whoami

Flávio Cunha

Graduado em Redes de Computadores pela FIAP - SP. Especialista em Segurança da Informação e Engenharia *web/mobile* pelo Centro Universitário Senac. Possui 22 anos de experiência com os temas de Segurança da Informação e *Cybersecurity*. Consultor atuante em empresas e instituições dos mais diferentes segmentos (Serviços de TI, *Call Centers*, Distribuidoras, Varejo, Setor Financeiro e Área da Saúde). Também exerce atividades acadêmicas, atuando como professor na faculdade Impacta Tecnologia, onde é docente dos módulos: Metodologia de análise de vulnerabilidades e *Business Continuity Management & CyberLaw*.

Especialista em Linux e sistemas *Foss* (*Free and Open Source Software*), foi um dos primeiros profissionais do Brasil a obter as certificações *Linux Professional Institute* LPIC1 e LPIC2. Recentemente obteve a certificação em *Cybersecurity* (CC) pela organização ISC2.

INTRODUÇÃO AO TEMA

- **CONTEXTO ATUAL E DESAFIOS**

nessusd &

1. Afinal, o que são vulnerabilidades?

- Uma vulnerabilidade é uma fraqueza ou deficiência em um sistema, processo, aplicativo, pessoa ou organização que pode ser explorada por uma ameaça para causar danos. Ex: indisponibilidades, roubos, destruição de informações, acessos não autorizados.

nmap -n -sV -p 80,8080,443 alvo.com.br

2. Vulnerabilidades && Ameaças && Riscos

- A **vulnerabilidade** é uma falha que pode ser explorada. A **ameaça** é o agente que pode explorar a vulnerabilidade para causar uma violação de segurança e o **risco** representa a probabilidade de uma ameaça explorar uma vulnerabilidade. Sendo que, o Graú de risco pode ser estimado através da fórmula:

Graú de risco = Probabilidade X Impacto

Desafios

1. Problemas a serem resolvidos dentro do processo de gestão de vulnerabilidades

- Identificação das vulnerabilidades.
- Priorização de riscos.
- Mão de obra qualificada.
- Custos.
- O contexto atual é desafiador:
  1. **Cenário de ameaças em constante evolução**: Novas tecnologias e vulnerabilidades.
  2. **Regulamentações e normas (conformidade):** GDPR, LGPD, PCI DSS e outras.
  3. **Impacto dos ataques cibernéticos:** Custos financeiros, danos à reputação, interrupção dos negócios.

Decisões que envolvem riscos dentro do contexto da gestão de vulnerabilidades

Mitigar ou reduzir o risco

- Mitigar ou reduzir o risco. Por exemplo: aplicar um *patch* de segurança ou fazer alguma correção na fonte de risco de um determinado ativo.

Transferir o risco

- "Terceirizar o risco". Por exemplo, o risco pode ser transferido para um parceiro terceirizado.

Decisões que envolvem riscos dentro do contexto da gestão de vulnerabilidades

Aceitar o risco

- Esta ação pode ser tomada quando o risco é classificado dentro de um limite aceitável pela companhia. Desta forma, nenhuma ação é tomada para eliminá-lo. Entretanto, outros fatores como regras de negócio podem levar uma empresa a aceitar um risco. E para estes casos, recomenda-se a formalização da decisão através da assinatura de um "**termo de aceite de risco**" previamente definido.

Evitar o risco

- Parar ou simplesmente descontinuar um ativo ou atividade que esteja sendo considerada como uma fonte de risco. Por exemplo: retirar do parque todas as estações com Windows 7 que são vulneráveis ao exploit EternalBlue – MS17-010. Neste caso, estamos eliminando a fonte do risco.

Atores por trás das ameaças

Hacker Black Hat

- Domina as principais técnicas para invasão de sistemas. Possui conhecimentos avançados sobre sistemas operacionais, redes, protocolos, linguagens de programação e criptografia. Usa estas habilidades para cometer ações criminosas e não age de acordo com a ética.

Atores por trás das ameaças

Hackativistas

- Possuem as mesmas habilidades do *hacker Black Hat*, mas agem de acordo com uma ideologia. Podem direcionar ataques para uma ou mais organizações que estão em desacordo com os seus ideais e conjuntos de valores. Como exemplo, temos o grupo ***Anonymous*** que surgiu no início dos anos 2000 e ficou famoso por suas ações de protestos online. Seu "*modus operandi*" inclui desde ataques a sites governamentais até a divulgação de informações confidenciais.

Atores por trás das ameaças

Cibercriminosos

- São grupos especializados que objetivam obter acessos não autorizados em arquivos e sistemas, muitas vezes, usando *malwares* ou *ransomwares*. Os ataques usando *ransomwares*, por exemplo, tem por finalidade criptografar os arquivos da organização alvo e posteriormente pedir um resgate para envio da chave de descriptografia. Normalmente, os criminosos pedem o resgate em moeda digital e ainda podem solicitar um valor adicional para não divulgar as informações obtidas na Internet, *Deep web* ou *Dark web* (dupla extorsão). O *LockBit* e o *Netwalker* são exemplos de grupos envolvidos com a disseminação do *ransomware*.

Atores por trás das ameaças

Script Kiddie

- Possui conhecimento superficial da teoria por trás das técnicas de invasão. Entretanto, consegue utilizar ferramentas prontas para fazer invasões e obter acessos não autorizados.

Relatório anual de ameaças cibernéticas 2024 - **Sonicwall**

Principais pontos de atenção

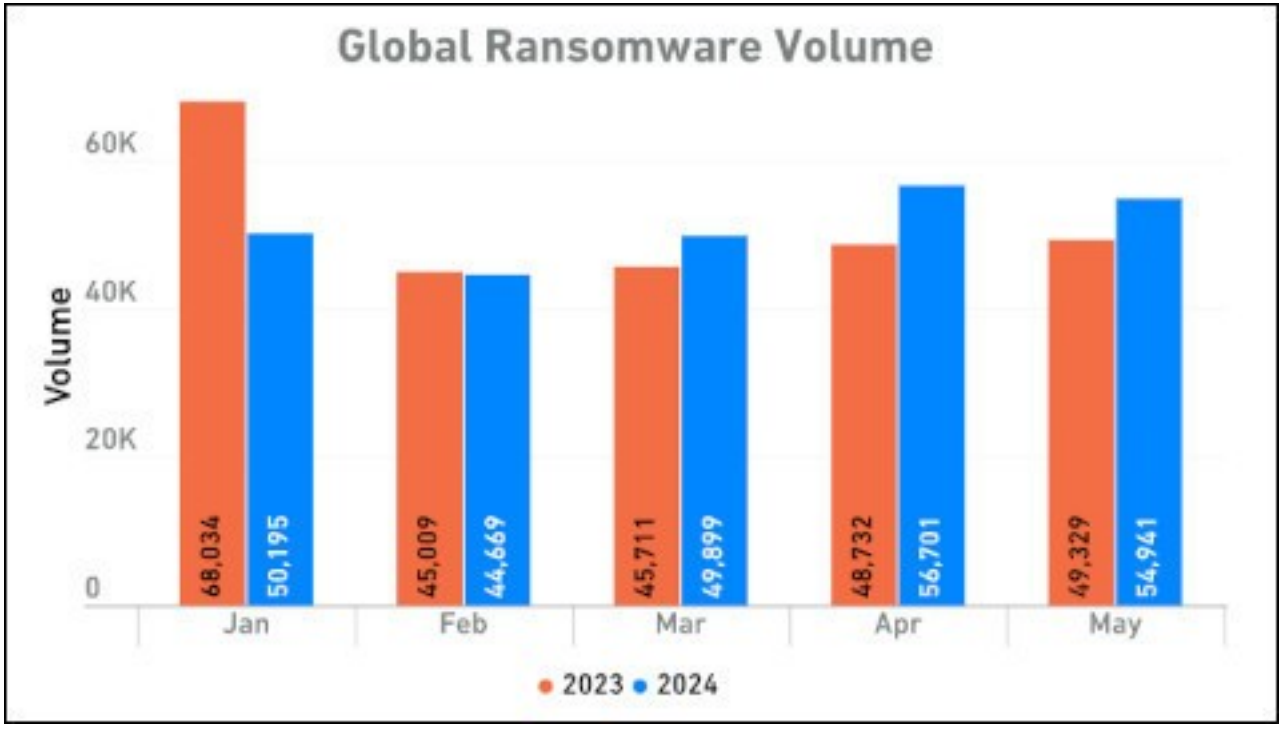
- A ameaça *malware* teve um aumento de 30% com relação ao mesmo período do ano passado.
- Aumento de *malware* na IOT (*Internet of things*): +107%.
- Aumento de *malware* nas ameaças criptografadas: +92%.

Relatório anual de ameaças cibernéticas 2024 - **Sonicwall**

Principais pontos de atenção

- Segundo o relatório, pelo menos 12,6% de todas as receitas das organizações estão expostas à ameaças cibernéticas sem a devida proteção. Em uma empresa de US$10 milhões, isto é equivalente a US$1,2 milhões.

Relatório anual de ameaças cibernéticas 2024 – Sonicwall: **Ameaça *Ransomware***



Considerações

- Aumento da ameaça *ransomware* nas Américas: América do norte (15%). América latina (51%). Entretanto, a região da EMEA (Europa, Oriente médio e África) está pressionando os números globais para baixo registrando uma queda de -49%. O que é positivo.

OPORTUNIDADES

- **OPORTUNIDADES. QUE A FORÇA ESTEJA COM VOCÊ!**

Oportunidades

Oportunidades dentro do cenário atual

1. **Inteligência Artificial e *Machine Learning*:** 1.1. A IA e o ML serão cada vez mais utilizados para identificar padrões de comportamento anômalo e detectar ataques em tempo real, antes que causem danos significativos. 1.2. A IA generativa será usada para criar ataques mais sofisticados e realistas, exigindo que as empresas desenvolvam defesas mais robustas.

2. **Segurança em Nuvem e Multicloud:** 2.1. A segurança será integrada desde o design das plataformas em nuvem, com foco em modelos de zero trust e criptografia. 2.2. As empresas precisarão adotar estratégias de segurança consistentes para gerenciar ambientes multicloud complexos

Oportunidades

Oportunidades dentro do cenário atual

3. IoT e segurança: A crescente adoção da Internet das Coisas (IoT) exigirá soluções de segurança específicas para proteger esses dispositivos vulneráveis.

4. Privacidade e regulamentação: 4.1. As leis de proteção de dados, como a LGPD no Brasil e a GDPR na Europa, continuarão a moldar as práticas de segurança das empresas. 4.2 **Privacidade by design**: A privacidade será integrada desde o início do desenvolvimento de produtos e serviços, com foco na proteção dos dados pessoais dos titulares.

Oportunidades

Oportunidades dentro do cenário atual

5. Computação Quântica: Ameaça aos algoritmos criptográficos atuais: A computação quântica representa uma ameaça potencial aos algoritmos criptográficos atualmente utilizados. Desta forma, a comunidade de segurança já está trabalhando no desenvolvimento de algoritmos criptográficos resistentes à computação quântica.

OBRIGADO!

Perguntas

https://www.linkedin.com/in/flavio-cunhaffc