local

Segundo o site SAP.com, houve um aumento de 358% nos ataques de malware, um aumento gigantesco. O'Que isso revela é que a cibersegurança não só deveria existir como também deveria ser massivamente aumentada e expandida, com o objetivo não só dos números de ataques diminuírem, como também pelo objetivo de criar o ambiente mais seguro possível para todos os usuários.

Tipos de cibersegurança, segundo o site SAP:

Segurança de aplicativos: consiste de programas como antivírus, antispyware, firewalls, programas de criptografia, etc.;

Segurança da IoT: consiste em proteger dispositivos da internet e as redes às quais eles estão conectados contra ameaças e violações, por meio da proteção;

Segurança da infraestrutura essencial: consiste na proteção de sistemas físicos e cibernéticos fundamentais que embasam nossa sociedade, como redes de eletricidade, sistemas de água e serviços de saúde pública;

Segurança de rede: consiste na proteção de login, senhas e segurança dos aplicativos.;

Segurança de ponto de acesso: consiste na proteção de desktops, laptops, sistemas sem fio e dispositivos móveis. Também inclui proteção antivírus e antimalware, segurança de IoT e segurança na nuvem;

Segurança da informação: tem como foco a manutenção da confidencialidade, integridade e disponibilidade de todos os dados digitais e analógicos das organizações;

Prevenção contra perda de dados: tem como foco impedir que dados confidenciais saiam da organização, sejam divulgados intencionalmente ou compartilhados sem querer. A tecnologia de DLP rastreia, identifica e impede o fluxo de informações não autorizadas com classificação, criptografia, monitoramento e aplicação de políticas;

Gestão de identidade e acesso (IAM): engloba autenticação de dois fatores, autenticação multifator, gestão de acesso privilegiado e biometria;

Gestão de eventos e informações de segurança (SIEM): monitoram e analisam dados e eventos de segurança em tempo real e ajudam as organizações a detectar e responder a ameaças cibernéticas antes que interrompam as operações de negócios. Usa inteligência artificial;

Usuário e seu ‘’treinamento’’ em questão da cibersegurança: os usuários finais são, ao mesmo tempo, a primeira linha de defesa contra os ciberataques e o elo mais fraco da cadeia de cibersegurança. É estimado que 90% dos ciberataques são causados por comportamento humano, ou seja, é sempre importante a difusão e aumento da cibersegurança.

TIpos de vírus/malware e prevenções segundo o site Estratégia:

Prevenção geral: no geral, as ações básicas para se defender de vírus, malware e ameaças cibernéticas é a instalação de um antivírus, antispyware e defender decente e a constante atualização do sistema.

Malware: é resultado da combinação das palavras inglesas “malicious” e “software”. O termo malware, portanto, abrange todo software malicioso que pode ser perigoso para o seu computador. Isso inclui vírus e cavalos de Tróia.

Ransomware: é um malware que bloqueia as ações ou encripta os dados do computador e pede ‘’dinheiro de resgate’’ para desbloqueá-las. a palavra ransomware vem de ransom (resgate, dinheiro de resgate) e ware (software). é responsável por milhões de dólares serem perdidos todos os dias, já que, os ataques ransomware tendem a focar pessoas de classe mais alta e até mesmo agentes do governo. graças a seu lucro constante, o ransomware está constantemente evoluindo. uma forma boa de se prevenir desta ameaça é um backup de dados preventivo.

Trojan: Não é considerado exatamente como um vírus ou como um worm. Trojan é o nome genérico para a entrega de malware. Ele se passa por um programa que tenha alguma utilidade para o usuário, coisas como versões ‘’gratuitas’’ de aplicativos como o photoshop, antivírus falsos ou filmes pirata. na realidade, este esconde um programa que pode infectar seu computador e facilitar com que outros usuários invadam ele, podendo até roubar senhas. Os meios de evitar a infecção são: evitar sites, links e downloads de aparência duvidosa e/ou ‘’boa demais para ser verdade’’.

Worms: são um tipo de malware mais perigoso do que o vírus comum, pois estes agem autonomamente e podem se auto-replicar inúmeras vezes em diferentes partes do computador, eles podem infectar o computador a partir de brechas e o acesso de sites perigosos. Eles podem roubar dados do computador e até se espalhar pela rede para outros

computadores, podendo infectar até mesmo os de empresas, Worms também podem abrir brechas para malwares mais perigosos poderem invadir a máquina.

Spyware: É um software destinado a coletar dados de um computador ou outro dispositivo, e encaminhá-los a terceiros sem o conhecimento do usuário.Os spywares podem ser desenvolvidos por firmas comerciais que desejam monitorar o hábito de seus usuários, sem eles saberem, para entender seus costumes e vender esses dados pela internet.

Autorun: ‘’autorun’’ é um recurso do windows que permite a auto execução de softwares e afins, foi criado para facilitar instalações. Porém, certos tipos de vírus podem tomar vantagem deste recurso, os vírus autorun ficam escondidos em pen-drives cds ou dvds infectados, que depois de instalados, mostram um ícone falso que silenciosamente infecta a máquina. um método de prevenção é desativar o recurso de autorun.

Keylogger: são sistemas maliciosos que monitoram cada tecla que o usuário pressiona no teclado, a fim de monitorar as ações deste. são considerados um tipo de spyware.

Adware: É um software projetado para criar e exibir anúncios no computador, redirecionar suas pesquisas para sites de anunciantes e coletar seus dados para fins de marketing. normalmente agem secretamente e podem certas vezes ter motivos legítimos para estarem no computador, tornando os às vezes imunes a antivírus. seu nome origina da combinação das palavras ‘’ad’’ (anuncio) e ‘’ware’’ (software).

Principais erros que os usuários cometem e suas consequências

Com base no artigo “Veja erros comuns relacionados à cibersegurança que muitas empresas cometem”, do site E-commerce Brasil, um dos erros mais comuns e que ainda cometem são o uso de senhas fracas e fáceis de adivinhar , ou até salvar senhas e acessos em um documento. Muitos outros erros são cometidos como ignorar as atualizações dos softwares e testes de segurança, não utilizar cofre de senhas, e confiar apenas em um antivírus , esses são os erros que toda empresa ou usuário que não tem conhecimento ou experiência são comuns de serem.

Provavelmente um dos erros mais perigosos em questão de cibersegurança é a instalação ou acesso de programas, links, sites perigosos, estes podem em alguns casos levar a máquina em um estágio onde uma formatação é basicamente obrigatória, alguns podem até mesmo formatar seu computador de uma vez só, fazendo você perder todos os arquivos nele salvos.

As consequências são óbvias: roubo de senhas, roubo de informações ou de documentos, perda de privacidade, sem contar os arquivos que danificam seu dispositivo abrindo páginas web ou compartilhando arquivos, roubos de dinheiro graças ao roubo de contas bancárias, etc.

Com todos esses riscos, de alta probabilidade, levam usuários a usar antivírus e se aprofundar na cibersegurança, procuram entender mais sobre como se proteger de vez , trazendo assim mais usuários para a área da cibersegurança.

Outra coisa que vale destacar no quesito de cibersegurança é que as ações de um usuário podem trazer consequências a outros, elas incluiriam: a instalação de Worms (já que estes podem infectar outros computadores na mesma rede e causar estragos imensos), o compartilhamento de vírus, sites ou links maliciosos com ou sem a consciência de que estes sejam perigosos, e o compartilhamento de falsa informação em relação a cibersegurança. Estas ações precisam sempre ser evitadas, pelo bem do usuário e também de outros.

Conclusão

Com a pesquisa, o grupo aprendeu um grande número de coisas envolvendo a cibersegurança, ameaças virtuais, tipos de vírus, etc. Também aprendemos sobre como se proteger na web. Outros conhecimentos também se expandiram como a funcionalidade de antivírus, o jeito que certos vírus funcionam e os tipos de cibersegurança.

Referências

SAP. O que é cibersegurança?. Disponível em: https://www.sap.com/brazil/products/financial-management/what-is-cybersecurity.html. Acessado em: 23 de agosto de 2023.

Softsell. Cibersegurança: entenda como funciona e qual o objetivo dessa área. Disponível em: https://www.softsell.com.br/ciberseguranca-entenda-como-funciona-e-quais-o-objetivo-dessa-area/. Acessado em 22 de agosto de 2023.

e-commercebrasil. Veja erros comuns relacionados à cibersegurança que muitas empresas cometem. Disponível em: https://www.ecommercebrasil.com.br/noticias/erros-ciberseguranca-empresas-first-tech Acessado em 23 de agosto de 2023.

Security Report. Parcerias e terceirização são caminhos para o GAP de profissionais em SI?. Disponível em: https://www.securityreport.com.br/ciberseguranca-escassez-de-profissionais-e-aspectos-sensiveis-dos-negocios/. Acessado em 18 de agosto de 2023.

Projeto Acadêmico. Pesquisa Quali-Quantitativa. Disponível em: https://projetoacademico.com.br/pesquisa-quali-quantitativa/. Acessado em 5 de Agosto de 2023.

Estratégia. Resumo sobre os tipos de Malware em Informática para Concursos. Disponivel em: https://www.estrategiaconcursos.com.br/blog/resumo-tipos-de-malware/. Acessado em 6 de Agosto de 2023.