Tempest

ACADEMY

Conference

2023

Engenharia social, Layer 8

Mitigando riscos com Gestão de Vulnerabilidades.

João Pedro Jordão

Tempest

ACADEMY

Conference

01 Engenharia Social, o que é?

02 Gestão de Vulnerabilidades, o que é?

03 Gestão de Vulnerabilidades + Engenharia Social

04 Conclusão

Engenharia Social, o que é?

Engenharia Social

Tempest
[ACADEMY]
Conference

Engenharia social é uma classe de ataques onde o atacante tem como objetivo persuadir pessoas para conseguir dados sensíveis, acesso de contas ou acessos a redes e sistemas.

Engenharia Social

Tempest
[ACADEMY]
Conference

A target of opportunity Attack:

- Maior distribuição.
- Em busca da melhor oportunidade.
- Normalmente sem foco específico.

Targeted:

- Foco no ataque a um indivíduo em específico ou a um pequeno grupo.
- Estudo externo, muitas vezes através do uso de redes social.
- Pode existir um contato prévio.

Clique para adicionar um título

Tempest

:ACADEMY:

Conference

Gestão de Vulnerabilidades, o que é?

Gestão de Vulnerabilidades

Tempest
[ACADEMY]
Conference

De acordo com o livro *“Practical Vulnerability Management”*, podemos definir Gestão de Vulnerabilidades como a prática de se manter atento às vulnerabilidades conhecidas em seu ambiente e, a partir desse conhecimento, resolver ou mitigar as vulnerabilidades para melhorar a postura geral de seu ambiente.

Gestão de Vulnerabilidades

Tempest
[ACADEMY]
Conference

Definido pela CISA tem como objetivo:

"Reduce the prevalence and impact of vulnerabilities and exploitable conditions across enterprises and technologies, including through assessments and coordinated disclosure of vulnerabilities reported by trusted partners."

Ciclo da Gestão

Tempest
ACADEMY
Conference

Fonte: Digital Defense

Tempest

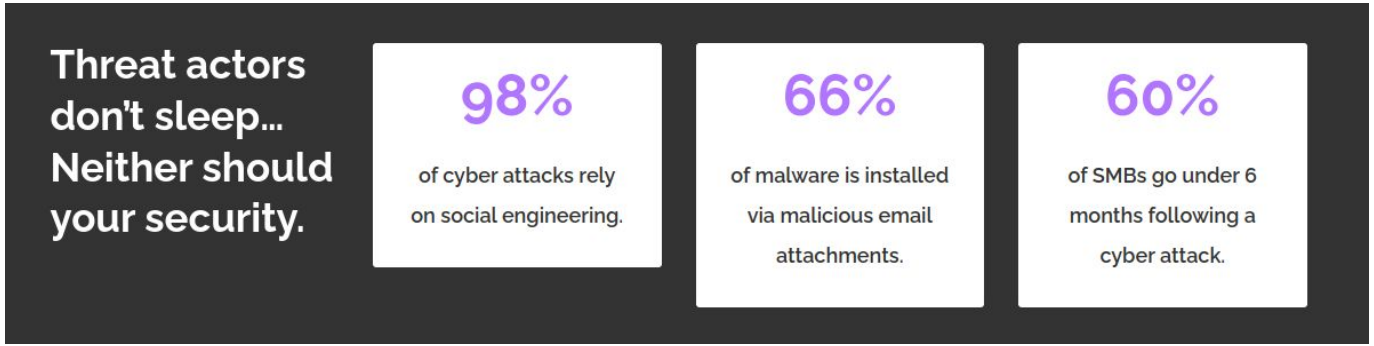
ACADEMY

Conference

Gestão de vulnerabilidades + Engenharia social

Motivação

- Fator Humano como maior causa de vazamento de segurança.
- Vishing tem um sucesso de 35%, mas quando somado ao Phishing sua taxa de sucesso sobe para 75%.
- A segurança da informação é dependente de 3 pilares: **Pessoas**, processos e tecnologia.



Fonte: Purplesec

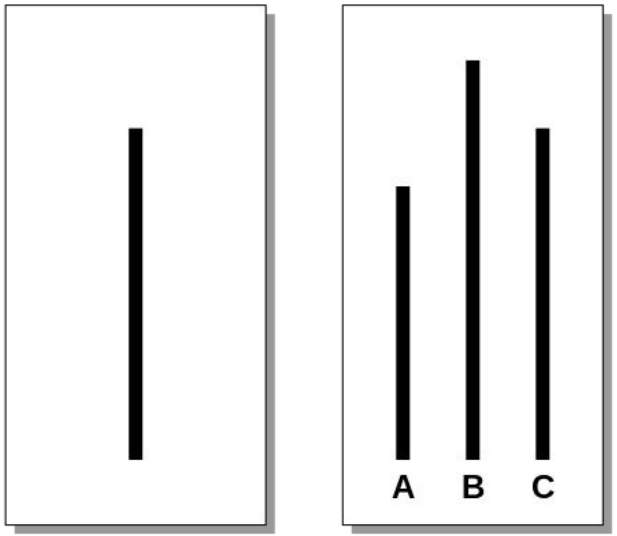
1ª fase: Detecção - Ataques

Tempest
[ACADEMY]
Conference

Tipos de ataques:
- Phishing
- Vishing
- Smishing
- Watering Hole Attack
- Pretexting
- Whaling Attacks

Vulnerabilidades Humanas:
- Reciprocidade
- Conformidade ou Prova social (Experimento de Asch)
- Simpatia
- Escassez
- Compromisso
- Autoridade

1ª fase: Detecção - Ataques

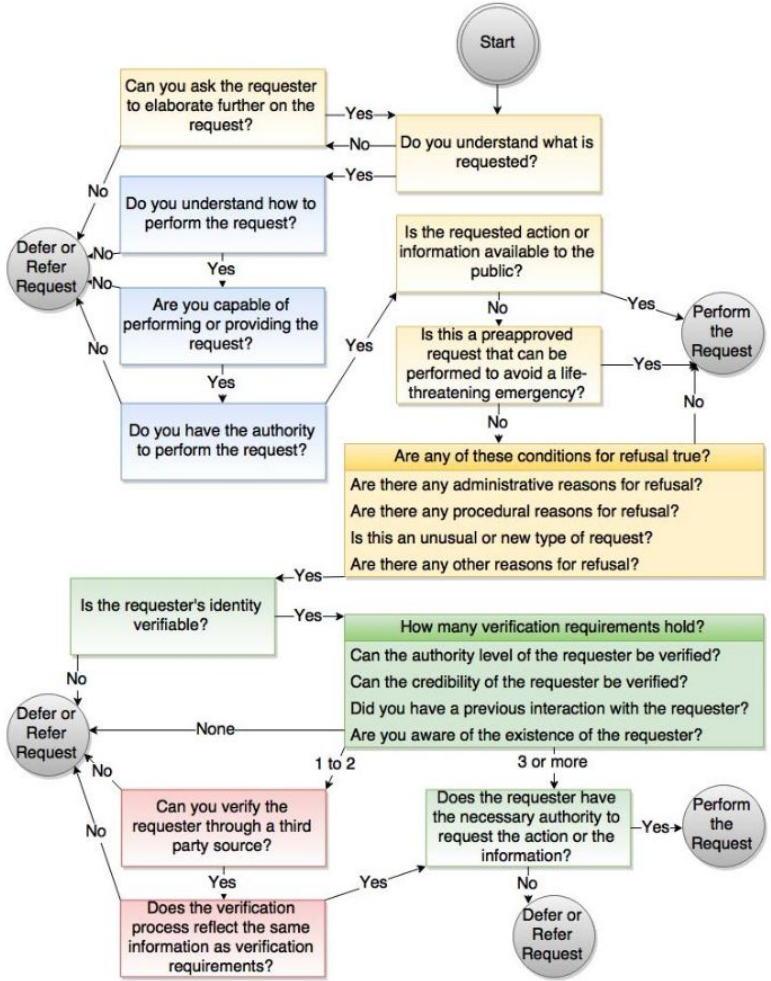


1ª fase: Detecção - Dificuldades

- Como são explorados.
- Como identificar pós exploração.

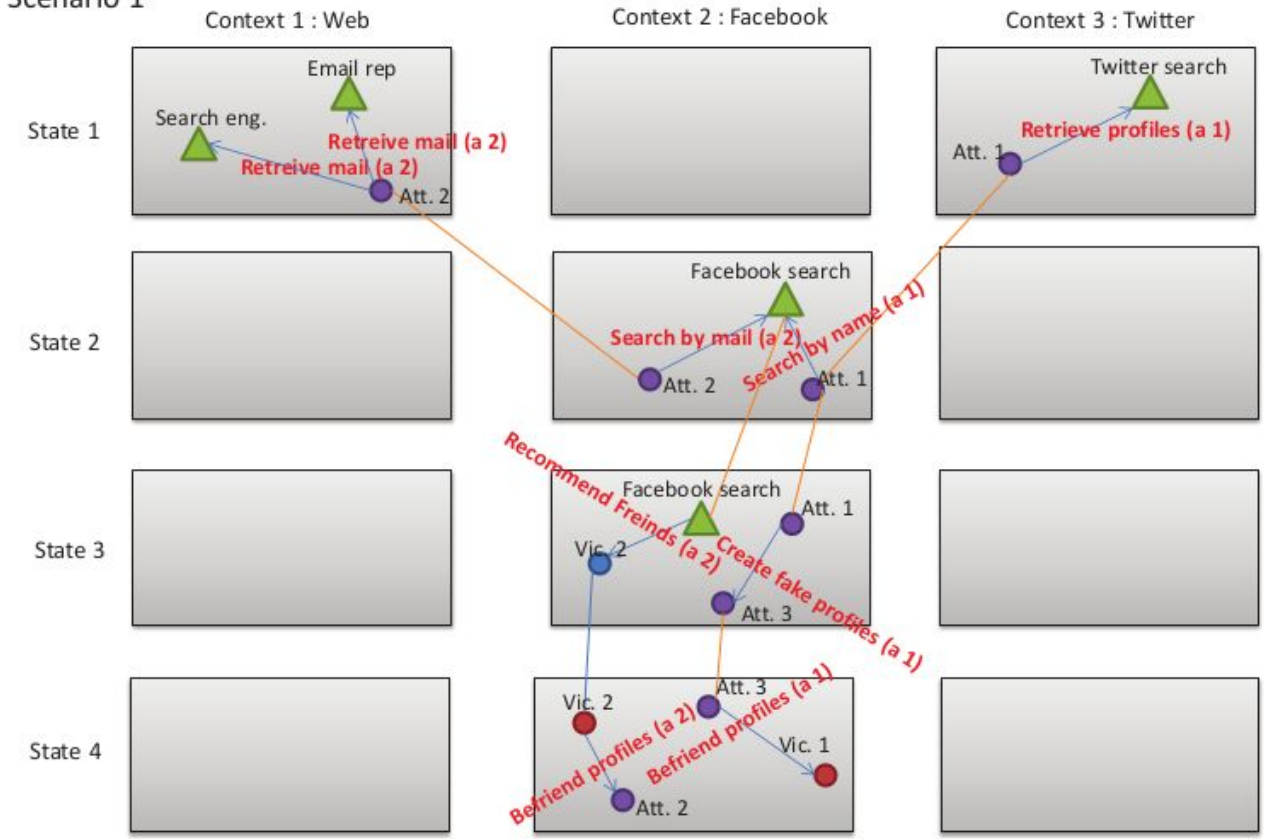
1ª fase: Detecção - Soluções

- Pentest contínuo
- Social Engineering Attack Detection Model (University of Pretoria)
- Multi Layered Graph Based (University of Technology of Troyes)



Tempest
ACADEMY
Conference

Scenario 1



2ª fase: Priorizar

Priorizar ativos:
- Identificar objetivos e tolerância de riscos da organização
- Importância do funcionário

Priorizar ataques:
- Severidade
- Exploração (Ex.: Keyloggers)
- Impacto
- Threat Intelligence

3ª fase: Avaliar

Tempest
[ACADEMY]
Conference

Nessa fase se torna necessário analisar os dados coletados até o momento.

4ª fase: Remediar

- **Constante intervenções (Cartazes, políticas, etc)**
- Garantia de detecções como SEADMv2
- Repasse de conhecimento sobre engenharia social

4ª fase: Remediar

The persuasion and Security Awareness Experiment(University of Twente):

- Hipóteses:

H1. O grupo que recebeu as intervenções estaria menos apto para sofrer o ataque.
H2. O grupo que não recebeu intervenções sofreria mais ataques diante de uma figura de autoridade.
H3. A intervenção diminuiria a relação entre autoridade e aceitação.

4ª fase: Remediar

The persuasion and Security Awareness Experiment(University of Twente):

- Hipóteses:

  H1. O grupo que recebeu as intervenções estaria menos apto para sofrer o ataque. **Accepted**

  H2. O grupo que não recebeu intervenções sofreria mais ataques diante de uma figura de autoridade. **Rejected**

  H3. A intervenção diminuiria a relação entre autoridade e aceitação. **Rejected**

4ª fase: Remediar

		Intervention		
		No	Yes	Total
Complied	No	27 (37.5 %)	29 (63.0 %)	56 (47.5 %)
	Yes	45 (62.5 %)	17 (37.0 %)	62 (52.5 %)
Total		72 (100 %)	46 (100 %)	118 (100 %)

		Authority		
		No	Yes	Total
Complied	No	26 (46.4 %)	30 (48.4 %)	56 (47.5 %)
	Yes	30 (53.6 %)	32 (51.6 %)	62 (52.5 %)
Total		56 (100 %)	62 (100 %)	118 (100 %)

5ª e 6ª fase: Verificar e Reportar

Tempest
[ACADEMY]
Conference

- Em que vetor por meio em que a maioria dos ataques são mais efetuados.
- Detectar quando eles acontecem.
- Mapear quais ‘Ativos’ são mais atingidos e sua criticidade.
- Apontar ‘correções’ possíveis.

Conclusão

- O “Fator Humano” é um ponto crítico para a segurança de qualquer sistema, uma vez que estão presentes em quase que todos os pontos de um arquitetura. No MITRE ATT&CK, aponta o em alguns pontos da corrente do atacante, como em sua fase de reconhecimento, inicial(Entrada na arquitetura) e movimentação lateral ou vertical.
- O gerenciamento da saúde da organização pode ser um fator crucial para mantermos o ambiente seguro.
- Pessoas não são máquinas, não existem patches de correção para as pessoas, mas existem processos que podem ser usados para que possamos evitar que o ataque ocorra. Os esforços para novas formas de detecção de ataques e identificação dos mesmos se tornam necessários para que possamos deixar os ambientes seguros.

Referências

[1] A. Cullen and L. Armitage, "The social engineering attack spiral (SEAS)," 2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security), London, UK, 2016, pp. 1-6, doi: 10.1109/CyberSecPODS.2016.7502347.

[2] Bullée, JW.H., Montoya, L., Pieters, W. et al. The persuasion and security awareness experiment: reducing the success of social engineering attacks. J Exp Criminol 11, 97–115 (2015). https://doi.org/10.1007/s11292-014-9222-7

[3] F. Mouton, A. Nottingham, L. Leenen and H. S. Venter, "Finite State Machine for the Social Engineering Attack Detection Model: SEADM," in SAIEE Africa Research Journal, vol. 109, no. 2, pp. 133-148, June 2018, doi: 10.23919/SAIEE.2018.8531953.

[4] Carrie Gates and Tara Whalen, Profiling the defenders, Proceedings of the New Security Paradigms Workshop, 107--114 (2004). https://doi.org/10.1145/1065907.1066044

[5] A. Cullen and L. Armitage, "A Human Vulnerability Assessment Methodology," 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), Glasgow, UK, 2018, pp. 1-2, doi: 10.1109/CyberSA.2018.8551371.

Referências

[6] M. Bezuidenhout, F. Mouton and H. S. Venter, "Social engineering attack detection model: SEADM," 2010 Information Security for South Africa, Johannesburg, South Africa, 2010, pp. 1-8, doi: 10.1109/ISSA.2010.5588500.
[7] F. Mouton, A. Nottingham, L. Leenen and H. S. Venter, "Finite State Machine for the Social Engineering Attack Detection Model: SEADM," in SAIEE Africa Research Journal, vol. 109, no. 2, pp. 133-148, June 2018, doi: 10.23919/SAIEE.2018.8531953.
[12] https://purplesec.us/learn/social-engineering/#GetStarted
[13] https://en.wikipedia.org/wiki/Watering_hole_attack
[14] https://blogs.cisco.com/security/department-of-labor-watering-hole-attack-confirmed-to-be-0-day-with-possible-advanced-reconnaissance-capabilities
[15] https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=f502d42f-d57c-4f6b-8bcd-45aec7764273&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
[16] https://www.kaspersky.com.br/resource-center/definitions/what-is-a-whaling-attack
[17] https://cxl.com/blog/cialdinis-principles-persuasion/#h-1-reciprocity-give-a-little-something-to-get-a-little-something-in-return

Referências

[18] https://www.youtube.com/watch?v=UGxGDdQnC1Y (Social Influence: Crash Course Psychology)
[19] https://pt.wikipedia.org/wiki/Experimentos_de_conformidade_de_Asch
[20] https://pt.wikipedia.org/wiki/Experi%C3%AAncia_de_Milgram
[21] https://www.youtube.com/watch?v=cFdCzN7RYbw
[22] https://en.wikipedia.org/wiki/Scarcity_(social_psychology)
[23] https://attack.mitre.org/
[24] F. Mouton, L. Leenen and H. S. Venter, "Social Engineering Attack Detection Model: SEADMv2," 2015 International Conference on Cyberworlds (CW), Visby, Sweden, 2015, pp. 216-223, doi: 10.1109/CW.2015.52.
[25] H. Aldawood and G. Skinner, “Educating and Raising Awareness on Cyber Security Social Engineering_Literature Review”, IEEE TALE Conference, Wollong, NSW, Australia, 2018, doi: 10.1109/TALE.2018.8615162