CIBERSEGURANÇA

Walker Douglas Garcia Pinto[1]
João Padilha Moreira[2]
Anderson Silva[3]

RESUMO

Neste artigo irei abordar alguns conceitos básicos sobre segurança da informação. Conceitos estes que são primordiais para a implementação e sustentação segura de projetos e rotinas diárias. Também irei abordar brevemente tipos de ataques cibernéticos, como eles são nocivos caso sejam explorados com sucesso e como se proteger destes ataques

Palavras-chave: Vírus, Malware, Ransoware, VPN, Segurança da Informação.

CYBER SECURITY

ABSTRACT

In this article I will cover some basic concepts about information security. These concepts are essential for the implementation and safe support of projects and daily routines. I will also briefly cover types of cyber attacks, how harmful they are if they are successfully exploited and how to protect against these attacks.

Keywords: Viruses, Malware, Ransoware, VPN, Information Security.

[1] Acadêmico do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. walker.garcia@alcidesmaya.edu.br

[2] Professor do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. joao_moreira@alcidesmaya.edu.br

[3] Professor do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. anderson_silva@alcidesmaya.edu.br

INTRODUÇÃO

Atualmente é muito comum ouvirmos falar sobre os termos, segura da informação, cyber security ou segurança cibernética. Todos eles significam absolutamente a mesma coisa, um padrão ou conjunto de especificações as quais visam tornar um fluxo, processo ou ambiente seguro. Tais práticas envolvem, dispositivos de camada física, camada lógica e camada pessoal (humano), quando todos estes 3 itens, estão de em total acordo, podemos afirmar que há uma maturidade no quesito segurança da informação.

Ter um ambiente seguro, está altamente associado a ter um firewall, antivírus e outros dispositivos de camada física e lógica, porém S.I(Segurança da Informação), vai além destes conceitos. Existe atualmente frameworks específicos para auxiliar no planejamento de ambientes, desenvolvimento de software seguro e resposta a incidentes de segurança.

Para elucidar tais frameworks, podemos citar o OWASP, NIST Framework, MITRE ATT&CK® e o Cyber Kill Chain.

O QUE É CIBERSEGURANÇA?

Este termo também conhecido como cyber security ou segurança da informação, é um conjunto de padrões, normas e práticas, que visam tornar ambientes seguros, ambientes estes compostos por dispositivos, sistemas e pessoas. Como pode-se observar, existe um item a ser protegido, os qual não está ligado diretamente a tecnologia, “pessoas”.
Quando falamos do fator humano, este é um dos mais vulneráveis, pois não se há controle sobre ações as ações humanas, irei abordar ainda neste artigo. técnicas que exploram este fator.

4º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396
Centro Histórico de Porto Alegre – Rio Grande do Sul – outubro – 2020.

Quando falamos sobre fatores tecnológicos, tais como: sistemas, dispositivos, roteadores etc. há a possibilidade de sermos preditivos em mantê-los seguros, aplicando políticas de acesso, controles de acesso físicos e lógicos, mantendo-os atualizados e implementando camadas extras de proteção. As camadas extras, quando estamos falando de redes e aplicações WEB, podem ser, Firewalls, Firewalls para aplicações WEB (WAF), IPS, IDS, essas camadas auxiliam o administrador de redes ou responsável pela segurança de redes, a terem maior controle sobre o que é trafegado, de onde vem, para onde vai, podendo assim filtrar o tráfego legítimo do tráfego malicioso.

Pois bem, este é o conceito que a grande maioria do sysadmins tem sobre S.I (Segurança da Informação), mas devido ao crescente aumento de ataques, vírus, malwares, fraudes e surgimento dos ransomwares, foi necessário criar padrões que vão além de firewalls, pois este são facilmente burláveis e muitas vezes não possuem inteligências para mitigar ataques que não são direcionados a redes.

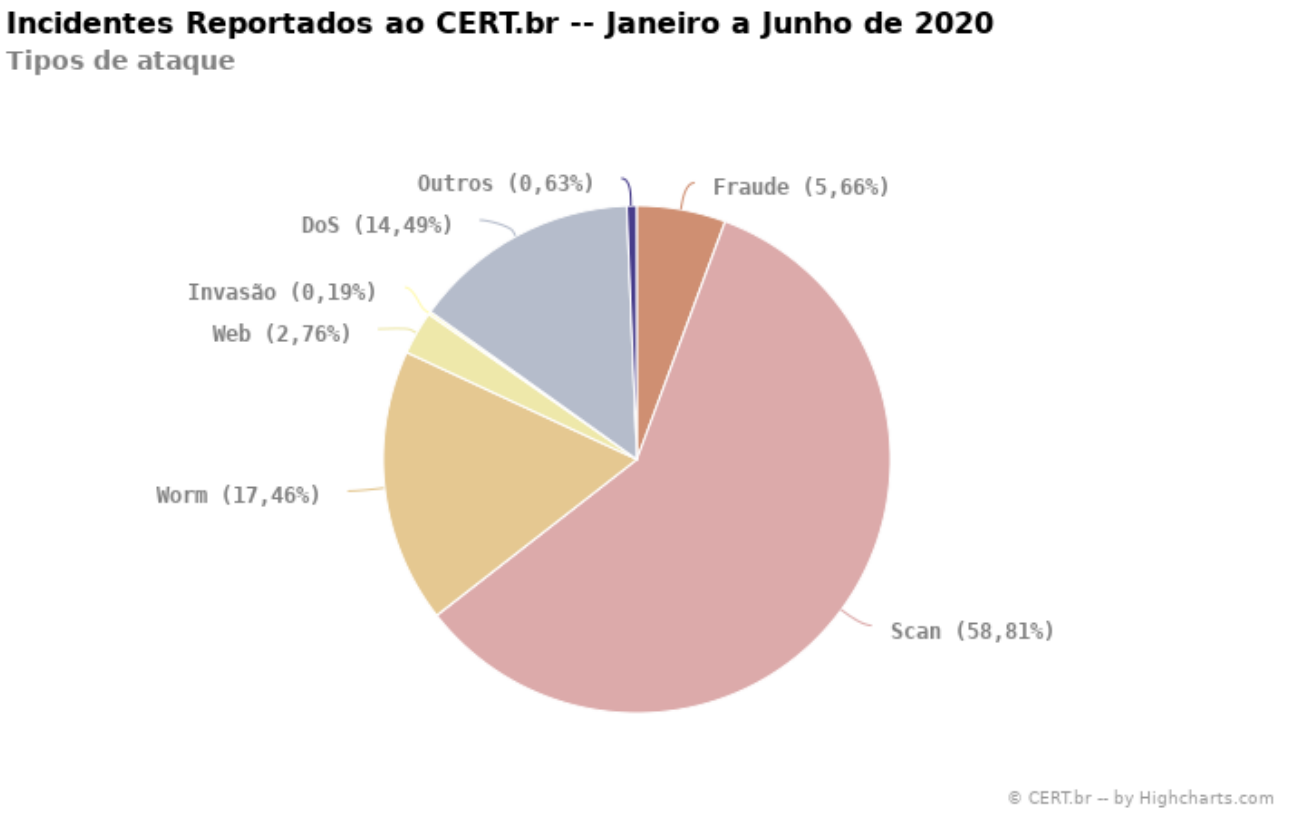
TIPO DE ATAQUES

Devido à complexidade das mais diversas ameaças, foram necessários categorizá-las, até mesmo para que possam se tratadas em uma resposta a incidentes de segurança.

Baseado em dados do portal cert.br, no primeiro semestre de 2020, os principais tipos e ataques detectados foram, Worm, DoS, invasão, web, scan, fraude e outros.

4º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396
Centro Histórico de Porto Alegre – Rio Grande do Sul – outubro – 2020.

Figura 01 – Incidentes Reportados



Fonte: Cert.br, 2020

Worm: Ameaças relacionadas a códigos maliciosos, os quais tendem a executar funções não autorizadas em sistemas, tais como, escalar privilégios, obter informações e roubar dados.

DoS: (Denial of Service), ataque visa interromper o acesso a sistemas, serviços ou redes, este por sua vez, causa indisponibilidade através dos excessivos acessos não legítimos, este ataque pode também ser do tipo distribuído, o qual chamamos de DDoS (Distribuited Denial of Service). Para efetivá-lo, não é necessário explorar sistema ou redes, mas apenas sobrecarregar sistemas com um número muito grande requisições.

4º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396
Centro Histórico de Porto Alegre – Rio Grande do Sul – outubro – 2020.

Invasão: Ataques que visam a exploração de sistemas devido a falhas de Dia 0 (Zero Day), os quais muitas vezes são efetivos, devido a sistemas não possuírem atualizações, patches de segurança aplicados, ou até mesmo, por serem sistemas antigos os quais não possuem mais suporte, mas ainda assim é possível explorar novos sistemas por falhas do tipo zero day.

Web: Este ataque está diretamente associado a sistemas WEB, como sites, portais, sistemas, formulários, lojas online e afins , dentro desta categoria, possuímos ataques do tipo XSS, SQL Injection, falhas as quais explorem sistemas mal programados, que geralmente não possuem mecanismos básicos de validação em campos de inserção de dados ou tratamento de chamadas internas.

Scan: Este não é de fato um ataque, mas sim uma fase primordial para execução de ataques, a qual visa identificar possíveis portas, serviços, tipos de sistemas operacionais e outras informações que serão utilizadas para descobrir fragilidades que possam comprometer o sistema.

Fraude: Este é um tipo de “ataque” que cresceu muito nos últimos anos, as fraudes podem envolver cartões de crédito, roubo de contas em redes sociais, transações falsas, como venda de imóveis, veículos, extorsão e chantagem.

Outros: Outros ataques que não os listados acima, podendo ser, um defacement por exemplo, tipo de ataque que visa desconfigurar sites.

COMO POSSO MANTER MEU AMBIENTE SEGURO?

Conforme descrito na introdução deste artigo, para manter o seu ambiente seguro, é indispensável seguir os principais frameworks de segurança da informação.

Os padrões adotados, visão manter um ambiente seguro e estável, levando em consideração o desenvolvimento de software, processos, infraestrutura e pessoas.

4º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396
Centro Histórico de Porto Alegre – Rio Grande do Sul – outubro – 2020.

O QUE SÃO ESSES FRAMEWORKS?

Eles são um conjunto de regras e boas práticas, adotados e seguidos mundialmente pelas grandes empresas, dos mais variados ramos. Tais conjuntos de regras, vão desde frameworks específicos para desenvolvimento de software seguro, como padrões de segurança física em datacenters por exemplo.

OWASP: Framework voltado ao desenvolvimento seguro de software, que visa treinar desenvolvedores para que estes escrevem códigos seguros, pensem em segurança como requisito primordial para o início de qualquer projeto (Security by Design), fornecendo laboratórios e dojos, para que desenvolvedores provêm suas habilidades em sistemas, as quais são elencadas por criticidade e probabilidade de exploração.

NIST Framework Cybersecurity: O NIST (Instituto Nacional de Padrões e Tecnologia) é um órgão de defesa do governo norte americano, o qual possui um conjunto de boas práticas para que se tenha um ambiente seguro. Este sendo um padrão de referência utilizado por gigantes do mundo da segurança da informação, como a McAfee por exemplo e outras empresas de solução de segurança tecnológica, visa o manter seguro empresas do setor privado, porém sua prática pode ser utilizada nos mais diversos setores.

MITRE ATT&CK®: Uma base de conhecimento global, que organiza, identifica e cataloga ameaças, baseado em comportamentos do mundo real. O MITRE usa o conceito de ATP (Advanced Persistent Threat), que são grupos financiados geralmente por governos, que se utilizam de suas técnicas avançadas em desenvolvimento de malwares e ransomwares para prejudicar nações inimigas, criando assim uma verdadeira guerra digital.
O MITRE identifica e cataloga estes grupos como dito acima, baseando-se em comportamento, mas como isso ocorre ? Através da coleta de artefatos de malwares, técnicas de infecção, evasão e outras, as quais acabam se tornando uma marca registrada especifica de cada grupo.

4º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396
Centro Histórico de Porto Alegre – Rio Grande do Sul – outubro – 2020.

CYBER KILL CHAIN: Este framework é amplamente utilizado na resposta a incidentes, de modo que ele possuiu 8 passos, os quais auxiliam na identificação de um ataque a na mitigação deste ataque. Estes estágios podem ser combinados a uma matriz disponível no site do MITRE, o qual conforme foi citado, categoriza técnicas de reconhecimento, evasão, camuflagem, roubo de dados e outros. É muito importante possuir um plano maduro de resposta a incidentes, para minimizar os impactos no ambiente, tendo em vista que, um atacante pode ficar até 90 dias no ambiente sem ser notado.

CONCLUSÃO

Como descrito neste artigo, segurança da informação vai além de tecnologias de firewall, é necessário ser estratégico e preditivo, pensar como um atacante para se proteger. Treinar e certificar profissionais, criar e desenvolver equipes para funções específicas. A realização de testes de intrusão periódicos, é extremamente importante para manter um ambiente seguro, porém é necessário ter uma política rígida de correção das vulnerabilidades encontradas, com datas, responsáveis e associar as fragilidades a áreas de negócio, a fim de mensurar setores críticos de uma empresa. Instruir colaboradores a terem consciência de conceitos básicos de segurança, para que não sejam enganados em ataques de phishing, esta é uma técnica que utiliza o envio de e-mails supostamente verdadeiros, com promoções, oportunidades de empregos, brindes e outras vantagens. Outro ataque que utiliza a fragilidade humana, são ataques de engenharia social, o qual um atacante fornece algumas informações para obter outras mais privilegiadas, passando-se por alguém com um cargo importante, um atendente de suporte da empresa de telefonia que deseja “confirmar” a senha da sua rede Wireless. Por fim, ter normas e diretrizes claras, com prazos bem definidos, baseados nos frameworks que citei acima e outros como a ISO 27001 ou ISAE 3402, que descreve padrões de segurança para prestadores de serviços, irão manter o ambiente

4º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396
Centro Histórico de Porto Alegre – Rio Grande do Sul – outubro – 2020.

seguro, estável e pronto para responder a qualquer incidente de segurança, pois haverá um plano estratégico bem elaborado e consolidado.

REFERÊNCIAS:

Applying Security Awareness to the Cyber Kill Chain - SANS
https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain, Acesso em: 2020

CYBERSECURITY FRAMEWORK - NIST
https://www.nist.gov/cyberframework, Acesso em 2020

Incidentes Reportados ao CERT.br -- janeiro a junho de 2020, CERT.BR
https://www.cert.br/stats/incidentes/2020-jan-jun/tipos-ataque.html, Acesso em 2020

OWASP Security Knowledge Framework, OWASP
https://owasp.org/www-project-security-knowledge-framework/, Acesso em 2020

OWASP Top Tem - OWASP
https://owasp.org/www-project-top-ten/, Acesso em 2020

MITRE
https://attack.mitre.org/, Acesso em 2020