Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Renan Max Cazelle Vieira

ENGENHARIA SOCIAL: O IMPACTO EMPRESARIAL

Americana, SP
2022

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

Renan Max Cazelle Vieira

ENGENHARIA SOCIAL: O IMPACTO EMPRESARIAL

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob orientação do Prof. Esp. Bruno Henrique de Paula Ferreira.
Área de concentração: Segurança da Informação.

Americana, SP
2022

Renan Max Cazelle Vieira

ENGENHARIA SOCIAL: O IMPACTO EMPRESARIAL

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação.

Americana, 03 de dezembro de 2022.

Banca Examinadora:

Orientador(a): Bruno Henrique de Paula Ferreira
Especialista
Fatec Americana Ministro Ralph Biasi

Carlos Henrique Rodrigues Sarro
Mestre
Fatec Americana Ministro Ralph Biasi

Elton Rafael Mauricio da Silva Pereira
Mestre
Fatec Americana Ministro Ralph Biasi

AGRADECIMENTOS

Antes de tudo quero agradecer a Deus pela oportunidade do fôlego da vida, por toda força e determinação que precisei para chegar até aqui.

Agradeço imensamente à minha mãe Lúcia Regina Cazelle, por sempre me apoiar e incentivar a busca pelo conhecimento através do estudo com humildade, respeito e resiliência.

Agradeço ao meu orientador Prof. Esp. Bruno Henrique de Paula Ferreira por todo apoio, paciência e ensinamento na elaboração e supervisão do trabalho.

Agradeço à minha esposa Dra. Juliana Fernandes de Lima por todo apoio e paciência nos momentos mais difíceis.

Agradeço todos os professores do curso de Segurança da Informação da FATEC Americana, que sempre me auxiliaram e passaram o conhecimento da melhor forma possível.

Por fim, agradeço todos meus amigos que estiveram comigo desde o início do curso, apoiando, compartilhando conhecimento e cobrando quando necessário.

If you know the enemy and know yourself you need not fear the results of a hundred battles.

-San Tzu (The art of War)

RESUMO

A tecnologia está em constante evolução e issto acaba refletindo diretamente no desenvolvimento de mecanismos e ferramentas para o uso doméstico e corporativo, muitas delas planejadas para segurança da informação, algo que contribui muito para a segurança das pessoas e da organização, mas o principal ativo e, na grande maioria, a maior vulnerabilidade a ser explorada continua a mesma: Pessoas.

Todo sistema necessita de uma equipe ou pessoas específicas para realizar ajustes e monitoramento, isto torna esses responsáveis em vítimas potenciais da engenharia social. Neste trabalho será apresentado alguns pontos importantes sobre a Segurança da Informação no meio organizacional, também será discutido sobre a Engenharia Social, algumas técnicas e meios utilizados por *hackers, crackers* e profissionais da Tecnologia da Informação com intuito de identificar e evitar esse tipo de ataque com mais precisão e assertividade.

Serão apresentadas três vulnerabilidades conhecidas, que já foram exploradas, solucionadas e posteriormente divulgadas pelo CVE, afim de compreender como essas vulnerabilidades foram exploradas e o que foi necessário para que a exploração tenha sido efetiva. Essas vulnerabilidades exploradas possuem um mesmo padrão básico de efetividade que é a necessidade de aplicação da Engenharia Social, desta forma será abordado dois cenários diferentes: original e personalizado, onde o primeiro cenário, original, trata-se das características intrínsecas da vulnerabilidade e o segundo cenário, personalizado, é uma simulação da vulnerabilidade modificada manualmente retirando as características que envolvam a necessidade da Engenharia Social para explorar com êxito a vulnerabilidade.

Neste contexto a Engenharia Social funcionará como um filtro nos dois cenários, comprovando a eficiência de ter conhecimento sobre o assunto para mitigar um ataque ou exploração de alguma vulnerabilidade e a compração entre um cenário que não há treinamentos sobre o tema com um cenário que esteja mais preparado, treinado e conscientizado. Esses dados serão mensurados com auxílio da Calculadora de Vulnerabilidade do CVSS.

Palavras Chave: SEGURANÇA DA INFORMAÇÃO; ENGENHARIA SOCIAL; VULNERABILIDADE.

ABSTRACT

Technology is constantly evolving and this ends up directly reflecting on the development of mechanisms and tools for domestic and corporate use, many of them designed for information security, something that contributes a lot to the security of people and the organization, but the main asset and for the most part, the biggest vulnerability to be exploited remains the same: People.

Every system needs a team or specific people to perform adjustments and monitoring, this makes those responsible potential victims of social engineering. This work will present some important points about Information Security in the organizational environment, it will also be discussed about Social Engineering, some techniques and means used by hackers, crackers and Information Technology professionals in order to identify and avoid this type of attack with more accuracy and assertiveness.

Three known vulnerabilities will be presented, which have already been exploited, resolved and later disclosed by CVE, in order to understand how these vulnerabilities were exploited and what was necessary for the exploitation to be effective. These exploited vulnerabilities have the same basic standard of effectiveness, which is the need to apply Social Engineering, thus two different scenarios will be addressed: original and personalized, where the first scenario, original, deals with the intrinsic characteristics of the vulnerability and the second scenario, customized, is a simulation of the vulnerability modified manually, removing the characteristics that involve the need for Social Engineering to successfully exploit the vulnerability.

In this context, Social Engineering will work as a filter in both scenarios, proving the efficiency of having knowledge on the subject to mitigate an attack or exploitation of some vulnerability and the comparison between a scenario where there is no training on the subject with a scenario that is more prepared, trained and aware. These data will be measured using the CVSS Vulnerability Calculator.

Keywords: *INFORMATION SECURITY; SOCIAL ENGINEERING; VULNERABILITY.*

SUMÁRIO

LISTA DE FIGURAS

1. INTRODUÇÃO

O mercado da Informação e a tecnologia de forma geral vem crescendo muito nos últimos anos, principalmente após a pandemia do Coronavírus (COVID-19) que ocorreu no fim de 2019, sendo necessário aplicar o isolamento social no mundo todo, desta forma houve um grande aumento de pessoas trabalhando remotamente, fazendo reuniões e planejamentos através de ferramentas e aplicativos on-line.

Atualmente a informação é definitivamente mais valiosa do que nunca, havendo a necessidade de que seja implementado certos critérios e segurança para manter as informações pessoais e profissionais protegidas dos ciberataques de hackers e de qualquer pessoa não autorizada ao acesso.

Essa demanda ocasionou um aumento de interesse significativo das pessoas e organizações referente a segurança da informação, buscando conhecimento e formando profissionais qualificados e capacitados com intuito de compor a vanguarda da empresa anulando ou mitigando esses riscos potenciais. O conhecimento sobre a funcionalidade das redes, acessos e ferramentas de hacking possui a mesma base para o atacante e para a vítima, que pode ser uma pessoa aleatória ou na maioria das vezes uma organização, a grande diferença está no uso do conhecimento e se a bússola moral do indivíduo ou organização está inclinada para o bem ou para o mal.

2. SEGURANÇA DA INFORMAÇÃO

A segurança da informação refere-se aos processos e ferramentas projetados e implantados para proteger informações comerciais confidenciais contra acessos não autorizados, modificações, interrupções e destruições de processos e serviços, a fim de fornecer integridade, confidencialidade e disponibilidade (NIST, 2003).

Esses processos e ferramentas são extremamente importantes para preparar o ambiente ou a organização para eventuais ataques internos e externos. A Segurança da informação possui uma construção heterogênea, sua elaboração exige a necessidade de considerar questões técnicas, estruturais, organizacionais, comportamentais e aspectos sociais (DHILLON, 2004, p.260).

Há muitas definições a respeito da segurança da informação, visando os negócios, pode-se defini-la como um ato de proteger a informação garantindo desta forma a continuidade dos negócios, mitigando os danos e intensificando aomáximo o retorno dos investimentos, inclusive as oportunidades de negócios (ALVES, 2006, p.15).

No entanto, há outras definições que a abordam de forma mais didática, como o autor Sêmola menciona a segurança da informação no artigo publicado no Campus do Rio de Janeiro, sob título “Gestão da Segurança da Informação**:** uma visão executiva “ da seguinte forma:

> Uma área do conhecimento que se destina prioritariamente à proteção de ativos da informação, impedindo os acessos não autorizados e todas as alterações que sejam indevidas, além de garantir a todo tempo sua disponibilidade e integridade (SÊMOLA, 2003).

Existem três princípios básicos que são essenciais para sustentarem a Segurança da informação, são eles: Confidencialidade, Disponibilidade e Integridade, ilustrado na Imagem 1. De acordo com (STALLINGS, 2014) pode-se compreender os três pilares da Segurança da informação da seguinte forma:

- Confidencialidade: Garantia de que a informação só poderá ser acessada unicamente por pessoas explicitamente autorizadas, é uma

proteção dos sistemas de informação que impede que pessoas não autorizadas tenham acesso às informações.

- Disponibilidade: É a certeza de que a informação estará sempre disponível a qualquer momento em que for necessária e de qualquer lugar.
- Integridade: A partir do momento que a informação foi armazenada, ela deve ser recuperada em seu formato original, sem qualquer alteração, garantindo a proteção dos dados e informações contra qualquer modificação intencional ou acidental que não esteja devidamente autorizada.

Imagem 1: Os 3 Pilares da Segurança da Informação

Fonte: AMARAL, 2015, Política de Segurança da Informação, p.4.

3. ENGENHARIA SOCIAL

A palavra Social, segundo (FERREIRA, 1999) no dicionário Aurélio de língua portuguesa refere-se à vida, relação de uma comunidade, sociedade e relacionamento entre indivíduos. Já a palavra engenharia é definida como a aplicação de métodos científicos ou empíricos à utilização de recursos da natureza em benefício ao ser humano.

Engenharia Social de forma geral é a ciência de manobrar os seres humanos de forma habilidosa para agirem em algum aspecto de suas vidas.

Segundo (HADNAGY, 2011) no livro *Social Engineering The Art of Human Hacking engenharia social é*: “O ato de manipular uma pessoa para tomar uma ação que pode ou não ser do melhor interesse do alvo. Seja obter informações, acessos ou fazer com que o alvo execute determinada ação.”

Essa ferramenta possui uma definição muito ampla e é usada todos os dias por pessoas comuns em situações cotidianas. Uma criança tentando convencer os pais a comprar doces ou um funcionário que solicita um aumento de salário está usando engenharia social. Infelizmente, também é usada por criminosos, vigaristas e pessoas de má índole para enganar outras pessoas com intuíto de obter informações que as tornem vulneráveis aos crimes. A engenharia social não pode ser classificada como algo bom ou ruim, pois como toda ferramenta ela é usada para usos diversos.

Um profissional de psicologia utiliza uma série de perguntas muito bem elaboradas para conseguir ajudar seu paciente a chegar à conclusão de que as mudanças de alguns aspectos são necessárias, da mesma forma que um criminoso usará perguntas específicas e bem concebidas para conseguir colocaro seu alvo em uma posição vulnerável. Os dois exemplos possuem objetivos e resultados completamente diferentes, mas ambos são caracterizados como engenharia social.

A engenharia social em relação ao meio tecnológico, quando visa a quebra de segurança de algo ou alguém possui uma outra definição, de acordo com o site (KASPERSKY, 2022): É uma técnica empregada por criminosos virtuais para induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com *malware* ou abrir *links* para sites infectados. Além disso, os hackers podem tentar explorar a falta de conhecimento do usuário.

3.1. Ferramentas de Engenharia Social

Quando se fala sobre a Engenharia social é indispensável o uso de ferramentas tanto para o indivíduo que fará a investida utilizando as ferramentas quanto para a vítima do ataque. O conhecimento sobre as ferramentas aumenta a efetividade do ataque, mas também pode ser utilizado como meio de proteção pela vítima durante o embate, portanto possui um

impacto relevante entre o sucesso e o fracasso da situação. Existem diversas ferramentas que auxiliam nessa questão, neste trabalho será abordado e ramificado, de forma resumida em três pontos principais: Investida direta, Investida Indireta e Softwares e Aplicativos.

3.1.1. Investida Direta

São os métodos de engenharia social que exigem um contato direto com a vítima onde através de uma conversa pessoalmente, troca de mensagens ou ligação é possível obter informações valiosas a respeito de algo que seja do interesse do atacante, como dados pessoais de uma empresa, horários de entrada e saída dos funcionários, localização da sala central, qualquer informação que possa ser aproveitada e estudada.

Nesse método é indispensável que se crie uma relação de confiança com a vítima, fazendo com que ela se sinta confortável em lhe passar algumas informações de forma indireta e para isso existem algumas técnicas que podem ser aplicadas, como a Técnica de espelhamento, por exemplo.

A técnica de espelhamento consiste em espelhar as ações, comportamentos e falas da vítima, sendo assim ela pode ser categorizada em espelhamento verbal (quando o atacante utiliza os mesmos jargões, gírias e características de falas da vítima) ou físico (utilização dos gestos ou comportamentos involuntários da vítima), ao notar que foi estabelecido um nível de confiança com a vítima é possível identificar se ela está na esfera de influência, conhecida como o termo francês “Rapport” que consiste em criar uma relação de confiança.

Após concluir o *Rapport* e identificar que a vítima está confortável e relaxada com a situação é possível modelar o rumo da conversa/interação, neste momento o atacante faz pequenos testes, como uma pergunta sobre algo que avítima gosta e após a resposta dela o atacante reafirma com as mesmas palavras que também gosta do que a vítima disse ou faz algum gesto, como coçar a cabeça e verifica se a vítima faz algo parecido em seguida. Dessa forma o atacante guiará a conversa até obter a informação que deseja (MARCELO e PEREIRA, 2005, p.3)

É importante mencionar, porém, que esses métodos de relações onde cria-se um laço de confiança são, de certa forma, instintivas e em sua grande maioria motivadas por benefícios ou danos que elas podem resultar, mais ainda, o objetivo é o equilíbrio exato entre os possíveis danos e benefícios, nesse contexto pode-se afirmar que o ser humano está envolvido nessas relações de negociações, quase que o tempo todo, segundo as ideias de (LAWLEY e TOMPKINS, 1994).

3.2. Investida Indireta

Os ataques por método de investida indireta são aqueles que não necessitam de contato verbal ou pessoal diretamente com a vítima, são estratégias e ferramentas que induzirem a vítima para cair em uma determinada armadilha, por meio de mensagens de textos, e-mails maliciosos, mídias físicas e outros meios.

Contudo nessa categoria há a necessidade de que a vítima interaja com o método utilizado pelo atacante e não diretamente com o atacante. Em um ataque por e-mail por exemplo, a vítima deve clicar no link malicioso para que o ataque tenha início e seja bem-sucedido. Aqui também existem inúmeros métodos de ataques, dentre eles alguns termos mais conhecidos como: Phishing, Baiting, Spoofing, entre outras.

3.2.1. Phishing

Segundo as ideias de (STRAVROULAKIS, 2010), pode-se definir que a investida indireta mais comum é por meio de “Phishing”, uma técnica que consiste na elaboração de uma mensagem de texto ou e-mail com um assunto do interesse da vítima, o objetivo nesse método é que a vítima se sinta atraída pelo conteúdo da mensagem e acabe clicando em algum link contido na mensagem, este link direcionará a vítima para alguma página suspeita pré-programada pelo atacante, ao clicar a vítima acaba concedendo informações pessoais de localização e sistema ou fazendo algum download malicioso que vai infectar a máquina, liberando acessos para o atacante que resultará em vazamentos de informações.

3.2.2. Baiting

Já o “Baiting” faz uso da curiosidade natural das pessoas, consiste basicamente em uma mídia física infectada, seja ela um cd, dvd, pen-drive, hd externo, entre outros. Essa mídia física é “esquecida” (de forma proposital) pelo atacante em algum lugar visível da organização e fica à espera de aguçar a curiosidade de alguma vítima, se a pessoal conectar a mídia em seu computador para verificar o que possui armazenado ela será imediatamente infectada por malwares contidos na mídia física (NORTON, 2021).

3.2.3. Spoofing

Por fim, no terceiro método “Spoofing” citado anteriormente, é muito parecido com o Phising e geralmente é utilizado junto de outros métodos, pois necessita previamente de uma coleta de informações da vítima, esse ataque utiliza as informações obtidas para adentrar no sistema se passando pela vítima, basicamente é uma falsificação de acesso onde o atacante se infiltra e realiza o ataque utilizando todas as informações e acessos da vítima, para isso é necessário obter endereçamento de IP, DNS ou e-mail. O atacante simula um endereço de IP confiável para editar uma página na internet e induz a vítima a digitar os dados de login interno nesse endereço, os dados digitados vão para o banco de dados do atacante que conseguirá infiltrar direto no sistema, (TANASE, 2003).

3.3. Softwares e Dispositivos

Esse método “sequestra” os dados da vítima por meio de programas e dispositivos equipados com softwares específicos para roubar e registrar informações da vítima, como equipamentos com GPS hacking instalados ou por ferramentas de inteligência online, como o Maltego, por exemplo. Conforme mencionado por (HADNAGY, 2011).

Referindo-se aos equipamentos de GPS *Hacking*, há o modelo *GPS TrackStick* g200 como exemplo na imagem 2. Esse dispositivo é projetado para ser instalado (de forma discreta e escondida do campo de visão) diretamente em veículos de locomoção, precisamente em qualquer parte metálica do veículo por meio de imã. Ele possui sensor de vibração para identificar se o veículo está em movimento e fornece informações sobre a rota exata, tempos das paradas,

velocidade alcançada e sentido de direção do veículo, sendo possível identificar a rota da vítima, seus pontos de paradas e a sua rotina.

Imagem 2: GPS TrackStick

Fonte: LUIZA, 2022, GPS tracker g200.

Todavia as ferramentas de coletas inteligentes de forma online são mais simples e fáceis de utilizar, o Maltego é um aplicativo *Open source* desenvolvido em Java que funciona perfeitamente em Sistemas Operacionais Windows, Mac e Linux, muito utilizado pelos profissionais da área de segurança, investigadores forense, jornalistas e até mesmo pesquisadores.

Esse aplicativo realiza uma varredura ou como é conhecido no meio da segurança “garimpagem de informações” correlacionando todos os servidores, *DNS*, *IP’s*, *email’s*, telefones, hospedeiros e até mesmo usuários. Com ele é possível realizar uma investigação minuciosa e muito bem detalhada, sendo necessário apenas o endereço de domínio do alvo. A interface do programa é exatamentecomo na imagem 3.

Imagem 3: Software Maltego

Fonte: MALTEGO, 2022, Maltego for windows.

4. CALCULADOR DO POTENCIAL DA VULNERABILIDADE

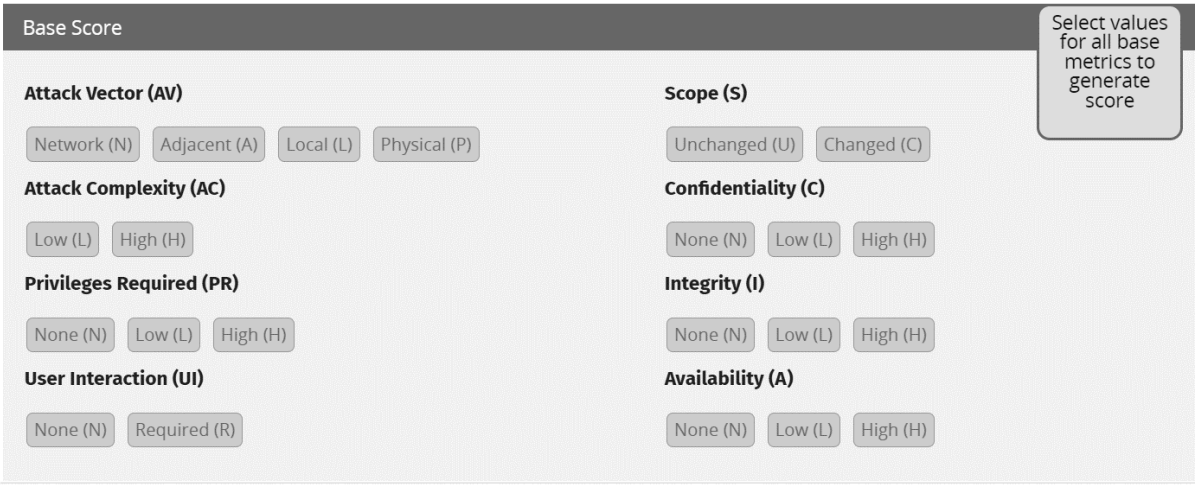
Para calcular o impacto das vulnerabilidades durante um ataque foi utilizada a calculadora de *Score* (FIRST, 2015). O *Common Vulnerability Scoring System* (CVSS) é uma estrutura aberta ao público, criada para comunicar características e gravidade das vulnerabilidades de inúmeros *softwares*, de forma geral trata-se de uma calculadora que mede o potencial e o impacto de uma determinada vulnerabilidade por meio de três grupos de métricas: *Base Score*, *Temporal Score* e *Environmental Score*.

Com o uso dessa ferramenta *web* é possível gerar uma escala de pontuação de 0.0 a 10.0, sendo 0 = Baixo risco e 10 = Alto risco, referente ao potencial do incidente de segurança, inserindo as informações e particularidades do ataque que foi feito e assim calcular os impactos que houveram na organização ou somente simulá-los. O resultado final pode variar em quatro escalas diferentes: Low = pontuação de 0.0 a 3.9, Medium = 4.0 a 6.9, High = 7.0 a 8.9 e Critical = 9.0 a 10.0.

4.1. Base Score

Esta métrica é responsável por representar as qualidades e características intrínsecas da vulnerabilidade que são constantes ao longo do tempo e aos ambientes dos usuários, incluindo metricas de explorabilidade e métricas de impacto, como ilustrado na imagem 4.

Imagem 4: Base Score



Fonte: FIRST, 2015. Common Vulnerability Scoring System. V.3.1

Attack Vector(AV): É a capacidade de exploração da vulnerabilidade durante o ataque.

Network(N): Vulnerabilidade que pode ser explorada remotamente.

Adjacent(A): Vulnerabilidade que pode ser explorada na mesma rede local (LAN) ou rede compartilhada, como bluetooth ou algum dispositivo que esteja conectado na rede interna, sub-rede ou IP local.

Local(L): Vulnerabilidade que precisa da interação de algum usuário/vítima para ser explorada, o usuário deve abrir algum arquivo malicioso, por exemplo.

Physical(P): A vulnerabilidade precisa que a vítima manipule fisicamente algum objeto malicioso, como colocar um pen-drive, cd/dvd ou arquivo de mídia infectado na máquina, por exemplo.

Attack Complexity(AC): É o nível de complexidade do ataque, se necessita de interações fora do alcance do atacante ou não.

Low(L): Não existe circunstâncias ou condições de acessos fora do alcance do atacante, é possível efetuar o ataque sem condições adicionais.

High(H): O sucesso do ataque depende de condições além do controle do atacante, como interação da vítima, por exemplo.

Privileges Required (PR): Refere-se ao nível de privilégio necessário que o atacante necessita durante o ataque para concluí-lo com êxito.

None(N): Não requer nenhum privilégio para efetuar o ataque.

Low(L): Requer privilégios que forneçam recursos básicos do usuário, geralmente afeta apenas configurações e arquivos do próprio usuário que possuem em sua grande maioria apenas informações e recursos “não sensíveis”.

High(H): Requer privilégios de controle significativo, geralmente acessos administrativos, permitindo total acesso. A engenharia social é muito utilizada nessa categoria.

User interaction (UI): Exigência de outra pessoa, além do próprio atacante, para concluir o ataque com sucesso.

None(N): Não necessita da interação de outra pessoa para concluir o ataque.

Required(R): O sucesso do ataque é totalmente dependente da interação de outra pessoa, seja através de execução de arquivo, clicando em links maliciosos ou configurações efetuadas pelo usuário que resultem em brechas de segurança.

Scope(S): Avalia o potencial da vulnerabilidade de afetar somente um componente ou se é possível impactar toda a estrutura do alvo além do seu escopo de segurança por meio do alvo inicial.

Unchanged(U): Quando o ataque não modifica o escopo, afeta somente o componente alvo, não repercutindo para outros recursos e equipamentos.

Changed(C): Quando a vulnerabilidade explorada tem potencial de afetar os recursos e equipamentos além do escopo de segurança, como um ataque que inicia em apenas uma máquina e consegue acesso ao roteador, infectando toda a destruição da rede interna do alvo.

Confidentiality(C): É o impacto para a confidencialidade dos recursos de informações devido a uma vulnerabilidade explorada com sucesso.

None(N): Não há alteração da confidencialidade no componente impactado, quando o atacante não consegue informações confidenciais.

Low(L): Há uma pequena perda de confidencialidade, quando o atacante consegue acesso a informações restritas e confidenciais, mas não tem controle sobre elas, neste caso a divulgação das informações obtidas não afeta a confidencialidade.

High(H): Perda total de confidencialidade, afetando todos os recursos dentro do componente impactado, quando o invasor consegue acesso às informações

extremamente restritas, como as senhas administrativas ou criptografia privada, por exemplo, que o invasor pode capturar essas informações e divulgar os dados sensíveis ou até mesmo negociar as informações obtidas.

Integrity(I): Impacto diretamente relacionado a confiabilidade e veracidade da informação.

None(N): Não há perda da integridade.

Low(L): Baixo impacto de modificação, modificação limitada que não ocasiona impacto considerável na integridade.

High(H): Perda total de integridade, o invasor consegue modificar qualquer arquivo protegido, as modificação impactam diretamente a integridade.

Availability(A): Perda da disponibilidade do componente impactado, como serviços *web*, aplicações, sites, entre outros, ausência de funcionamento de um serviço ou componente.

None(N): Não há impacto na disponibilidade.

Low(L): A disponibilidade do componente é levemente afetada, interrompendo alguns programas ou funções, mas não totalmente o componente afetado.

High(H): Perda total da disponibilidade, o atacante consegue interromper totalmente os serviços, acessos e funções do componente afetado, negando inclusive os novos acessos.

4.2. Temporal Score

A métrica Temporal reflete as características de uma vulnerabilidade que podem mudar ao longo do tempo, mas não entre os ambientes dos usuários, exemplificado na imagem 5.

Imagem 5: Temporal Score

Fonte: FIRST, 2015. Common Vulnerability Scoring System. V.3.1

Exploit Code Maturity (E): A maturidade do código de exploração está ligada à sua disponibilidade pública do código, a divulgação do código explorado, podendo ser o código autônomo, funcional ou ausência do código de exploração.

Not Defined(X): Não há informações suficientes para escolher algum dos outros valores.

Unproven(U): Nenhum código de exploração disponível, apenas teorias.

Proof-of-Concept (P): A prova de conceito é quando o código de exploração está disponível, mas não pode ser usado de forma prática em todos os sistemas, o código/técnica não é funcional em todas as situações, necessitando de modificações complexas.

Functional(F): A vulnerabilidade existe e o código de exploração está disponível, sendo funcional na maioria dos sistemas.

High(H): Existe o código autônomo funcional e seus detalhes estão amplamente disponíveis o código de exploração funciona em todos os sistemas.

Remediation Level(RL): O nível de remediação refere-se a urgência e efetividade da remediação da vulnerabilidade, podendo usar soluções alternativas e até “hotfixes” que oferecem remediação provisória.

Not Defined(X): Não há informações suficientes para escolher algum dos outros valores.

Unavailable(U): Não houve efetividade e urgência na remediação.

Workaround(W): Há soluções alternativas de remediações não oficiais disponíveis, como um *patch* próprio criado por algum usuário.

Temporary Fix(T): Há alguma solução oficial temporária disponível, isto inclui

o *hotfix*, geralmente uma solução momentânea até que seja resolvido de fato com alguma atualização.

Official Fix(O): Possui a solução oficial do fornecedor disponível, geralmente por meio de patch ou upgrade.

Report Confidence(RC): O relatório de confiança mede o grau de confiança, de certeza na existência da vulnerabilidade e toda a credibilidade dos detalhes técnicos conhecidos.

Não Defined(X): Não há informações suficientes para escolher algum dos outros valores.

Unknown(U): Há somente relatos de que a vulnerabilidade está presente, os relatórios indicam que a causa da vulnerabilidade é desconhecida.

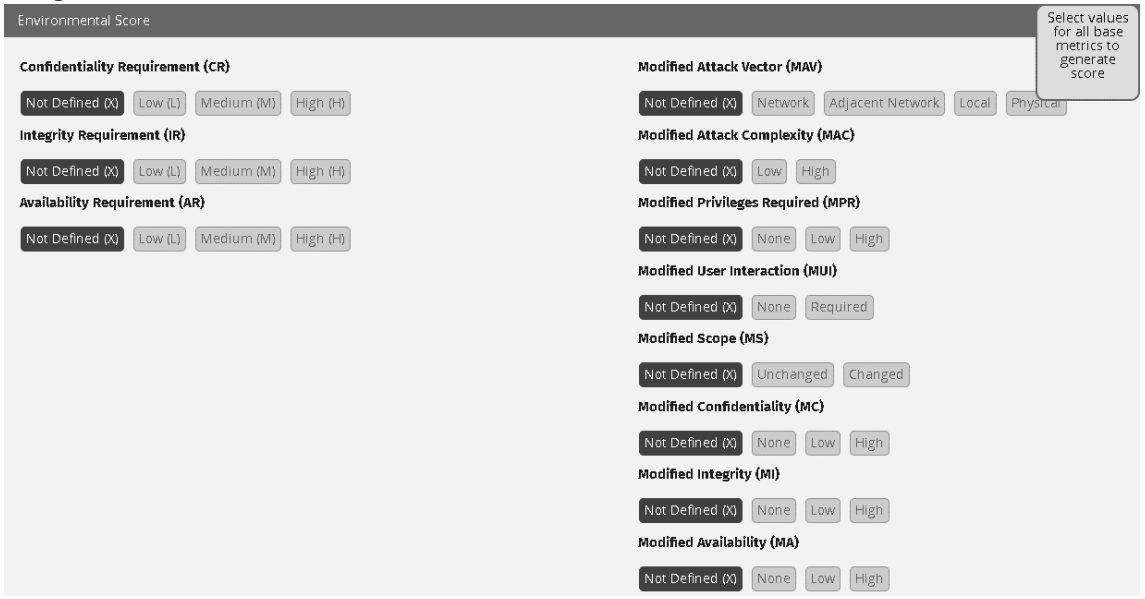
Reasonable(R): Detalhes significativos são publicados, mas os pesquisadores não tem total confiança na causa raiz ou não possui acesso ao código fonte para verificar.

Confirmed(C): Existem os relatórios detalhados e a reprodução funcional é possível.

4.3. Environmental Score

Por fim a métrica Ambiental que representa as características de uma vulnerabilidade que são relevantes e exclusivas para um determinado ambiente de usuário. Incluindo a presença de controles de segurança que podem mitigar as consequências de um ataque bem-sucedido e a importância relativa de um sistema vulnerável, ilustrado na imagem 6. Como esta métrica engloba características das outras duas citadas anteriormente, ela será utilizada unicamente neste trabalho para calcular o potêncial das vulnerabilidades e o comparativo das mesmas.

Imagem 6: Environmental Score



Fonte: FIRST, 2015. Common Vulnerability Scoring System. V.3.1

Confidentiality Requirement (CR), Integrity Requirement (R), Availability Requirement (AR): Permitem a personalização da pontuação do CVSS dependendo da importância do ativo afetado, de acordo com o ponto de vista do usuário. O nível de exigência varia entre Não Definido(X), Baixo(L), Moderado(M) e Alto(H).

Modified Attack Vector(MAV), Modified Attack Complexity(MAC), Modified Privileges Required(MPR), Modified User Interaction(MUI), Modified Scope (MS), Modified confidentiality(MC), Modified Integrity(MI), Modified Availability(MA): Os valores são os mesmos da calculadora do *Base Score* mencionada anteriormente, medindo o impacto das modificações resultantes da vulnerabilidade explorada e também permite a personalização da pontuação.

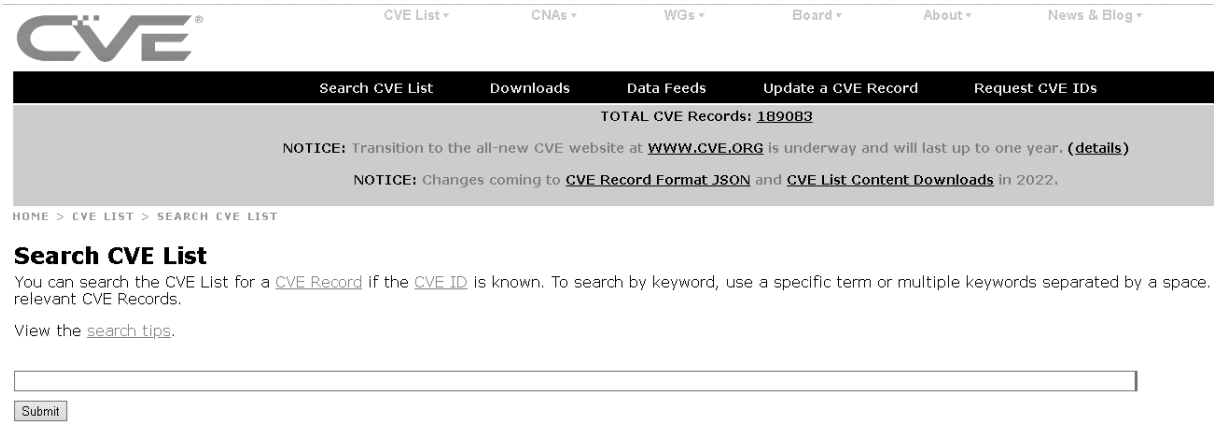
4.4. Vulnerabilidades CVE

O *Common Vulnerabilities and Exposures* (CVE) é um site público que possui um banco de dados onde são registradas as vulnerabilidades e exposições relacionadas à segurança da informação. Este sistema foi lançado oficialmente para o público em setembro de 1999, é financiado pelo Departamento de Segurança Interna dos Estados Unidos, operado pela *Mitre Corporation* e monitorado pela *National Cybersecurity* (FFRDC).

As vulnerabilidades publicadas e conhecidas possuem um identificador único que

a partir de 2015 padronizou-se a seguinte nomenclatura: prefixo CVE + ano + dígitos arbitrários, que geralmente seguem a ordem das vulnerabilidades publicadas anteriormente (MITRE, 2020). A página para pesquisar as vulnerabilidades conhecidas é exatamente como na imagem 7.

Imagem 7: Banco de Pesquisa de Vulnerabilidades CVE



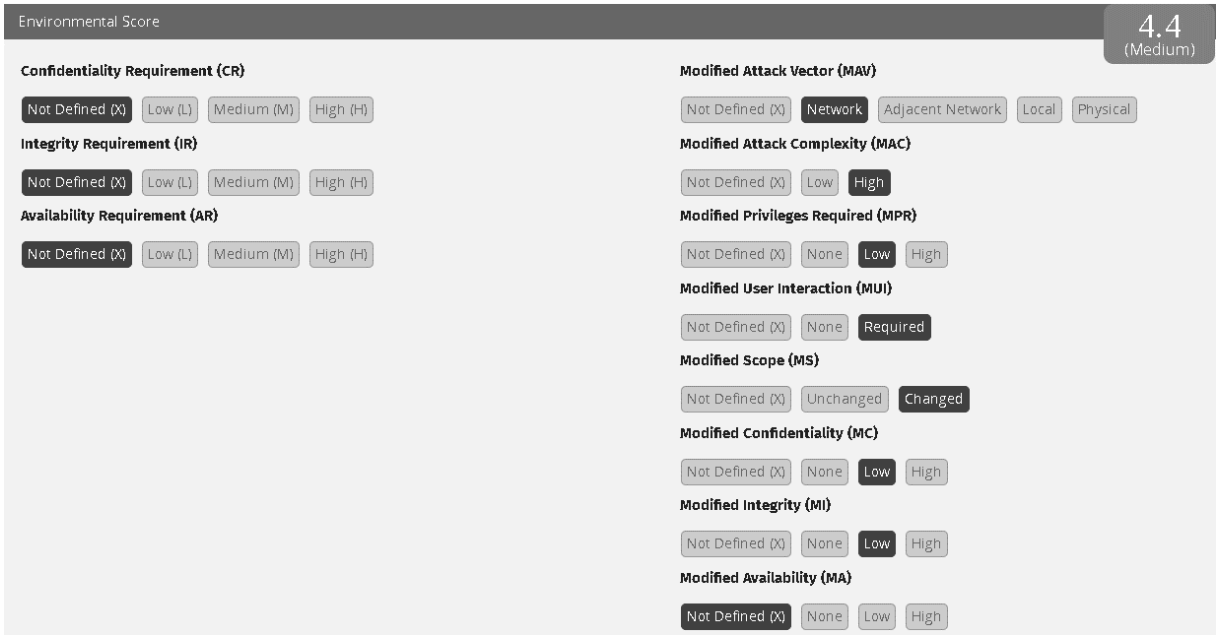
Fonte: MITRE, 2020. Search CVE List.

4.4.1. Vulnerabilidade Número 1: CVE-2022-36633 – Teleport

Teleport é uma ferramenta de *software* Linux que permite a transferência de arquivos via rede local, em sua versão 9.3.6 e posteriormente na 10.1.1 uma vulnerabilidade foi identificada que deixou a ferramenta exposta à injeção de comando, possibilitando execução remota de códigos, desta forma o invasor poderia criar um link de instalação do agente *Secure Shell* (SSH) malicioso através do endereço eletrônico da rede, codificando um escape *bash* (interpretador de comandos shell), substituindo o arquivo original pelo arquivo malicioso e enviando o link de download para a vítima. Portanto a vulnerabilidade não está dentro da ferramenta original em si, mas no código fonte que pode ser modificado, explorado e em seguida enviado para alguma vítima efetuar a instalação. Nesta vulnerabilidade a utilização da engenharia social é indispensável para a efetividade do ataque, pois se o download for feito da fonte oficial não ocorrerá o problema. A vulnerabilidade foi publicada no dia 24 de agosto de 2022 e já existem novos patches com versão atualizada para evitar essa vulnerabilidade (MITRE, 2022).

Abaixo será demonstrado o potencial de risco original da vulnerabilidade selecionando os campos afetados pela vulnerabilidade e gerando um valor de 0 a 10 no canto superior direito, conforme a imagem 8.

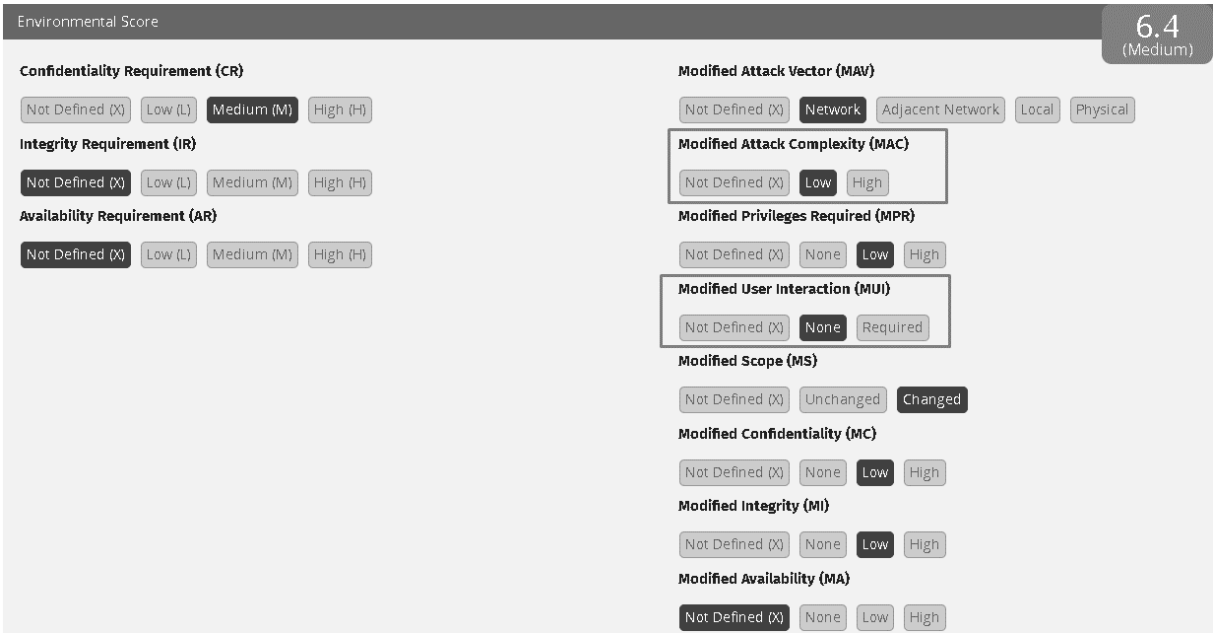
Imagem 8: Potencial de Risco Original da Vulnerabilidade 1



Fonte: FIRST, 2015. Common Vulnerability Scoring System. V.3.1

Em seguida na Imagem 9 há a simulação do potencial de risco da vulnerabilidade personalizado, alterando os campos que incluem a engenharia social para que a exploração da vulnerabilidade seja efetiva, demonstrando um novo valor de risco potencial em um cenário que não fosse necessário vitimas de engenharia social.

Imagem 9: Potencial de Risco Personalizado da Vulnerabilidade 1



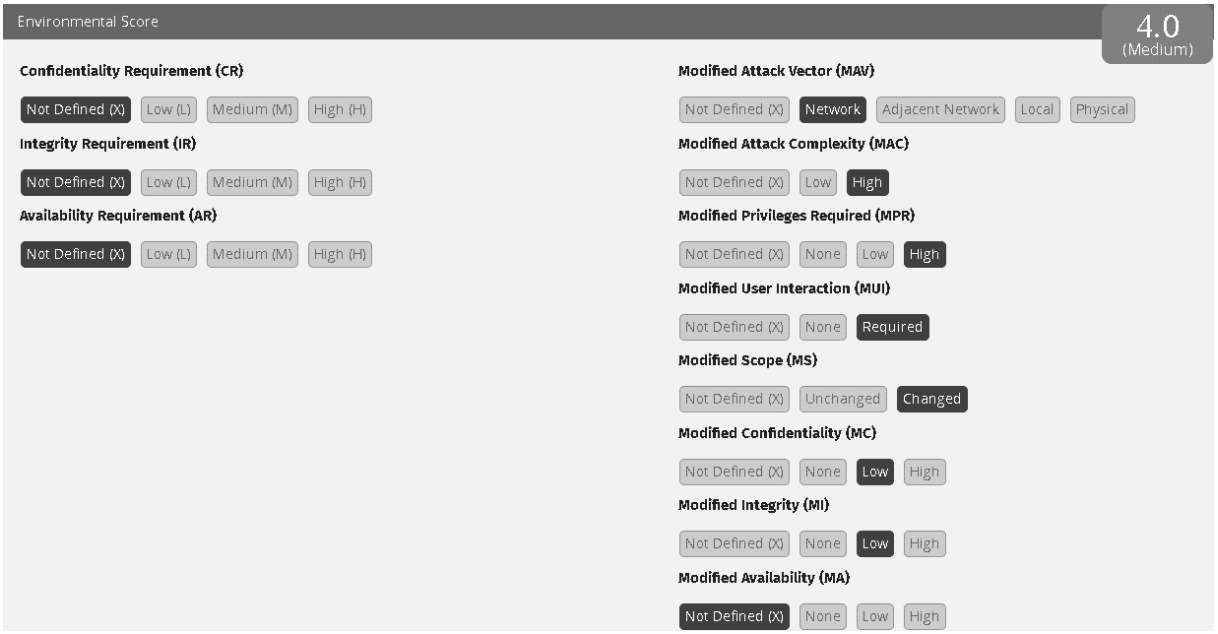
Fonte: FIRST, 2015. Common Vulnerability Scoring System. V.3.1

4.4.2. Vulnerabilidade Número 2: CVE-2022-24918 – Javascript XSS

JavaScript é uma linguagem de programação estruturada muito utilizada em aplicações web juntamente com HTML e CSS que são outras linguagens amplamente utilizadas. Essa Vulnerabilidade permitia que um usuário autenticado criasse um link com código XSS *Javascript* refletido (*Cross-site Scripting*, ataque de injeção de código malicioso em aplicações *web*, por ser refletido não está alojado em um servidor de destino, portanto deve ser entregue diretamente a vítima). O link redireciona para a página actionconf.php do programa Zabbix *Frontend* onde todo o conteúdo pode ser modificado, personalizando e induzindo a vítima a clicar nos links maliciosos e preencher algum formulário, que pode conceder acesso remoto a máquina da vítima. Essa vulnerabilidade foi publicada no dia 08 de março de 2022 e já existem *patches* de correção Java para conter a mesma (MITRE, 2022).

Abaixo será demonstrado o potencial de risco original da vulnerabilidade selecionando os campos afetados pela vulnerabilidade e gerando um valor de 0 a 10 no canto superior direito, conforme a imagem 10.

Imagem 10: Potencial de Risco Original da Vulnerabilidade 2

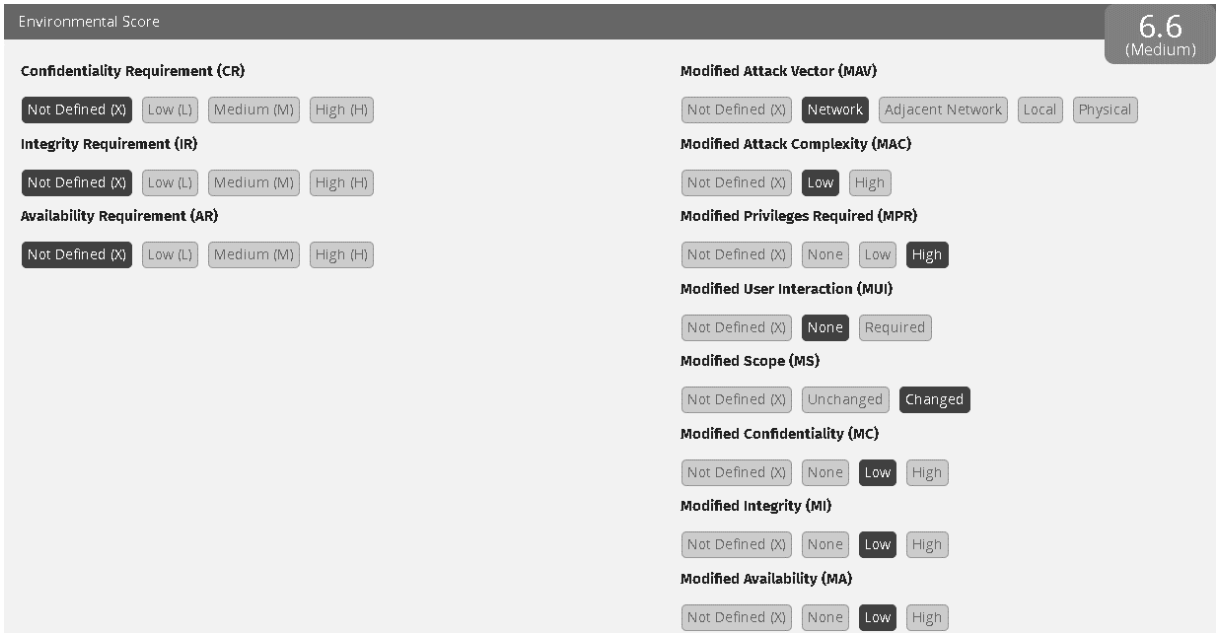


Fonte: FIRST, 2015. Common Vulnerability Scoring System. V.3.1

Abaixo na Imagem 11 é possível verificar a simulação do potencial de risco da vulnerabilidade personalizado, alterando os campos que incluem a engenharia social para que a exploração da vulnerabilidade seja efetiva, demonstrando um novo valor de risco potencial em um cenário que não fosse necessário vitimas de engenharia

social.

Imagem 11: Potencial de Risco Personalizado da Vulnerabilidade 2



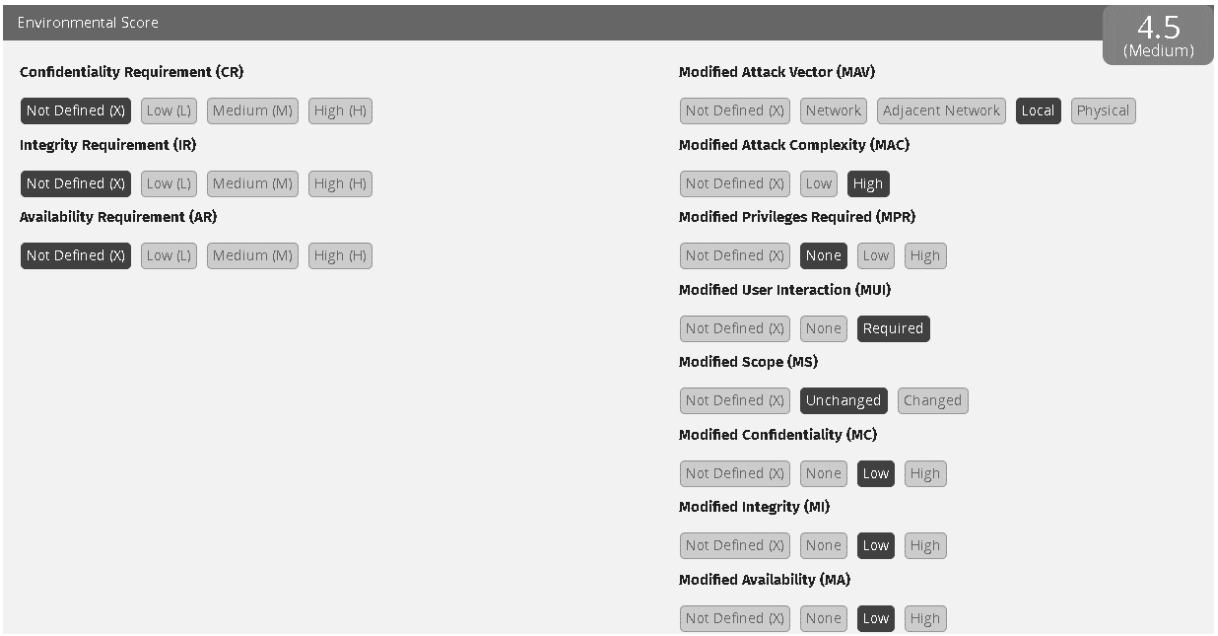
Fonte: FIRST, 2015. Common Vulnerability Scoring System. V.3.1

4.4.3. Vulnerabilidade Número 3: CVE-2015-1098 – Apple iWork

A Vulnerabilidade do Apple iWork (aplicativos corporativos da Apple que incluem processadores e editoresde textos) ocorreram nos sistemas iOS versão 8.3 e OSX versão 10.10.3 permitindo que invasores remotos executem códigos arbitrário ou negação de serviço (por meio de corrupção de memória) através de um arquivo iWork criado pelo atacante. O atacante cria e modifica o arquivo iWork com código arbitrário e envia para a vítima ou salva em dispositivos de armazenamento como pen-drive, cd-dvd, hd externo, entre outros. Ao abrir o arquivo inicia-se o código alterado que causa uma corrupção de memória que acaba deixando o dispositivo ou máquina afetada sem funcionamento. A vulnerabilidade foi publicada no dia 08 de abril de 2015 e é necessário realizar a atualização para uma nova versão do sistema para resolver o problema (MITRE, 2015).

Abaixo será demonstrado o potencial de risco original da vulnerabilidade selecionando os campos afetados pela vulnerabilidade e gerando um valor de 0 a 10 no canto superior direito, conforme a imagem 12.

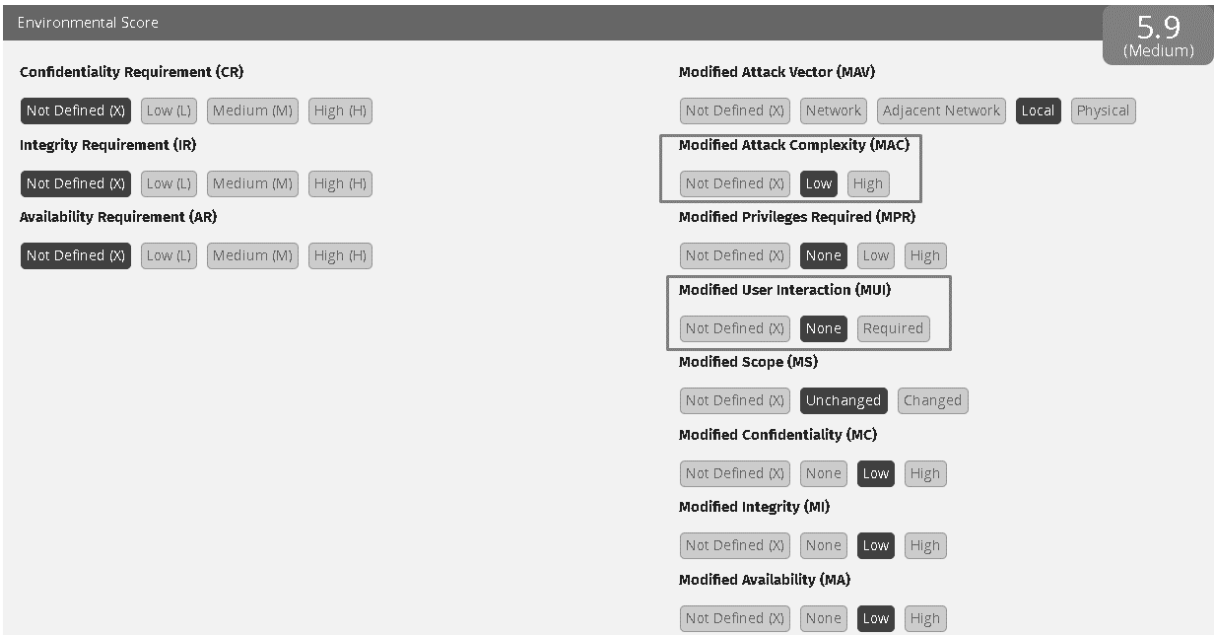
Imagem 12: Potencial de Risco Original da Vulnerabilidade 3



Fonte: FIRST, 2015. Common Vulnerability Scoring System. V.3.1

Em seguida na Imagem 13 contem a simulação do potencial de risco da vulnerabilidade personalizado, alterando os campos que incluem a engenharia social para que a exploração da vulnerabilidade seja efetiva, demonstrando um novo valor de risco potencial em um cenário que não fosse necessário vitimas de engenharia social.

Imagem 13: Potencial de Risco Personalizado da Vulnerabilidade 3



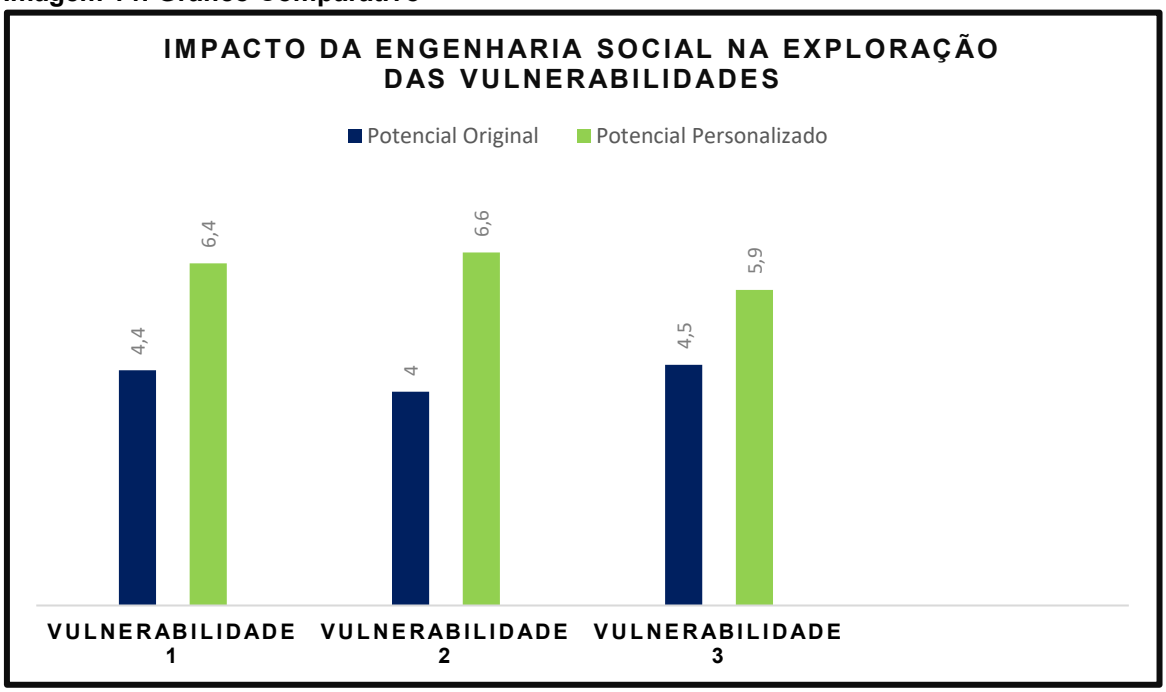
Fonte: FIRST, 2015. Common Vulnerability Scoring System. V.3.1

4.4.4. Resultados e Gráfico Comparativo

Ao personalizar as vulnerabilidades alterando os campos que incluem engenharia social é notável que há um aumento significativo do potencial de risco da vulnerabilidade explorada, na Vulnerabilidade 1 o *Score* aumentou de 4.4 para 6.4, um aumento de 2.0 pontos e se manteve na escala “medium”. Na Vulnerabilidade 2 o *Score* aumentou de 4.0 para 6.6, um aumento de 2.6 pontos e permaneceu na escala “low”, ficando muito próxima da escala “medium”. Já na Vulnerabilidade 3 o *Score* aumentou de 4.5 para 5.9, um aumento de 1.4 pontos e também se manteve na escala “medium”.

Para analisar e compreender de forma mais simplificada os resultados do Potencial Original e do Potencial Personalizado (retirando o filtro da engenharia social do contexto) serão apresentados, de forma sintetizada, no gráfico da imagem 14 abaixo.

Imagem 14: Gráfico Comparativo



Fonte: Imagem Própria do Autor

4.5. Política de Segurança e a Mitigação de Vulnerabilidades

Os riscos de segurança e engenharia social nas organizações, muitas vezes formam um conjunto para o sucesso de uma invasão, eles são constantes e se adaptam diariamente, com treinamentos e conscientização sobre termos tecnológicos esses riscos tendem a diminuir, mas para que seja realmente controlado, garantindo

que a organização está preparada para eventuais incidentes, é necessário que haja uma política de segurança bem aplicada e implementada na instituição.

Uma política de segurança, de forma geral, é um conjunto de regras, normas e padrões que tem como principal objetivo proporcionar o controle e gerenciamento da segurança nas organizações, para que essa política seja bem estruturada e funcional, recomenda-se a utilização da norma ABNT ISO 27002 que possibilita um pacote completo de informações e diretrizes para estabelecer uma política de segurança efetiva, além de garantir um passo a mais para a qualificação de certificações profissionais.

A ISO 27002 é um padrão internacional de segurança que inclui as melhores práticas para iniciar, implementar, manter ou melhorar o gerenciamento de processos, pessoas e tecnologias. Baseando-se nesse modelo explicativo de instruções sobre as melhores práticas, é possível criar e monitorar um gerenciamento que inclua as 14 seções desse padrão conforme abaixo (ABNT ISO 27002, 2005):

Seção 1: Política de Segurança da Informação: Possibilita orientação e direção de acordo com os requisitos do negócio e regulamentos relevantes.

Seção 2: Organização da Segurança da Informação: Estabelecimento de uma estrutura de gerenciamento para controle e implementação da segurança da informação na organização.

Seção 3: Segurança em Recursos Humanos: Assegura que os colaboradores e partes externas estejam cientes de suas responsabilidades.

Seção 4: Gestão de Ativos: Identificação e definição da proteção dos ativos.

Seção 5: Controle de Acesso: Limita os acessos às pessoas explicitamente autorizadas.

Seção 6: Criptografia: Assegura o uso e efetividade da criptografia para criar uma proteção sobre as informações da organização.

Seção 7: Segurança Física e do Ambiente: Previne os acessos físicos não autorizados e interferências nos processos da organização.

Seção 8: Segurança nas Operações: Garante a operação segura e correta dos processamentos da informação.

Seção 9: Segurança nas Comunicações: Proteção das informações em rede e processamento das informações.

Seção 10: Aquisição, Desenvolvimento e Manutenção de Sistemas:

Garante que a segurança da informação esteja presente em todo o ciclo de vida dos sistemas da informação, requisitos e serviços internos e externos.

Seção 11: Relacionamento na Cadeia de Suprimento: Possibilita a proteção dos ativos e acessos externos.

Seção 12: Gestão de incidentes de segurança da informação: Assegura o gerenciamento de incidentes de segurança da informação e notificação sobre fragilidades.

Seção 13: Aspectos da Segurança da Informação na Gestão da Continuidade do Negócio: Refere-se a continuidade da segurança da informação nos sistemas de gestão da organização.

Seção 14: Conformidade: Evita eventuais violações de quaisquer obrigações legais relacionadas aos requisitos de segurança.

Utilizando essas 14 seções como base e, de certa forma um passo-a-passo, para elaboração de uma política de segurança que seja gerenciada e monitorada por pessoas qualificadas, o potêncial de risco de vulnerabilidades e brechas de segurança será drásticamente reduzido impactando positivamente no fluxo diário das operações da organização, proporcionando uma segurança nas atividades e processamentos, além de estar dentro do padrão internacional para a certificação de boas práticas de segurança da norma ISO 27002, aumentando considerávelmente o nível competitivo e seriedade da organização.

5. CONCLUSÃO

A engenharia social permanece sendo um fator de alto potencial de risco para as organizações, ao analisar as três vulnerabiliades exploradas neste trabalho, quando alterado os requisitos de engenharia social e mudando o cenário da vulnerabilidade original (que possui os filtros da engenharia social no contexto) para um cenário onde não seja necessário esse filtro ou que ele poderia ser, de certa forma burlado, pode-se concluir então que houve um aumento médio de 2.0 pontos no potencial de risco.

Desta forma é imprescindível que haja uma política de segurança que inclua a conscientização e treinamento sobre a engenharia social nas organizações para todos os colaboradores, ainda que forçoso, pois muitos ataques surgem ou utilizam como

base essas tentativas de persuasão usando a engenharia social para conseguir informações ou acessos, caso a vítima tenha conhecimento desse assunto, sobre as técnicas e os mecanismos que podem ser utilizados o sucesso do ataque ou exploração da vulnerabilidade é extremamente reduzido.

Assim é possível poupar recursos financeiros da organização além de contribuir e assegurar que a Integridade, Confidencialidade e Disponibilidade, os três pilares da Segurança da Informação, sejam preservados com mais controle, algo que é muito valioso para uma organização que pretende se manter competitiva no mercado.

REFERÊNCIAS

ALVES, Gustavo Alberto. **Segurança da Informação:** Uma visão inovadora da gestão. Rio de Janeiro: Ciência Moderna, 2006.

AMARAL, Luiz Míra. **Política de Segurança da Informação**, 2015. Disponível em: <https://docplayer.com.br/129087659-Politica-de-seguranca-da-informacao.html> Acesso em: 08 de out. 2022, às 11:07hrs.

ANTÔNIO Marcelo; MARCOS Antônio. **A Arte de Hackear Pessoas**. Rio de Janeiro: Brasport. 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. **NBR/ISO/IEC 27002:** Tecnologia da informação - Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2007.

DHILLON, G. (2004). **Business Process Management Journal:** Realizing benefits on an information security program, Vol.10, No.3, p.260. Disponível em:<https://www.emerald.com/insight/content/doi/10.1108/bpmj.2004.15710caa.002/full/html> Acesso em: 14 de maio de 2022, às 18:47.

FERREIRA, Fernando N. F. **Segurança da Informação**. Rio de Janeiro: Ciência Moderna. 2003.

FERREIRA, Aurélio Buarque de Holanda. **Novo Aurélio Século XXI:** O dicionário da língua portuguesa, 3. ed. Petrópolis: Nova Fronteira, 1999.

FIRST, 2015. **Common Vulnerability Scoring System Calculator**. V.3.1. Disponível em: <www.first.org/cvss/calculator/3.1> Acesso em: 01 de Outubro de 2022 às 09:20hrs.

FIRST, 2015. **Commom Vulnerability Scoring System Specification Document**. Disponível em: < https://www.first.org/cvss/v3.1/specification-document> Acesso em: 19 de Novembro de 2022 às 17:43hrs.

HADNAGY, Christopher. **Social Engineering:** The Art of Human Hacking. Indianapolis: Wiley Publishing Inc. 2011.

KASPERSKY, **Engenharia Social:** Definição, 2022. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/what-is-social-engineering> Acesso em: 07 de maio de 2022, às 13:30hrs.

LAWLEY, James; TOMPKINS, Penny. **Rapport: The Magic Ingredient**. Personal Success. Londres, 1994.

LUIZA, Magazine. **GPS Tracker G200**, 2022. Disponível em: <https://www.magazineluiza.com.br/gps-tracker-g200/p/jh219b5g08/es/otes/?&seller_id=luisaranhas&utm_source=google&utm_medi

um=pla&utm_campaign=&partner_id=69080&gclid=Cj0KCQiA1NebBhDDARIsAANiDD3uJiyeSdFJUJbh81qnIl6l9fzd29diviEn-o5CI7iD-tZQVIUCfMwaAhycEALw_wcB&gclsrc=aw.ds> Acesso em: 18 de Junho de 2022 às 11:24hrs.

MALTEGO, Technologies. **Maltego for Windows**, 2022. Disponível em: <https://www.maltego.com/downloads/> Acesso em 18 de Junho de 2022 às 11:51

MITRE, 2020. **Search CVE List**. Disponível em: <https://cve.mitre.org/cve/search_cve_list.html> Acesso em: 19 de Novembro de 2022 às 18:07hrs.

NIST; Barker, Willian C. **Information Security**, 2003. Disponível em: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-59.pdf> Acesso em: 14 de maio de 2022, às 18:10hrs.

NORTON, **What is Social Engineering? A definition + techniques to watch for**, 2021. Disponível em: <https://us.norton.com/blog/emerging-threats/what-is-social-engineering> Acesso em: 11 de Junho de 2022 às 13:23hrs.

SÊMOLA, Marcos. **Gestão da Segurança da Informação:** Uma visão executiva. Rio de Janeiro: Campus, 2003.

STALLINGS, William; BROWN, Lawrie. **Segurança de Computadores:** Princípios e práticas. 2 ed. Rio de Janeiro: Elsevier, 2014.

STAVROULAKIS, Peter; STAMP, Mark. **Handbook of Information and Communication Security**, Berlin: Springer-Verlag. 2010.

TANASE, Matthew. **IP Spoofing Defense: An Introduction**, 2003. Disponível em: <https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=9d18fc06-b229-4c4a-8ca5-7386d0870c01&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments> Acesso em: 11 de Junho de 2022 às 13:57hrs.