Segurança na Apreensão e Armazenamento de Criptomoedas

João Maurício Barros Ascensão

Dissertação para obtenção de Grau de Mestre em

Segurança de Informação e Direito no Ciberespaço

Orientador: Prof. Miguel Nuno Dias Alves Pupo Correia

Júri

Presidente: Prof. Carlos Manuel Costa Lourenço Caleiro

Orientador: Prof. Miguel Nuno Dias Alves Pupo Correia

Vogal: Prof. Nuno Miguel Carvalho dos Santos

Dezembro 2020

Agradecimentos

Em primeiro lugar gostaria de dar os maiores e mais sinceros agradecimentos ao meu orientador, Professor Miguel Pupo Correia, por me ter sugerido este tema, por ter estado sempre disponível para me esclarecer dúvidas e pela incansável ajuda durante todo o processo de desenvolvimento deste trabalho. Sem a sua ajuda nada disto seria possível. Um especial Obrigado.

Em segundo lugar gostaria de agradecer ao Inspetor Ricardo Vieira da PJ de Lisboa pela disponibilidade na realização da reunião que serviu de linha condutora para este trabalho.

Gostaria de agradecer também à minha família, em especial à minha mãe, por todo o apoio e motivação dado ao longo do ano. Quero também agradecer aos meus amigos e conhecidos pela companhia e motivação durante as longas noitadas de estudo e trabalho nesta dissertação.

Por fim, mas não menos importante, gostaria de agradecer ao Instituto Superior Técnico que em parceria com a Escola Naval e com a Universidade de Direito de Lisboa me proporcionaram dois anos de muita aprendizagem e crescimento a nível, académico e pessoal, no Mestrado de Segurança de Informação e Direito no Ciberespaço.

Muito Obrigado!

Resumo

Com o aumento da popularidade das criptomoedas e o consequente crescimento do número de crimes e ataques cibernéticos, tornou-se importante a utilização de mecanismos que protejam e mantenham as criptomoedas armazenadas em segurança - as *wallets*.

Após uma investigação criminal que envolva criptomoedas, a PJ apreende essas criptomoedas e armazena-as em *wallets*. Neste trabalho foi realizado um método de análise de ameaças a cinco possíveis tipos de *wallets* que a PJ pode implementar: *Paper Wallet, Mobile Wallet, Web Wallet, Desktop Wallet* e *Hardware Wallet*. Com o objetivo de identificar aquela que está sujeita a um menor número de ameaças e, consequentemente, a um menor número de ataques internos e externos. Após a análise, o tipo de *wallet* que apresentou maior viabilidade em termos de segurança foi a *Hardware Wallet*, pois, para além de estar sujeita a um menor número de ameaças e ataques, apresenta boas características para armazenar grandes quantidades de criptomoedas durante longos períodos de tempo.

O facto de a chave privada estar sob o controlo de uma pessoa pode levar à perda total do valor de criptomoedas em caso de destruição da chave, falecimento da pessoa ou inexistência de *backups* dos dados.

Daí surgiu a ideia de criar um modelo hierárquico baseado em conceitos de *Secret Sharing*: dividir a chave que dá acesso às criptomoedas por um número de *shares* e por um número de participantes (conceito de *Secret Sharing*), de modo a não deixar esta chave sob o controlo de apenas uma pessoa. Isto significa que se torna mais difícil alguém com atividades ilícitas em mente aceder às criptomoedas. Contribuindo assim para uma melhoria significativa dos níveis de segurança das criptomoedas apreendidas pela PJ.

Palavras-chave: Análise de Ameaças, Árvores de Ataque, Criptomoedas, Secret Sharing, Wallets

Abstract

With the increase in the popularity of cryptocurrencies and the consequent increase in the number of crimes and cyber-attacks, it became important to use mechanisms that protect and keep cryptocurrencies safely stored in wallets.

After a criminal investigation involving cryptocurrencies, the Judiciary Police seizes these cryptocurrencies and stores them in wallets. In this work, a threat analysis method was applied to five possible types of wallets that the Judiciary Police can implement: Paper Wallet, Mobile Wallet, Web Wallet, Desktop Wallet, and Hardware Wallet. To identify the one that is subject to the least number of threats and consequently to the least number of internal and external attacks. After the analysis, the type of wallet that showed the best reliability in terms of security was the Hardware Wallet, because, in addition to being subject to fewer threats and attacks, it has good characteristics for storing large amounts of cryptocurrencies for long periods of time.

The fact that the private key is under the control of a person can lead to the total loss of the value of cryptocurrencies, in case of destruction of the key, death of the person, or no backups of the data.

Hence, the idea to create a hierarchical model based on Secret Sharing concepts: divide the key that gives access to cryptocurrencies by several shares and by many participants (Secret Sharing concept) so as not to leave this key under the control of one person only. This means that it becomes more difficult for someone with illegal activities in mind to access cryptocurrencies. Thus contributing to a significant improvement in the security levels of the cryptocurrencies seized by the Judiciary Police.

Keywords: Threat Analysis, Attack Trees, Cryptocurrencies, Secret Sharing, Wallets

Índice

Lista de Tabelas

Lista de Figuras

Capítulo 1

1. Introdução

As criptomoedas têm-se tornado cada vez mais populares ao longo dos anos, por todo o mundo. A *Bitcoin*, criada em 2008 por *Satoshi Nakamoto* [1], é a criptomoeda mais conhecida. Trata-se de um sistema de pagamento que funciona com base em algoritmos de *software open source* que usam uma rede global *peer-to-peer* para a criação de novas moedas e registar e validar as transações. As transações neste sistema são feitas utilizando chaves criptográficas (chave privada e pública) e cada utilizador tem em sua posse as suas chaves privadas e um mecanismo para as guardar em segurança [3] [18].

As chaves privadas são essenciais para a realização de transações, pois são elas que permitem identificar o dono das *bitcoins*. Estas são usadas principalmente para assinar as transações de criptomoedas e consequentemente gastá-las tendo em conta a chave pública correspondente. Sendo estas chaves privadas o ativo mais importante a proteger por parte das pessoas que têm essas criptomoedas, é necessário a utilização de mecanismos que as armazenem em segurança. A esses mecanismos dá-se o nome de *Wallets* - usadas para transferir as criptomoedas e para armazenar as chaves privadas em segurança [3].

A *Bitcoin* veio trazer muitas vantagens para as pessoas e organizações que fazem qualquer tipo de pagamento *online*, como por exemplo: os utilizadores têm total controlo do seu dinheiro; não existe qualquer tipo de pagamento de taxas adicionais nas transações; não existe nenhuma entidade financeira responsável pelas transações e armazenamento do dinheiro (sistema descentralizado); as transações são irreversíveis e não é necessário o uso dos dados pessoais do utilizador, garantindo assim total anonimato. [1] [3].

Por outro lado, as características apresentadas em cima chamaram à atenção dos criminosos. O facto de a *Bitcoin* ser um sistema de pagamento descentralizado, ou seja, sem nenhuma entidade reguladora, e ser possível realizar transações em anonimato, fez com as forças de autoridade por todo o mundo ficassem preocupadas com a realização de transferências ilegais de produtos e serviços e com outros tipos de crimes *online*, como por exemplo a lavagem de dinheiro [11].

Em Portugal a entidade responsável pelas investigações criminais é a Polícia Judiciária. Em relação a crimes cibernéticos que envolvam criptomoedas, a PJ (acrónimo de

Polícia Judiciária) tem uma unidade própria para estes casos, a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) [10].

3.1. Problema

Na ocorrência de atividades ilícitas cibernéticas que envolvam criptomoedas a PJ é a entidade responsável pela investigação e respetiva apreensão de todo o equipamento tecnológico, nomeadamente as *wallets*, que são onde estão guardadas as criptomoedas envolvidas na atividade criminosa. Depois de concluída a investigação, é necessário armazenar em segurança o montante de criptomoedas apreendidas. E para armazenar estes montantes de criptomoedas a PJ tem algumas soluções: vários tipos de *wallets* (*Paper Wallet*, *Mobile Wallet*, *Web Wallet*, *Desktop Wallet*, *Hardware Wallets*, entre outras). Cada tipo de *wallet* apresenta as suas características, mas o foco deste trabalho dar-se-á na componente de segurança, ou seja, o objetivo é escolher um tipo de *wallet* que cumpra o maior número de requisitos de segurança para a PJ poder armazenar as criptomoedas apreendidas, com o mínimo risco de as perder ou serem roubadas, e de preferência que não tenha custos demasiado elevados. Posteriormente a ser escolhido o tipo *wallet* mais seguro para a PJ, vai ser apresentada uma proposta de melhoria da segurança no armazenamento de criptomoedas em *wallet,* usando *Secret Sharing*.

3.2. Metodologia

Os tipos de *wallets* em análise são: *Paper Wallet*, *Mobile Wallet*, *Web Wallet*, *Desktop Wallet* e *Hardware Wallet*.

Para a escolha do melhor e mais seguro tipo de *wallet* a implementar por parte da PJ recorrer-se-á a um processo de análise de ameaças, ou seja, vai ser escolhido um método para determinar os tipos e as quantidades de ameaças a que cada tipo de *wallet* está sujeito. Para isso será usada uma metodologia de identificação de ameaças, conhecida como *STRIDE* [25], onde será feita uma análise entre as ameaças dessa metodologia e as ameaças identificadas em cada tipo de *wallet*.

Identificadas essas ameaças de cada *wallet*, vão ser usadas as árvores de ataque como método para identificar que tipo e a quantos ataques está cada *wallet* sujeita. Após elaboradas essas árvores de ataque vão ser escolhidos parâmetros para avaliar e analisar cada ataque da árvore e perceber aqueles que têm maior probabilidade de acontecer a cada tipo de *wallet*.

Tendo em conta o tipo de *wallet*, a identificação das ameaças e a avaliação dos parâmetros das árvores de ataque, vai ser escolhida a mais segura como proposta de implementação para a PJ.

Feito isto, será apresentada uma proposta de melhoria da segurança no processo de armazenamento das criptomoedas, tendo como base a aplicação de conceitos de Secret *Sharing* de *Shamir* [34]. O objetivo é apresentar uma proposta de um modelo em que as chaves privadas que dão acesso às criptomoedas não fiquem sob o controlo de uma pessoa única, mas sim de um determinado número, definido pelos responsáveis das investigações. O foco, mais uma vez, prende-se na questão da segurança das chaves privadas que consequentemente dão acesso aos montantes de criptomoedas.

Apesar de na tese ser referida inúmeras vezes a PJ, o conteúdo da tese é unicamente da responsabilidade do seu autor. A tese não foi validada pela PJ nem constitui de forma alguma uma proposta dessa entidade.

3.3. Organização da Dissertação

A dissertação está organizada da seguinte forma:

- **Capítulo 2** discute algum trabalho relacionado com tema.
- **Capítulo 3** apresenta um método de análise de ameaças como solução para o problema.
- **Capítulo 4** apresenta um modelo como proposta de melhoria para a segurança da informação no processo de armazenamento das criptomoedas.
- **Capítulo 5** sumariza os resultados obtidos, apresenta uma solução para o problema e algum trabalho futuro.
- **Capítulo 6** apresenta as referências.

Capítulo 2

2. Trabalho Relacionado

Neste capítulo é providenciada uma visão geral das melhores contribuições relacionadas com o tópico da dissertação. Inicialmente, da secção 2.1. até à 2.3., será abordado o tema das criptomoedas, mais concretamente a *Bitcoin*, e todos os conceitos à volta desta moeda digital. Na secção 2.4. falar-se-á das *wallets*, que são o mecanismo de armazenamento e transferências das criptomoedas. Na secção 2.5. será abordado o tema de como são realizadas as apreensões e o devido armazenamento das criptomoedas por parte da PJ. Na secção 2.6. irá ser apresentado e explicado um método da análise de ameaças e implementação de árvores de ataque, que serão utilizados mais à frente no capítulo 3 como métodos determinantes para saber qual dos diferentes tipos de *wallets* é o que apresenta menos ameaças e consequentemente é mais segura para a PJ implementar. Finalmente, na secção 2.7., falar-se-á do *secret sharing* como proposta de melhoria da segurança da informação no processo de armazenamento das criptomoedas na sede da PJ.

2.1. Criptomoedas

Quando existe um pagamento de um serviço ou simplesmente uma transação entre indivíduos, existe uma série de acordos e transações feitas, sem as pessoas que vão realizar o pagamento ou a transação terem conhecimento, entre a instituição financeira e outros, permitindo assim que o dinheiro seja transferido [7].

As criptomoedas são dinheiro digital que fisicamente não existe, mas que podem ser convertidas para qualquer tipo de moeda física. Estas surgiram como meio para a realização de trocas entre pessoas ou organizações, com o grande objetivo de substituir as entidades terceiras responsáveis pela regulação e realização de todas as transações monetárias (ex. bancos, companhias como a *Paypal* e outras entidades financeiras) por meio de um *software* capaz de realizar este tipo de atividades, ao qual se deu o nome de *blockchain* e criptografia, como método para atingir altos níveis de confiabilidade e segurança nas transações [7] [8].

Na década de 90 existiram imensas tentativas para criar uma moeda digital, mas infelizmente sem sucesso. *DigiCash*, *Hashcash* ou *Bitgold* foram alguns desses casos. Uma das primeiras propostas foi a *DigiCash* [10], criada por *David Chaum* em 1989, em que este

propunha um sistema de transferência de dinheiro utilizando chaves criptográficas para a realização de transferências de dinheiro [9].

A *Bitcoin* é a moeda digital mais famosa, mas existem muitas outras: *Ethereum*, *Ripple* e *Litecoin* são exemplos de outras criptomoedas muito conhecidas [7].

2.2. *Bitcoin*

Esta moeda digital veio a propósito do grande desenvolvimento do comércio *online* e da exclusiva dependência em instituições financeiras para a realização de transações. As pessoas quando fazem uma transação, dependendo da distância entre elas, são alvo de custos adicionais (as taxas) e a transação pode demorar alguns dias até ser efetuada, deixando uma das partes à espera [1].

Existiram muitas tentativas para a criação de moedas digitais, mas apenas em 2008 uma entidade com o pseudónimo de *Satoshi Nakamoto* publicou um artigo "*Bitcoin: A Peer-to-Peer Electronic Cash System*" [1] em que propõe a existência de uma moeda digital descentralizada, a *Bitcoin*, usando uma rede *peer-to-peer* (rede de computadores que permite a partilha de serviços e dados sem existência de um servidor central). Esta nova moeda consiste num sistema de pagamento eletrónico baseado em princípios criptográficos que permite que duas entidades efetuem transações de dinheiro diretamente, sem recorrer a entidades terceiras.

Depois deste tipo de moeda digital ser emitida, não existe qualquer forma de gerar unidades adicionais, ou seja, apresentam um limite de unidades. No caso da *Bitcoin* o limite é de 21 milhões de unidades [7].

As transações da *Bitcoin* são computacionalmente irreversíveis, isto é, desde que uma das entidades envolvidas na transação efetue um pagamento não poderá voltar atrás e essa quantidade de *bitcoins* é automaticamente retirada da *wallet* [1].

Em relação ao processo de funcionamento destas transações, cada utilizador tem à sua disposição um *software* para realizar a transferência de *bitcoins* e a sua chave privada, que é usada para ter acesso ao endereço público do montante de *bitcoins* e para assiná-la respetivamente. Este *software* realiza uma operação matemática que combina a chave pública do destinatário das *bitcoins*, a chave privada do utilizador que pretende realizar a transferência e a respetiva quantidade de *bitcoins* que o mesmo vai transferir. Depois de efetuada esta operação, o resultado é enviado através da rede distribuída da *Bitcoin* de modo a que a transação seja verificada/validada. Em suma, a combinação da chave pública do destinatário e a chave privada do utilizador que pretende enviar as *bitcoins* são o que fazem uma transferência ser possível [1] [8].

A *Bitcoin* foi o primeiro tipo de moeda digital conhecida em formato *open source* e com uma ligação *Peer-to-Peer*. Esta moeda não tem nenhum servidor centralizado para a sua emissão, armazenamento e respetivas transações e usa uma rede pública distribuída, suportada por uma base de dados, a *Blockchain*, que requer uma assinatura eletrónica e é suportada pelo protocolo *Proof-of-Work*, que fornece a segurança e a legitimidade das transações monetárias [1].

A *Bitcoin* é uma das moedas mais famosas e bem-sucedidas no mundo do comércio na *Internet* e das criptomoedas, porque possuí algumas características exclusivas e muito vantajosas, tais como [1] [12]:

- é uma moeda **descentralizada**, um dos objetivos principais de *Satoshi Nakamoto* quando criou a *Bitcoin* era que a rede fosse independente de qualquer autoridade financeira ou estrutura organizacional. Esta moeda foi desenhada para todas as pessoas, negócios e máquinas envolvidas na mineração e verificação das transações.
- o **anonimato e a transparência**, nos dias de hoje as entidades financeiras (ex. bancos) conseguem ver *online* tudo sobre os seus clientes como por exemplo: o histórico do crédito, todos os dados pessoais, hábitos de consumo, entre outros. Como a *Bitcoin* é completamente diferente, a *wallet* do utilizador não precisa de estar associada à informação pessoal do mesmo. Este anonimato permite que as finanças dos utilizadores não sejam governadas e monitorizadas por nenhuma entidade. O anonimato da *Bitcoin* é um pouco relativo, pois todas as transações efetuadas são registadas e armazenadas publicamente na *blockchain*. Se o endereço da *wallet* for usado publicamente é possível saber a quantidade de *bitcoins* existentes nessa *wallet*, estudando simplesmente os blocos da *blockchain*. Mas é muito difícil associar esse endereço da *Bitcoin* a uma pessoa. Depois existem pessoas que gostam de fazer transações fora do radar e para isso é necessário tomar algumas medidas, como por exemplo, utilizar uma *wallet* que priorize a segurança e seguir regras mais simples, como a utilização de diversos endereços e não transferir grandes quantidades de dinheiro para uma *wallet*.
- **não repudiável**, a partir do momento em que um utilizador faz a transferência de *bitcoins* para um destinatário é impossível reverter esta operação, a não ser que o destinatário envie de volta a quantidade de *bitcoins* transferida. Esta medida assegura a receção do pagamento evitando qualquer tipo de enganos nas transações.
- **velocidade**, a rede *Bitcoin* processa pagamentos ou transferências a uma velocidade muito rápida, podendo-se dizer mesmo que quase instantânea, apenas demora alguns minutos se o destinatário se encontrar na outra ponta do globo. Por exemplo, se este mesmo processo fosse realizado por um banco poderia demorar alguns dias e provavelmente iriam ser cobradas taxas adicionais [1] [12].

Existem ainda algumas questões que a *Bitcoin* tem que melhorar para começar a ser usada por mais pessoas. Uma delas é o facto de que a sua legislação não é igual de país para país. Em alguns países não existe qualquer tipo de legislação para esta moeda e em alguns o seu uso é até mesmo proibido. Outras questões baseiam-se no facto de a maioria das pessoas não perceber como funcionam este tipo de moedas e como é que se consegue manter o anonimato e a segurança na realização de uma transação [11] [12].

Uma das coisas que levanta mais preocupações sobre a *Bitcoin* e as outras criptomoedas existentes é o facto de serem descentralizadas, ou seja, não existe nenhuma entidade reguladora, o que promove o comércio e as transferências ilegais de produtos e serviços por todo o mundo. Associando ao facto de as transações serem anonimizadas, torna-se muito difícil de controlar os crimes cibernéticos [11] [12].

2.3. *Blockchain*

Um dos conceitos revolucionários que veio adjacente com a *Bitcoin* [1] foi o da *Blockchain*. A *Blockchain* é um sistema descentralizado que regista todas as transações de bitcoins efetuadas em blocos, usando diversos computadores que estão interligados por uma rede *Peer-to-Peer*. Por outras palavras, a *blockchain* é uma enorme base de dados de registos de transações [4] [7].

As mudanças na *blockchain* são feitas adicionando a nova informação no fim desta. Cada nova adição de informação ou bloco contém um conjunto de transações [7].

A *Blockchain* veio permitir que os registos da sua estrutura de dados pudessem ser atualizados com o mínimo de risco de *hacking* ou adulteração de dados. Este foi um dos objetivos de *Nakamoto* [1], não deixar ninguém alterar os registos da *blockchain* para poder gastar o dinheiro duas vezes, isto é, roubar as *bitcoins* [4] [5] [7].

A solução que *Nakamoto* [1] viu para este problema de gastar as moedas mais do que uma vez foi tornar a adição de novas transações de *bitcoins* na *blockchain* numa “competição”, à qual deu o nome de *Mining*. O processo de *mining* foi criado para manter a segurança da *blockchain* e de todas as transações de *bitcoins* [4].

Este processo funciona da seguinte forma: são feitas cópias das transações e estas são transmitidas a cada instante via *broadcast,* para todos os computadores da rede para verificação. Posteriormente os *miners* (responsáveis pelo processo de *mining*) tentam encontrar o mais rápido possível o número mágico, *hash* – sequência aleatória de números e de letras que, encriptado junto com as transações e com o novo bloco da *blockchain*, cria um *hash* que começa por um determinado número de zeros. Este *hash* é muito difícil e leva algum tempo a encontrar, mas depois de ser encontrado pode ser verificado pelos restantes *miners*. O primeiro *miner* a resolver este problema e a chegar ao *hash* recebe um prémio em *bitcoins*

e tem o privilégio de adicionar um novo bloco (registo de uma nova transação) na *blockchain* [4] [5].

O *miner* pode ser um indivíduo ou um grupo de indivíduos que tem como tarefas a execução do *software* da *Bitcoin* na rede, detetar os pedidos de transações dos utilizadores, agregar esses pedidos, validá-los e adicioná-los nas *blockchain* como novos blocos. Estes competem entre si para colocar num bloco da *blockchain* a última transação efetuada. Esta competição mantém a *blockchain* segura e sem ser necessário a presença de uma entidade externa para realizar e regular o processo, pois, como já foi referido, é muito difícil de resolver este problema a todo o instante e é necessário muito poder de computação, significando assim que ninguém consegue ganhar acesso aos *links* encriptados nem os alterar na *blockchain* [4] [5].

Uma caraterística muito importante na *blockchain* é que os registos seguem uma ordem cronológica, não permitindo assim que a mesma pessoa gaste o dinheiro duas vezes. Exemplo: imagine-se que um sujeito A gastou todas as suas *bitcoins*, quando tentar realizar uma transferência para um sujeito B, esta será rejeitada, pois está registado na *blockchain* que o sujeito já realizou uma transação com essas *bitcoins*, estando sem nenhuma atualmente. A segurança e confiabilidade dos registos da *blockchain* são assegurados através do uso do algoritmo de criptografia [4] [5].

Atualmente existem pessoas e organizações a tentar aplicar os conceitos da *blockchain* para outras áreas e processos para além da movimentação de dinheiro, nomeadamente, no desenvolvimento de aplicações governamentais, de gestão de cadeias de abastecimento, saúde, agricultura e outras aplicações que usufruem de bases de dados. Estas novas aplicabilidades da *blockchain* podem vir a substituir serviços como as redes sociais (ex.: *Facebook, Instagram*) e outras aplicações como é o caso da *Uber* [5] [6] [7].

2.4. *Wallets*

As criptomoedas ao contrário dos outros tipos de moedas tradicionais são moedas digitais. Assim sendo, é necessário ter outro tipo de cuidados com este tipo de moedas, principalmente no que toca à sua aquisição, ao seu armazenamento, às suas transações e aos riscos às quais estão suscetíveis. Como as criptomoedas não existem em qualquer tipo de formato físico, não podem ser armazenadas em espaço físicos. Ao contrário das moedas tradicionais que são armazenadas em espaços físicos (ex. bancos, cofres), o único elemento que é armazenado nas moedas digitais são as chaves privadas. Estas chaves são usadas para aceder ao endereço público e assinar as transações, por isso devem ser armazenadas em segurança [13].

Com o crescente aumento da popularidade das criptomoedas nos sectores financeiros e de negócios, começou a ser cada vez mais importante ter dispositivos ou mecanismos altamente seguros para guardar as chaves privadas [3].

Daí surgiram as *wallets* que são usadas para realizar transações de criptomoedas e também são responsáveis por armazenar as chaves privadas em segurança. A combinação entre a chave pública do destinatário e a chave privada do utilizador é o que faz uma transação de criptomoedas ser possível [13].

Como as chaves privadas são o elemento mais importante na transferência de criptomoedas, este elemento é muito propício a ataques por parte de criminosos, visto que quem estiver na posse dessa chave torna-se dono do montante de criptomoedas da transação [14].

Ao longo dos anos tem-se assistido a um crescimento do número de casos de roubo de criptomoedas por todo o mundo, como foi o caso da *DragonEx* [41] que sofreu um ataque cibernético em que lhe foram roubados mais de sete milhões de dólares e a *Cryptopia Limited* [42], uma empresa baseada em Nova Zelândia, que foi alvo de ataques de *hackers* e teve um prejuízo de mais de dezasseis milhões de dólares. Os números de roubos de criptomoedas têm subido, pois muitas pessoas e organizações têm um valor muito grande de fundos nas chamadas *hot wallets*. As *hot wallets* não são nada mais que um *software* instalado num computador ou *smartphone* com ligação direta à *Internet*. O facto de estas *wallets* serem mais práticas nas trocas de criptomoedas faz com que as pessoas as usem mais, mas devido à sua ligação à *Internet* por vezes torna-as um alvo fácil para os atacantes. Uma das sugestões para estas situações é o armazenamento de pequenos valores de criptomoedas neste tipo de *wallet* e guardar as maiores quantias nas chamadas *cold wallets*. As *cold wallets* são aquelas que não têm qualquer ligação à *Internet*, estando assim as chaves privadas muito mais seguras. Estas *wallets* normalmente são armazenadas em dispositivos de *hardware* ou em papel [3] [14].

Existem diversos tipos de *wallets* dentro das duas categorias apresentadas anteriormente, cada uma com as suas características e risco de armazenamento associado. O risco nestas *wallets* é a possibilidade das mesmas perderem a informação ou esta ser corrompida, informação essa que contém as chaves privadas. Em baixo serão descritos os cinco tipos de *wallets* que vão ser alvo de análise no capítulo 3.

2.4.1. Paper Wallet

A *Paper Wallet* é um documento em formato de papel, que contém um endereço público, onde podem ser recebidas criptomoedas, e uma chave privada que permite gastar e transferir as mesmas usando esse endereço. Normalmente, este tipo de *wallets* incluem *QR*-

Codes de forma a permitir um rápido *scan* e, posteriormente, adicionar a chave ao *software* da *wallet* para realização da transação [13].

As *Paper Wallets* são geradas utilizando serviços próprios, como é o caso da *BitAddress,* em que é possível que os utilizadores criem um endereço *Bitcoin* completamente aleatório com a sua própria chave privada. Posteriormente, estas chaves podem ser impressas e guardadas em segurança [3] [13].

Este tipo de *wallet* está dentro da categoria das *cold wallets*, que são excelentes para guardar grandes quantias de dinheiro a longo prazo, mas não tem muita praticabilidade como as *wallets* instaladas em computadores ou *smartphones* [3].

Como o próprio nome indica, neste tipo de *wallet* as chaves privadas são armazenadas em formato de papel, tornando ataques de *hackers*, *malwares*, tentativas de *phishing* ou qualquer outro tipo de ataque cibernético praticamente impossíveis. A única possibilidade de comprometer a segurança deste tipo de *wallet* é no ato do *scan* do *Qr-Code*.

O facto de as chaves privadas (informação privada e crítica) estarem impressas num documento em papel requer um conjunto de medidas extraordinárias, como por exemplo: colocar o documento dentro de um saco de plástico fechado, à prova de água e de desgaste ou armazená-lo num cofre seguro [13].

A *paper wallet* apresenta bons índices de segurança quanto ao número de ameaças ou vulnerabilidades a que está suscetível [3] [13].

2.4.2. Mobile Wallet

As *Mobile Wallets* funcionam como uma aplicação para um *smartphone* onde é possível a realização de uma gestão financeira do dinheiro do utilizador e de transferências de fundos. Pode-se dizer que a *mobile wallet* é o equivalente digital às carteiras físicas que as pessoas usam para guardar o dinheiro. Funciona como uma conta de um banco onde se pode armazenar qualquer montante monetário, só que na realização de transações não existe qualquer cobrança de taxas adicionais e não é necessário que o utilizador introduza os dados do seu cartão e *pin* sempre que realizar uma transação [13] [16].

Este tipo de *wallet* insere-se na categoria das *hot wallets*, ou seja, podem ser usadas a qualquer altura do dia e estão ligadas à *Internet* para ter uma maior velocidade durante o uso. As *hot wallets* são muito práticas para o dia-a-dia das pessoas, principalmente porque permitem efetuar transações (independentemente do valor) muito rápidas [3].

Embora a utilização da *mobile wallet* seja muito conveniente e prática, existe um senão, o facto de estar ligada à *Internet* torna-a menos segura contra os ataques do ciberespaço (ex. *malwares*, tentativas de *phishing*, entre outros), aumentando o risco de o utilizador poder ficar sem os montantes de criptomoedas armazenados. Outro senão é o caso

de alguém ganhar acesso ao *smartphone* onde está a *mobile wallet* e o utilizador poder perder o controlo dos fundos lá armazenados. [3] [13] [16].

2.4.3. Web Wallet

As *Web Wallets* guardam as chaves privadas em servidores de uma empresa ou organização, que estão sempre *online* e são controlados por terceiros. Qualquer funcionário com acesso à rede corporativa pode aceder à sua *web wallet* e consequentemente gerir os seus fundos desde que tenha um dispositivo ligado à *Internet* em sua posse [13].

Este tipo de *wallet* está dentro da categoria das *hot wallets*, pois pode-se ter acesso à *web wallet* a partir de um computador ou smartphone (dispositivo ligado à *Internet*), tornando as transações de criptomoedas simples e rápidas, mas aumentado os riscos de ataques de *malware*, *phishing* e outros tipos de ataque. Se os servidores da empresa ou organização não forem bem protegidos pode levar a que seja possível aceder às chaves privadas das *wallets* de todos os funcionários e consequentemente roubar as suas criptomoedas lá armazenadas [3] [13].

Mais uma vez, este tipo de *wallet* apresenta alguma falta de segurança, tanto no armazenamento de criptomoedas como nas suas transações, devido ao facto de os dispositivos que acedem à *web wallet* estarem ligados à *Internet* e de apresentarem um maior número de ameaças e vulnerabilidades no seu funcionamento [3] [13].

2.4.4. Desktop Wallet

As *Desktop Wallets* são instaladas num computador e as chaves privadas são armazenadas no disco rígido do mesmo [13].

A *Desktop Wallet* faz parte das *hot wallets*, pois são muito práticas de usar, mas são pouco seguras aos ataques do ciberespaço devido à sua ligação direta à *Internet* [3].

Este tipo de *wallet,* embora também esteja ligado à *Internet,* é considerado um pouco mais seguro do que a *Web* e *Mobile wallet*, pois os seus dados não dependem de terceiros e são mais difíceis de roubar. Sendo que se o computador for roubado, o utilizador pode perder todos os fundos de criptomoedas que lá estiverem armazenados [3] [13].

Tendo em conta todos os fatores apresentados, este tipo de *wallet* é uma boa solução para pessoas que fazem transações de pequenos valores de criptomoedas [3] [13].

2.4.5. Hardware Wallet

As *Hardware Wallets* são um tipo de *cold wallets* que guardam as chaves privadas num dispositivo de *hardware* seguro (encriptado) sem ligação à *Internet,* durante muito tempo e têm também a capacidade de assinar transações *offline*. Normalmente as *cold wallets* servem apenas para armazenar grandes valores de criptomoedas durante grandes períodos de tempo e não têm muita flexibilidade de uso, mas a *hardware wallet* conseguiu unir essas duas características e tornar-se na maneira mais segura de armazenar qualquer montante de criptomoedas, apresentando o melhor rácio de segurança/funcionalidade de entre todos os tipos de *wallets*. *Ledger Nano*, *Trezor* e *BitSafe* são bons exemplos de *hardware wallets* [3] [13] [15].

2.5. Apreensão das Criptomoedas por parte da PJ

Este trabalho tem como foco principal a melhoria da segurança do processo de apreensão e armazenamento de criptomoedas, derivado de atividades cibernéticas ilícitas por parte da PJ, principal órgão organizacional de combate ao cibercrime.

A unidade da PJ responsável pela apreensão de criptomoedas é a UNC3T [19] (Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica). Esta unidade operacional é especializada na prevenção, deteção, investigação e centralização de crimes que envolvam meios tecnológicos ou informáticos, como por exemplo: burla informática, espionagem, ciberterrorismo, entre outros.

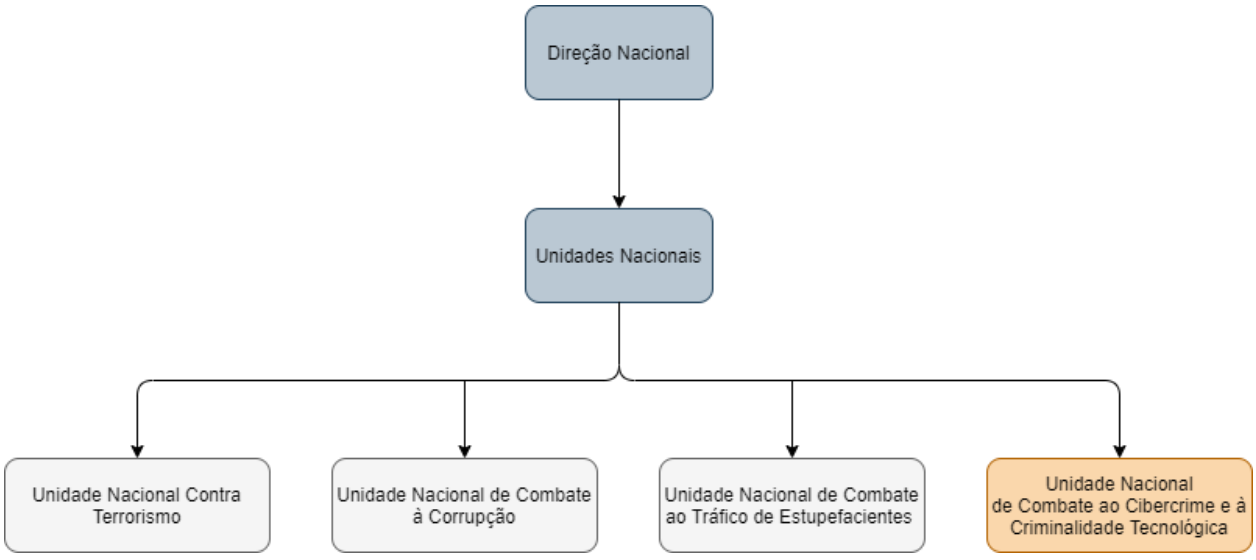

Figura 2.1: Organograma das Unidades Nacionais da PJ.

Esta unidade (UNC3T) [19] é responsável também por:

- Centralizar e tratar toda a informação criminal referente aos crimes, envolvendo tecnologias informáticas;
- Apresentar análises e estratégias dos crimes que aconteceram em território nacional;
- Recolher e tratar dados estatísticos;
- Apoiar e colaborar nas ações de prevenção, deteção e investigação das atividades desenvolvidas pelas entidades nacionais relacionadas com a segurança do ciberespaço;
- Desenvolver e manter o Plano Nacional da PJ para a Prevenção e o Combate ao Cibercrime com a cooperação do Centro Nacional de Cibersegurança;
- Comemorar protocolos de colaboração técnica e científica com outras entidades;
- Garantir o funcionamento de um grupo consultivo com finalidades de aconselhamento estratégico, formativo, técnico, jurídico e científico de todos os eventos relacionados com ciberespaço;
- Garantir ajuda na formação inicial e contínua dos funcionários nas áreas da segurança da informação e da cibersegurança.

Numa investigação judiciária relacionada com criptomoedas os inspetores da PJ, em conjunto com a sua equipa de investigação, reúnem provas suficientes para apreender o indivíduo ou os indivíduos responsáveis pela atividade cibernética ilícita. Dirigem-se à morada do criminoso, fazendo-se acompanhar por um mandato, fazem a apreensão de todo o material tecnológico que possa estar envolvido no crime, nomeadamente, computadores, *pen drives*, discos, *wallets*, entre outros. De realçar que para fazer a procura de *wallets* é necessário um *software* próprio para esse efeito. Depois de apreendido todo o material tecnológico, este é trazido para a sede da PJ para investigação. Após a investigação estar concluída é realizado o armazenamento do montante de criptomoedas envolvidas no ato malicioso nas respetivas *wallets,* segundo a regência da PJ.

2.6. Método de Análise de Ameaças

A segurança dos sistemas de *software* é um tema muito importante para o bom funcionamento das organizações. Cada vez mais as organizações são alvo de ataques de negação de serviço, ataques de violação da integridade dos dados e ataques com finalidades de divulgação de informação confidencial, como é o caso de dados de clientes, dados de carácter financeiro e até mesmo dados sensíveis sobre o processo de negócio. Cada vez mais

as organizações estão a reforçar os seus sistemas contra possíveis ataques, mas, mesmo assim, têm sofrido com estes atos de cibercrime. Isto acontece porque a tecnologia está a evoluir a um ritmo exponencial e todos os dias surgem novas formas de explorar vulnerabilidades nos sistemas das organizações [20].

Os atacantes apenas precisam de encontrar uma vulnerabilidade de segurança para ter acesso e comprometer os sistemas de uma organização. A solução mais indicada para estes ataques não voltarem a acontecer, ou o impacto do ataque ser menor, é a realização de uma análise de todos os requisitos que o sistema precisa para garantir a sua segurança, o bom mapeamento das potenciais ameaças e vulnerabilidades e o risco a associado a estas numa fase inicial do *design* do sistema. Este processo tem o nome de Análise de ameaças.

A análise de ameaças ou *threat modeling* [22] é uma atividade que visa a abstração de um sistema e a identificação das capacidades, motivos e objetivos dos atacantes. O seu principal objetivo é a identificação de ameaças e vulnerabilidades que possam de qualquer forma violar a segurança de uma organização, tendo como resultado final a reprodução e catalogação rigorosa das ameaças e vulnerabilidades do sistema, bem como o risco associado a cada uma delas [21].

A análise de ameaças [22] permite definir requisitos mais específicos de segurança para a fase de desenho de sistemas de *software*, ou seja, existem os requisitos mínimos que as normas de segurança apresentam, mas com a realização deste método consegue-se ir mais ao detalhe das necessidades dos sistemas da organização. Uma boa análise de ameaças permite que os responsáveis pela segurança dos sistemas de *software* consigam facilmente, e com mais precisão, estimar as capacidades dos atacantes e avaliar vulnerabilidades do sistema. É necessário fazer a avaliação dos custos envolventes com as atividades de mitigação das ameaças ou vulnerabilidades do sistema e definir muito bem os requisitos adicionais. Após isto, cabe à organização escolher qual das ameaças e vulnerabilidades quer mitigar, transferir ou aceitar o risco de uma possível violação por parte de um atacante [21].

Passando agora para as etapas do processo de análise de ameaças, este processo é elaborado tendo em conta os seguintes passos:

A) Descrição e Caracterização do Sistema

Na primeira etapa [21] do processo de análise de ameaças os responsáveis pelo desenho da segurança dos sistemas precisam de ter um elevado grau de conhecimento do sistema, perceber e saber as necessidades de todos os componentes e ligações e definir *use cases* de atividades a realizar e as suas dependências. A melhor maneira de estruturar esta informação é desenhar um esquema com todas as relações e o modo de funcionamento do sistema (ex. UML) [22]. Basicamente, nesta primeira fase elabora-se um modelo

pormenorizado com todas as relações do sistema a ser implementado. De realçar que nesta etapa ainda não é necessário pensar no que pode correr mal com o sistema, apenas há uma descrição do sistema no seu modo de funcionamento normal.

B) Identificação dos Ativos e Pontos de Acesso do Sistema

Feita a caracterização do sistema chega a altura de pensar em quais são os ativos e pontos de acesso críticos do sistema. Um ativo é um recurso concreto ou abstrato que o sistema tem que proteger contra atividades maliciosas por parte dos atacantes. Bases de dados, *softwares*, servidores, dados e processos de negócio são exemplos de ativos presentes nas organizações. Um ponto de acesso é o que os atacantes vão utilizar para ter acesso aos ativos, ou seja, os atacantes vão explorar as vulnerabilidades e tentar ganhar acesso a estes pontos de acesso com o objetivo final de aceder aos ativos da organização. *Internet* corporativa, *VPN*, ficheiros de configuração e portos de *hardware* são exemplos de pontos de acesso [21] [22].

É importante nesta fase que os responsáveis pela análise de ameaças se coloquem no papel dos atacantes e que consigam visualizar os ativos e pontos de acesso mais críticos e vulneráveis a ataques. É essencial descobrir e definir quais são as potenciais adversidades ao sistema, as motivações, os objetivos dos atacantes e a quantidade de informação que os ataques têm sobre o sistema [21].

C) Determinar as Ameaças ao Sistema

Após o sistema, ativos e pontos de acesso estarem bem definidos e caraterizados, é altura de fazer a seguinte questão: “O que pode correr mal?” [24]. A resposta a esta pergunta é dada utilizando uma técnica de identificação de ameaças e vulnerabilidades, mais conhecida como *STRIDE* [25]. A *STRIDE* foi inventada por *Kohnfelder* e *Garg* [23] e corresponde a uma sigla em que cada letra significa um tipo de ameaça distinto a que um sistema está sujeito. Em suma, através deste conjunto de ameaças consegue-se identificar os tipos de ataques que o sistema pode sofrer [21].

Na tabela 2.1 segue a explicação do que significa cada ameaça *STRIDE* e o vetor da segurança que esta afeta num sistema.

Ameaças	Definição	Vetor da Segurança Afetado
S (*Spoofing*) - Falsificação	Tipo de ataque em que uma pessoa ou programa consegue autenticar-se como sendo outra, falsificando dados de forma ilegítima	Autenticidade
T (*Tampering*) - Adulteração	Modificar dados que não são supostos	Integridade
R (*Repudiation*) - Repúdio	Negação da execução de uma ação	Não Repúdio
I (*Information Disclosure*) - Divulgação de Informação	Expor informação a pessoas que não têm autorização de a ver	Confidencialidade
D (*Denial of Service*) - Negação de Serviço	Ataques desenhados para não deixar um sistema providenciar o seu serviço	Disponibilidade
E (*Elevation of Privilege*) - Elevação de Privilégio	Quando um utilizador ou programa sem privilégios ganha privilégios para fazer algo que não é suposto fazer	Autorização

Tabela 2.1: Ameaças *STRIDE*

Depois de identificadas as ameaças é necessário analisá-las e averiguar se o sistema está suscetível a estas. Uma das possíveis formas de fazer essa análise é a criação de árvores de ataque. As árvores de ataque já existem há muitos anos e de diversas formas, mas, segundo dados mais recentes, têm sido descritas como um método que caracteriza e sistematiza a segurança de um sistema, baseando-se nos possíveis ataques a que o mesmo está vulnerável [28]. O objetivo destas árvores é ilustrar um conjunto de possíveis ataques com um determinado objetivo final, com o intuito de descobrir vulnerabilidades no sistema.

Primeiramente, antes de se passar à construção da árvore, é necessário identificar o(s) objetivo(s) do sistema [26]. De realçar que se esse objetivo não for cumprido é sinal de que o sistema não é seguro contra um determinado ataque e que a organização pode sofrer grandes prejuízos. Após concluído o passo anterior, foca-se num dos objetivos e coloca-se no nodo raiz da árvore de ataque. Depois identificam-se todos os diferentes ataques que comprometem a segurança desse objetivo nos nodos abaixo do nodo raiz. Esta parte da construção repete-se as vezes que forem necessárias até serem encontrados todos os possíveis ataques ao objetivo da árvore. Os nodos mais abaixo, também chamados nodos folha, demonstram as formas como o atacante vai realizar o ataque, ou seja, os sub objetivos. Cada caminho da árvore de ataque representa um ataque único ao objetivo do sistema e consequentemente à organização [27].

Em relação à estrutura da árvore de ataque [26] [27] [30], os nodos folha podem ter dois tipos de relações:

- ***"AND"* (E):** Representa que todos os sub objetivos do ataque devem ser cumpridos para o ataque se realizar. **Ex:** para partir a janela de um carro é preciso uma pedra "**E**" um tecido para abafar o som no ato de partir.
- ***"OR"* (OU):** Representa que se qualquer um dos sub objetivos do ataque for cumprido, o ataque vai realizar-se. **Ex:** para assaltar um carro, pode-se arrombar a porta "**OU**" partir a janela do carro.

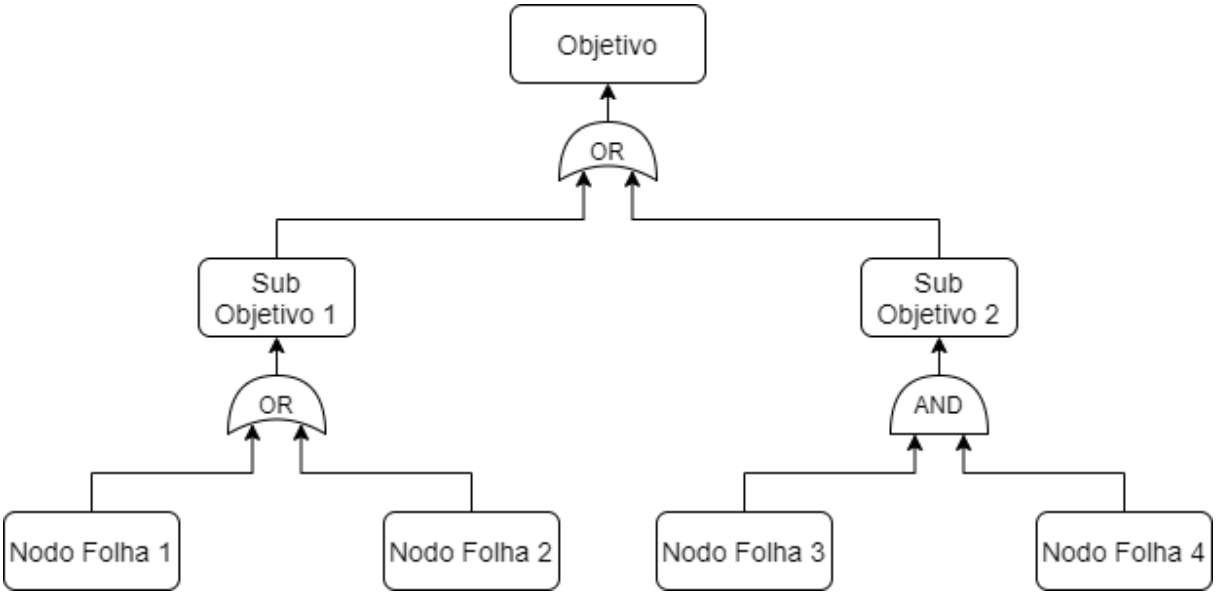

Figura 2.2: Exemplo Estrutural de uma Árvore de Ataque

Neste processo de construção da árvore de ataque podem-se utilizar outras árvores de ataque similares previamente feitas e incorporar alguns exemplos de ataques de modo a agilizar temporalmente este processo.

Após a árvore estar desenhada, todos os ataques mapeados e todas as relações entre nodos definidas passa-se para a fase de definir os parâmetros de análise dos nodos e calcular os seus valores. Os nodos das árvores de ataque podem ter os seguintes parâmetros de análise (estes parâmetros vão variando conforme os objetivos do sistema): se o ataque é intrusivo ou não, se é legal ou ilegal, o custo associado, as habilidades do atacante, os acessos do atacante, a probabilidade de sucesso dos diferentes ataques, o impacto de cada ataque e a dificuldade do ataque. Estes são alguns exemplos de possíveis parâmetros de análise numa árvore de ataque [26].

Depois de estarem definidos os parâmetros a usar e os valores de cada nodo devidamente atribuídos chega-se à fase final do processo de construção da árvore de ataque

que é a fase da avaliação e respetivas conclusões. Nesta etapa os analistas de segurança avaliam todos os valores dos nodos da árvore de ataque e respetivos caminhos, de modo a averiguar se o objetivo do sistema está vulnerável ou não, qual o tipo de ataque com maior probabilidade de sucesso e quais as vulnerabilidades que a organização tem que mitigar antes que seja tarde demais [26].

Estas árvores de ataque ajudam as organizações a gerir de forma mais otimizada o orçamento para a segurança, os efeitos das medidas de segurança em diferentes sistemas e os níveis de segurança de cada ativo da organização [26].

Em suma, nesta etapa da análise de ameaças analisa-se o desenho do sistema com todas as entidades críticas (ativos, pontos de acesso e canais de comunicação) e percorre-se cada uma delas identificando as possíveis ameaças, seguindo a tabela de ameaças *STRIDE*, e criam-se, ao mesmo tempo, hipóteses para as ameaças que violem a segurança dessas entidades. Depois com essas ameaças constrói-se um perfil de ameaça, usando árvores de ataque baseadas nos diferentes tipos de ataque que o sistema pode sofrer e consequentemente causar prejuízo.

D) Mapeamento dos Ativos

Nesta etapa há uma validação da lista de ativos elaborada na fase **B)**, com o objetivo de verificar se todos os ativos foram incluídos na fase de determinar as ameaças e construção da árvore de ataque. Este mapeamento serve para identificar os ativos mais críticos para a organização e determinar o risco que cada responsável pelo ativo está disposto a aceitar. Tendo em conta estes dois parâmetros, é possível definir quais são os ativos prioritários para a organização [22].

Podem ser atribuídos três valores diferentes aos ativos de um sistema:

1. **Elevado:** os ativos classificados com o valor “elevado” devem estar debaixo de medidas severas de segurança. Estes ativos têm um grau de criticidade muito alto para a organização e normalmente estão ligados a sectores de controlo de sistemas ou têm valores financeiros grandes.
2. **Médio:** estes ativos normalmente estão ligados a serviços menos críticos para a organização e com valores financeiros intermédios.
3. **Baixo:** ativos com menos importância e valor financeiro para a organização.

E) Avaliação de Risco

O risco [31] não é nada mais que o impacto de uma ameaça relacionado com a probabilidade dessa ameaça alguma vez se materializar.

Das ameaças e vulnerabilidades retiradas, tanto da identificação das ameaças *STRIDE* como da árvore de ataque, é possível retirar informação sobre qual a ameaça com

um nível maior de risco para a organização. Para ser retirada esta informação deve-se ter em conta o risco associado a cada ativo, o impacto desses ativos, o dano aos ativos em caso de ataque, o tamanho das vulnerabilidades e a probabilidade de ocorrência das ameaças [22].

Com uma boa avaliação de risco consegue-se desenvolver e implementar controlos de segurança, monitorizar estes controlos e com isto facilitar as decisões internas das organizações, em relação às ameaças e vulnerabilidades, nomeadamente no que toca à aceitação desnecessária de risco, às decisões de risco de ativos com criticidades diferentes, à aceitação do risco quando este supera os custos da organização e a antecipar e gerir o risco [31].

F) Plano de Mitigação

A última etapa do processo de análise de ameaças é a construção de um plano de mitigação. Este plano é composto por contramedidas que visão a mitigação das ameaças identificadas pelos analistas de segurança.

Para se identificar contramedidas resultantes da análise de ameaças explicadas anteriormente é necessário avaliar a lista de contramedidas já existente e o mapa de relações entre as contramedidas e as vulnerabilidades e, posteriormente, elaborar uma análise que visa a procura da combinação mais eficaz entre os dois requisitos referenciados. O resultado desta combinação mais eficaz é uma nova contramedida que posteriormente será adicionada ao plano de mitigação de ameaças.

O resultado final do processo de análise de ameaças é um conjunto de contramedidas que irão mitigar as ameaças identificadas num sistema. Estas contramedidas geralmente não são todas implementadas por questões de orçamento, prioridades, tempo, recursos necessários, entre outros. O objetivo passa por implementar aquelas que têm uma melhor relação custo-eficiência contra as ameaças identificadas.

2.7. *Secret Sharing*

Nos dias de hoje a Segurança da Informação tem um papel muito importante nas operações realizadas dentro e fora das empresas ou organizações. A principal preocupação é tornar a informação confiável, autenticável e protegê-la de ser alterada antes de chegar ao recetor final. É necessário [33] tomar ações contra os funcionários incompetentes (funcionários que cometem erros e não sabem que os cometeram), funcionários que tenham em mente a realização de atos maliciosos (Ex: executar ações sem a devida autorização, roubo/fuga de informação, sabotagem de equipamentos ou operações, exploração de

vulnerabilidades, entre outros) e prevenir as organizações contra os ataques externos que possam comprometer o seu bom funcionamento. Uma das soluções encontradas para melhorar os níveis da segurança da informação nestas operações foi o uso do *Secret Sharing*.

O *Secret Sharing* [32] foi primeiramente introduzido em 1979 por *Adi Shamir* [34] e *Blakley* [35], com o objetivo de garantir a confidencialidade, integridade e disponibilidade de dados que não são acessíveis a todos os funcionários [40]. É um método criptográfico desenhado para proteger um "segredo" (dados), distribuindo esse segredo por um *n* número de participantes e por um número *k* de *shares*, de maneira a que apenas seja possível reconstruir o segredo se se reunirem condições suficientes para tal. Outros subgrupos de participantes que não têm os requisitos para aceder a estes dados (segredo), não têm qualquer tipo de conhecimento sobre a informação do segredo. A cada participante é alocado uma parte do segredo (*share*). Um participante com apenas uma parte do segredo não o consegue reconstruir sozinho.

Um modelo de *Secret Sharing* garante que quando um subgrupo de participantes que não está no grupo principal onde é partilhado o segredo não tem qualquer conhecimento da informação sobre o segredo, ou seja, consegue-se assegurar por completo a segurança e a confidencialidade da informação durante o processo de reconstrução do segredo.

Existem diversos modelos de *Secret Sharing*, desde os mais básicos até aos mais complexos. Em baixo seguem-se alguns dos modelos existentes.

2.7.1. *Secret Sharing* Eficiente

Este tipo de modelo de *Secret Sharing* [38] é utilizado para assegurar a segurança de um segredo de uma maneira distribuída. Normalmente é muito usado para a gestão de chaves criptográficas. Neste modelo um segredo *s* é distribuído por *n* participantes e por *k shares*, de maneira que *s* seja facilmente reconstruído a partir de um determinado número de *shares*. É definido um número mínimo de *shares* necessários para a reconstrução do segredo, isto é, mesmo que um grupo de participantes tenha conhecimento de *k-1 shares* não consegue aceder a qualquer informação sobre o segredo *s*. Por exemplo: suponha-se que é necessário aceder a informação de um segredo partilhado por *n* participantes (cada um com o seu *share*), e nem todos os participantes conseguem estar fisicamente presentes, seguindo este modelo, à priori é criada uma condição de limite mínimo de participantes necessário para reconstruir o segredo. Tendo isto em conta, e mesmo com a falta de alguns participantes, é possível aceder à informação do segredo e prosseguir com essa atividade ou operação. A ideia deste esquema de *Secret Sharing (Shamir)* [34] veio oferecer uma maior segurança e confiabilidade em casos em que haja destruição de *shares* ou violações da segurança.

Este modelo é muito mais confiável que os métodos tradicionais de gestão de chaves criptográficas em que a chave é guardada numa simples localização (computador, *pen drive*, cofre ou até mesmo no cérebro humano), pois mesmo na ocorrência de um incidente não planeado, como por exemplo uma avaria do computador, sabotagem de esquipamentos ou morte súbida de algum dos participantes, este consegue oferecer uma forma de reconstruir o segredo e de aceder à respetiva informação.

Uma das limitações deste modelo de *Secret Sharing* é a possível existência de participantes fraudulentos durante o processo de reconstrução do segredo. Se durante o processo de reconstrução do segredo um dos participantes tiver um *share* sabotado, todos os outros participantes irão receber a informação de um segredo inválido, ao invés que o participante fraudulento conseguirá reconstruir o segredo correto, pois sabe todos os *shares* que são confiáveis. A solução para esta limitação é o uso de redundância de *shares*, ou seja, a criação de *backups* para todos os dados envolvidos na reconstrução do segredo com o intuito de detetar os participantes fraudulentos e prevenir que a informação do segredo seja corrompida [38].

2.7.2. *Secret Sharing* Proactivo

Num modelo de *Secret Sharing* o responsável (*dealer*) partilha um segredo por *n* participantes, e mesmo que exista um número de *shares* corrompidos é sempre possível recuperar a informação desse *share*. O que acontece é que com o passar do tempo o número de *shares* corrompidos pode aumentar, e o limite de *shares* que podem ser corrompidos é ultrapassado, contribuindo para uma violação/descoberta do segredo. Ao contrário dos outros modelos, o *Secret Sharing* Proactivo tem estas situações em conta. Este modelo permite ter grandes níveis de confidencialidade durante o tempo de partilha de um segredo, mesmo quando um determinado número de *shares* esteja corrompido. Quando se fala num determinado número de *shares* corrompidos, é o correspondente a pelo menos *n/2-1*, isto é, a confidencialidade é mantida apenas com uma maioria não corrompida de *shares*. Se um grupo de *shares* for corrompido para lá do limite de confiabilidade definido, o segredo pode ser temporariamente desvendado. Uma das medidas utilizadas para manter a confidencialidade em caso de corrupção de *shares* é o *reboot* ao fim de cada ciclo temporal de partilha do segredo. Este modelo parte do principio em que os *shares* e grupos de *shares* possam apagar os dados da sua memória e que estes dados não possam ser recuperados por outros grupos [36].

2.7.3. Secret Sharing Verificável

Este modelo de *Secret Sharing* é uma proposta que visa aumentar os níveis de segurança contra os participantes fraudulentos. Para atingir um maior grau de segurança nos grupos de participantes em que está a ser partilhado um segredo, existe um protocolo de verificação que permite que os participantes fidedignos consigam recuperar um segredo único, evitando assim corrupções nos *shares* dos participantes, e uma possível violação dos segredos partilhados. Este protocolo de verificação tem como principal característica o facto de não serem apenas os participantes envolvidos na partilha do segredo que verificam que os *shares* tenham sido bem distribuídos, mas sim todas as pessoas envolvidas o conseguem fazer [37].

2.7.4. Secret Sharing Multi-Segredo

Este modelo veio melhorar a eficiência dos modelos de *Secret Sharing* Eficiente. Estes últimos são pouco eficientes, pois os *shares* apenas podem ser usados para reconstruir um segredo, enquanto que o *Secret Sharing* Multi-Segredo, permite que quando os *shares* são gerados pelo *dealer* inicial, estes possam ser reutilizados para a reconstrução de outros segredos. Para ocorrer uma segura troca de informação na reconstrução dos vários segredos é necessária uma chave adicional. Esta chave irá permitir que os segredos já descobertos não estejam disponíveis para outros participantes que não façam parte do grupo em que o segredo foi desvendado [39].

2.7.5. Limitações Gerais do Secret Sharing

O *Secret Sharing* [33] não é um método perfeito e como tal apresenta um problema, o tamanho da informação de cada *share* no processo de reconstrução do segredo. Em alguns esquemas de *Secret Sharing*, as estruturas de acesso precisam de um grande volume de dados em relação ao número de participantes, ou seja, quanto maior for o número de participantes, maior será a quantidade de dados existentes nas estruturas de acesso. Tendo em conta este problema, os participantes poderão não ter memória suficiente para armazenar todos os pedaços de dados.

Alguns modelos de Secret Sharing não permitem que os *shares* distribuídos inicialmente pelo dealer possam ser reutilizados para a reconstrução de vários segredos, fazendo com que esses modelos não sejam tão eficientes [39].

Existem modelos de Secret Sharing que não asseguram uma total segurança na presença de participantes fraudulentos, fazendo com que a integridade da informação do segredo seja violada.

Capítulo 3

3. Análise de Ameaças ao Armazenamento de Criptomoedas

Atualmente já existem departamentos na polícia que são responsáveis por monitorizar as transações de criptomoedas, confiscar e encontrar casos em que estejam a ser realizados crimes envolvendo estas moedas, como por exemplo: lavagem de dinheiro, compra e venda de material ilícito, roubos envolvendo criptomoedas, fraudes e muitos mais. Os criminosos tentam ao máximo aproveitar o facto de a legislação das criptomoedas em alguns países ainda não estar bem definida para realizar as suas atividades ilícitas e não serem apanhados.

O processo de apreensão de criptomoedas resultante de atos criminosos é feito da seguinte forma: ao ser detetada alguma atividade ilegal por parte da PJ, rapidamente esta tenta chegar ao local onde está a ser realizada a infração. Após a chegada ao local e captura do criminoso, inicia-se o processo de apreensão das criptomoedas. Numa fase inicial os inspetores responsáveis confiscam todo o material no local do crime, identificam e fazem a respetiva triagem de todos os aparelhos eletrónicos que possam estar envolvidos de certa forma com o crime. Feita essa triagem, o próximo passo passa pela análise de todas as transações realizadas pelo criminoso e investigar onde estão guardadas as criptomoedas. Por exemplo, se o computador ou o *smartphone* estiver ligado consegue-se verificar a existência de *wallet*s (*web wallets, desktop wallets, mobile wallets*) e realizar uma investigação do montante de criptomoedas envolvidas na atividade criminosa. Para se realizar este tipo de investigações recorre-se a um *software* propício de análise.

É de realçar que quando as entidades responsáveis apreendem as criptomoedas, o criminoso deixa de ter acesso às mesmas. Quando são encontradas as *wallet*s com o respetivo montante de criptomoedas, essas são confiscadas e cabe às entidades responsáveis armazená-las da maneira mais segura.

Este trabalho foca-se nesta última etapa de armazenamento, pois é aqui que as criptomoedas apreendidas são guardadas, em *wallets*.

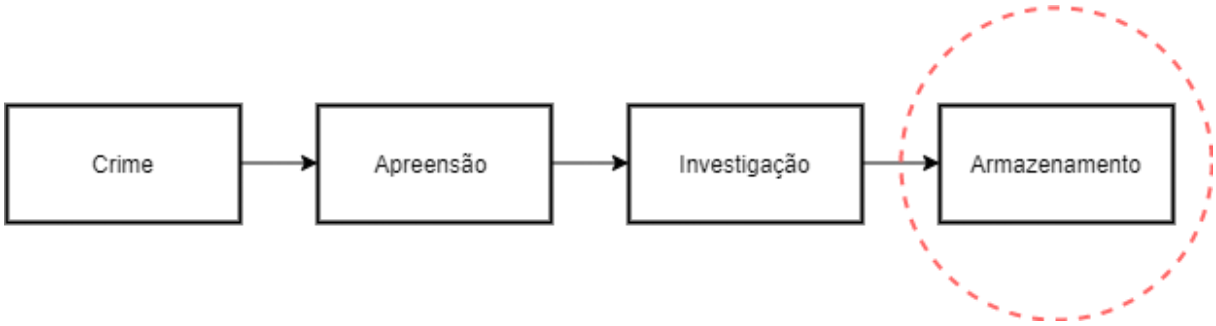

Figura 3.1: Fluxo das Atividades dos Crimes Envolvendo Criptomoedas.

Neste capítulo vai ser realizada uma análise de ameaças ao processo de armazenamento de criptomoedas em diferentes tipos de *wallet*s dentro da sede da PJ. O objetivo desta análise é verificar qual dos tipos de *wallet*s é o que apresenta menos ameaças e vulnerabilidades de segurança e consequentemente menos risco de ataques internos ou externos, de modo a tornar este processo de armazenamento o mais seguro possível.

Para se chegar à conclusão anterior vão ser realizadas algumas etapas do processo de análise de ameaças, nomeadamente, a fase da descrição e caracterização, identificação dos ativos e pontos de acesso e, finalmente, a fase de determinação das ameaças. Na primeira das fases apresenta-se um modelo do sistema que será alvo da análise, uma descrição do que o sistema faz e os seus intervenientes, e uma caracterização das relações existentes entre cada entidade do modelo. Na segunda fase são identificados os ativos e pontos de acesso mais críticos do modelo, bem como algumas ideias de como é que os atacantes poderão aceder à informação que está dentro das *wallets*. Na fase de determinação das ameaças vai ser usada a tabela de ameaças *STRIDE* para identificar os tipos de ameaças a que as *wallets* estão sujeitas e as árvores de ataque, para avaliar quais dessas ameaças têm maior probabilidade de se materializarem em ataques. Vão ser elaboradas cinco árvores de ataque (uma para cada tipo de *wallet*) e uma análise dos parâmetros escolhidos para a avaliação de cada árvore de ataque. Feita essa análise chega-se finalmente ao objetivo deste capítulo, verificar qual o tipo de *wallet* mais seguro para a PJ implementar, após a apreensão de criptomoedas fruto de atividades ilícitas.

Os tipos de *wallets* que podem armazenar as criptomoedas apreendidas após uma investigação policial podem ser:

- *Paper Wallets*
- *Mobile Wallets*
- *Web Wallets*
- *Desktop Wallets*
- *Hardware Wallets*

Estes são os tipos de *wallets* que serão alvo da análise de ameaças e consequente construção de árvores de ataque, para decidir qual das cinco reúne melhor índice de segurança para a PJ poder implementar.

3.1. Identificação e Caracterização

Esta análise de ameaças vai ser elaborada a cinco tipos de *wallets*, em que cada uma delas armazena de forma diferente a chave privada que dá acesso ao montante de criptomoedas.

Desde já, vai ser assumido que as *wallets* são guardadas dentro da sede da PJ, em dispositivos de *hardware*, com ou sem ligação à internet, em servidores ou em cofres. Este modo de armazenamento depende do tipo de *wallet*. Assim sendo, as *Paper Wallet*s vão ser guardadas em cofres, as *Mobile Wallet*s e as *Desktop Wallet*s vão ser guardadas em dispositivos *hardware*s com ligação à *internet* (ex. computadores e *smartphones*), as *Web Wallet*s em Servidores corporativos e as *Hardware Wallet*s em dispositivos de *hardware* sem ligação à *internet* (ex. *pen drives*, discos externos, entre outros).

É de frisar que normalmente as organizações que apreendem criptomoedas e as guardam em *wallet*s optam apenas por um dos tipos de *wallet*s apresentados em cima (o mais seguro do ponto de vista deles e das análises de segurança que realizaram).

A figura 3.2 apresenta o modelo do sistema em análise neste capítulo, com todos os componentes intervenientes e suas relações.

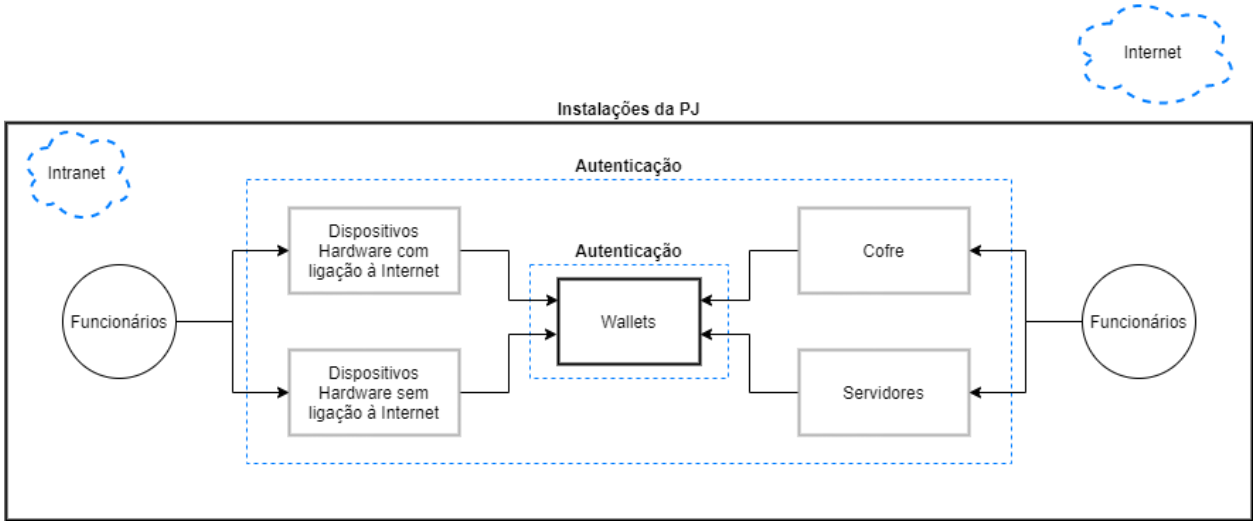

Figura 3.2: Modelo do Sistema

Neste modelo estão representadas todas as componentes envolvidas no processo de armazenamento de criptomoedas em *wallet*s na sede da PJ.

Bem no centro do modelo pode-se encontrar a entidade "*Wallet*s". Nestas são onde estão armazenados os montantes de criptomoedas apreendidas nas investigações da PJ. Esta entidade é a mais importante de todo o sistema e é também a entidade que não se quer que nenhum ataque tenha acesso à sua informação. O objetivo deste sistema é que as criptomoedas estejam armazenadas em *wallet*s na sede da PJ com os maiores níveis de segurança possíveis, ou seja, proteger o acesso indevido e não autorizado à informação das *wallet*s. Estas *wallet*s estão protegidas por um fator de autenticação, uma *password* de acesso. Apenas quem conhece essa *password* da *wallet* consegue ter acesso às chaves privadas e consequentemente ao valor de criptomoedas lá armazenado.

As quatro entidades à volta são os lugares ou dispositivos diferentes em que se pode armazenar as *wallet*s. Cada uma desta entidades está protegida com um fator de autenticação e apenas funcionários autorizados têm as credenciais de acesso. Se qualquer outra pessoa (interna ou externa) ou funcionários sem autorização tentar ganhar acesso à informação presente nas *wallet*s é considerado uma violação de segurança ao sistema. Pessoas internas são interpretadas como pessoas que visitam as instalações da PJ e pessoas externas são interpretadas como atacantes.

O limite deste sistema representado pelo retângulo maior são as instalações físicas da PJ. Dentro deste limite existe a *Intranet* que é uma rede privada que apenas pode ser acedida por utilizadores ou funcionários internos, com credenciais de acesso, e as restantes entidades referidas anteriormente. Todas as entidades dentro deste limite seguem as normas e diretrizes da PJ. Fora deste limite existe a *Internet* à qual a PJ não tem legislação, mas defende-se dos seus perigos usando *firewalls* e antivírus.

Neste modelo estão representadas todas as formas de armazenar as criptomoedas e são utilizadas as setas para identificar as únicas pessoas que podem ter acesso a elas. Sendo que, para ter acesso terão que ter as credenciais de acesso para os diversos níveis de autenticação instalados no sistema.

3.2. Identificação de Ativos e Pontos de Acesso

Agora que já é conhecido o sistema e o que faz e estão identificadas todas as entidades e relações intervenientes, é altura de passar à identificação dos ativos e pontos de acesso. Os ativos mais críticos deste sistema são:

- ***Wallet*s:** onde estão armazenados os montantes de criptomoedas.
- **Cofre:** espaço físico onde podem estar guardadas as *paper wallets*.
- **Servidores:** tecnologia onde podem estar guardadas as *web wallets*.

- **Dispositivos *Hardware* com ligação à *Internet*:** dispositivos onde podem estar guardadas as *mobile* e *desktop wallets*.
- **Dispositivos *Hardware* sem ligação à *Internet*:** dispositivos onde podem estar guardadas as *hardware wallets*.

As *wallet*s são o ativo mais crítico de todo o sistema, pois o objetivo é que ninguém aceda ao seu conteúdo sem estar devidamente autorizado. Os restantes quatro ativos são também muito críticos para o sistema, porque uma vez comprometida a sua segurança, torna-se mais fácil aceder às *wallet*s.

Em relação os pontos de acesso mais críticos do sistema, tem-se:

- ***Internet***
- ***Intranet*:** rede corporativa limitada a utilizadores ou funcionários com permissões de acesso.
- **Funcionários:** consideram-se os funcionários um ponto de acesso, pois estes podem ser um meio utilizado por um atacante para ter acesso às *wallet*s.

Estes três pontos de acesso são os únicos meios que podem ser utilizados para comprometer a segurança dos ativos críticos do sistema.

Identificados os ativos e pontos de acesso críticos para o sistema, é necessário pensar e identificar os objetivos, motivações dos atacantes e a quantidade de informação que estes sabem do sistema. Na tabela 3.1 segue uma tabela resumo com a descrição de cada um destes parâmetros.

Parâmetros	Descrição
Objetivos dos atacantes	Obter os montantes de criptomoedas
Motivos dos atacantes	Enriquecer, satisfação pessoal, conflitos no trabalho e comprometer a segurança da organização
Quantidade de informação que os atacantes sabem sobre o sistema	Se não for funcionário da PJ, não tem qualquer tipo de informação sobre o sistema. Se for um funcionário da PJ com autorização de acesso às *Wallet*s, tem conhecimento de toda a informação sobre o sistema. Caso contrário não tem conhecimento de rigorosamente nada.

Tabela 3.1: Parâmetros dos Atacantes

Nota: para este sistema existem dois tipos de atacantes: os atacantes externos que são pessoas que elaboram o ataque fora das instalações da PJ e os atacantes internos que são os funcionários da própria organização.

Nesta fase da análise de ameaças é importante também começar a pensar em alguns exemplos de adversidades que podem comprometer o sistema. Funcionários corruptos ou maliciosos, avarias de dispositivos de *software* ou *hardware*, falhas nos diferentes níveis de autenticação, falta de atualização dos dispositivos, *firewalls* e antivírus e catástrofes naturais são alguns dos exemplos de adversidade que comprometem a segurança do sistema.

3.3. Determinação das Ameaças

Nesta etapa é quando se identifica o que pode correr mal com o sistema, por outras palavras, é a fase de identificação das ameaças.

Para determinar as ameaças do sistema em análise usou-se a tabela de ameaças *STRIDE* [23] e relacionou-se com os ativos e pontos de acesso críticos do sistema [29]. Cada ativo ou ponto de acesso que está marcado com um “x” nos tipos de ameaças *STRIDE* representa que este está sujeito a este tipo de ameaça. Em sentido oposto, os que não estiverem marcados com um “x”, não estão sujeitos a esse tipo de ameaça.

Ativos/Pontos de Acesso	Ameaças *STRIDE*					
	Falsificação	Adulteração	Repúdio	Divulgação de Informação	Negação de Serviço	Elevação de Privilégio
*Wallet*s	**x**	**x**		**x**		
Cofre	**x**	**x**		**x**		
Servidores	**x**	**x**		**x**	**x**	
Dispositivos *Hardware* com ligação à Internet	**x**	**x**		**x**	**x**	
Dispositivos *Hardware* sem ligação à Internet	**x**	**x**		**x**		
Internet					**x**	
Intranet					**x**	
Funcionários	**x**		**x**	**x**		**x**

Tabela 3.2: Ameaças *STRIDE* por Ativos e Pontos de Acesso do Sistema

Utilizou-se esta tabela de ameaças com o objetivo de facilitar a identificação de algumas ameaças a que o sistema está sujeito. As restantes ameaças e vulnerabilidades vão ser identificadas nas árvores de ataque que são o passo seguinte desta etapa.

Para cada tipo de *wallet* vão ser elaboradas árvores de ataque com o objetivo de descobrir novas ameaças, vulnerabilidades e traçar um perfil de atacante. Cada árvore de ataque vai estar relacionada com estas ameaças já identificadas. Primeiramente será feita uma descrição deste tipo de *wallet*, bem como a que ativo está relacionada. Posteriormente será desenhada a árvore de ataque com as suas respetivas relações e descrição dos possíveis ataques ao sistema. E finalmente proceder-se-á à avaliação dos parâmetros da árvore de ataque escolhidos para este sistema.

Quanto à avaliação dos parâmetros da árvore de ataque, vão ser construídas tabelas após o desenho das árvores de ataque, em que cada ataque vai ser avaliado segundo os parâmetros escolhidos. Os parâmetros de avaliação escolhidos para analisar este sistema são:

- **Dificuldade técnica do ataque:** tem que ver com o nível e conhecimento técnico para a execução do ataque.
- **Probabilidade de sucesso do ataque:** probabilidade de esse ataque se materializar e comprometer o sistema.

- **Custo do ataque:** valor monetário necessário para a execução do ataque.

A escala de valores para cada parâmetro tem as seguintes atribuições:

- Baixo
- Médio
- Elevado

Atribuídos todos os valores aos parâmetros de análise faz-se a avaliação para cada tipo de *wallet* e no final comparam-se os valores e escolhe-se o tipo de *wallet* com menos ameaças e vulnerabilidades. O objetivo passa por escolher um tipo de *wallet* para a PJ implementar quando apreende criptomoedas resultantes de crimes.

3.3.1. *Paper Wallet*

Neste tipo de *wallet* a chave privada encontra-se encriptada na forma de *QR-Codes* em formato de papel. Como o próprio nome indica, este tipo de *wallets* são praticamente impossíveis de sofrer qualquer tipo de ataque externo (ex. *hackers*).

Para os atacantes o principal objetivo é ter acesso às criptomoedas que estão dentro da *paper wallet*. Este tipo de *wallet*s são guardadas normalmente em espaços físicos, sob a proteção de um responsável. Para esta *wallet* vai ser usado um cofre como espaço físico de armazenamento.

Para ter acesso à *wallet* serão esquematizados na figura 3.3 os possíveis ataques numa árvore de ataque.

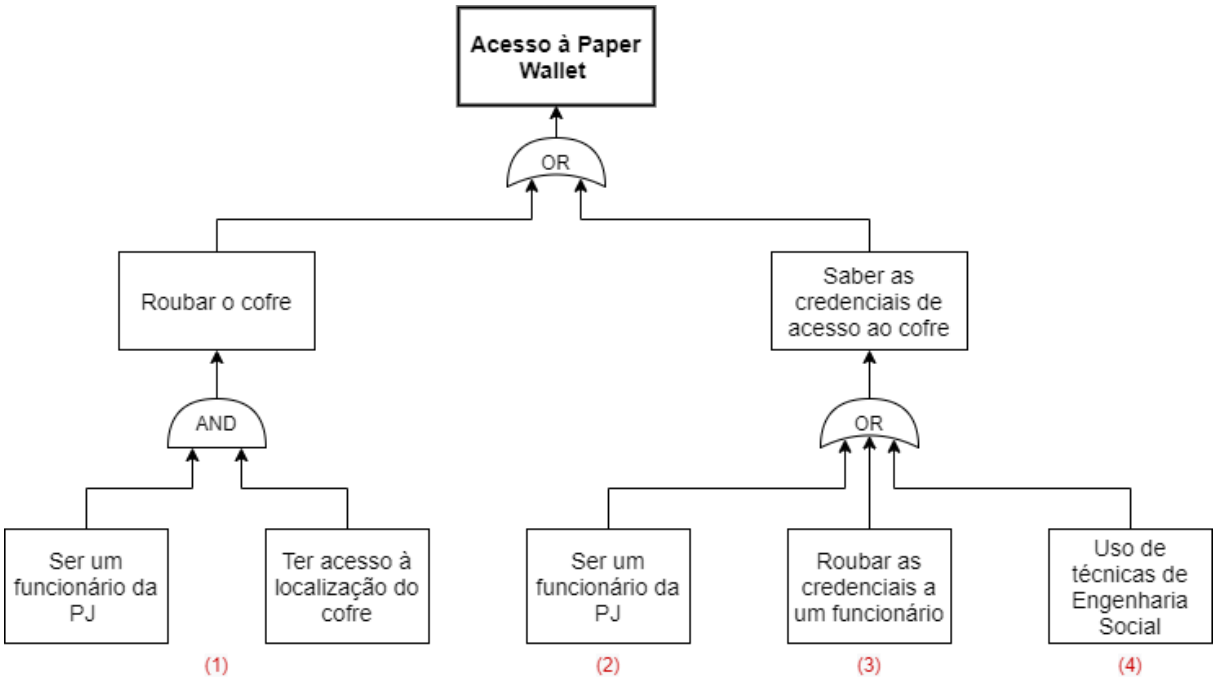

Figura 3.3: Árvore de Ataque ao Acesso à *Paper Wallet*

Nota: os números entre parêntesis na árvore de ataque identificam os possíveis ataques à segurança da *paper wallet*.

De realçar que neste tipo de *wallet* as ameaças são internas, ou seja, a única possibilidade de aceder à *paper wallet* é se o atacante for um funcionário da PJ. Por vezes, insatisfação com o trabalho ou rendimentos, pressões emocionais e/ou mau estar familiar levam a que os funcionários ajam de maneira incorreta e tentem prejudicar a organização.

Neste tipo de *wallet* existem duas formas diferentes de um atacante tentar aceder à *paper wallet* e roubar as criptomoedas lá armazenadas. Uma delas é roubar o cofre onde está esta *wallet* e a outra é obter as credenciais de acesso ao cofre. Tendo em conta estas duas formas de aceder à *paper wallet* conseguiu-se através da árvore de ataque retirar quatro possíveis ataques.

No primeiro ataque **(1)**, se existir um funcionário que tenha em mente atos maliciosos para com a organização e tiver acesso à localização do cofre, pode conseguir roubar o cofre e consequentemente aceder à *paper wallet*. Neste ataque existe uma relação de *"AND",* porque uma pessoa apenas consegue roubar o cofre se for funcionário e souber onde fica o cofre dentro das instalações da PJ, caso contrário é muito difícil roubar o cofre.

A segunda forma de aceder à *paper wallet* é saber as credenciais de acesso ao cofre onde esta está guardada. Para isto acontecer existem três diferentes possibilidades e não

existe qualquer grau de dependência entre estas. Usou-se, neste caso, uma relação de *"OR",* pois basta uma delas ser cumprida e são conhecidas as credenciais de acesso ao cofre.

No segundo ataque **(2)**, se existir um funcionário que tenha em mente atos maliciosos na organização e souber as credenciais de acesso ao cofre, muito facilmente consegue aceder à *paper wallet*.

No terceiro ataque **(3)**, se um funcionário roubar as credencias de outro que tenha as credenciais de acesso ao cofre consegue aceder à *paper wallet*. Neste ataque pode-se concluir, segundo a tabela de ameaças *STRIDE*, que a falsificação é a principal ameaça.

E finalmente no quarto ataque **(4)** há o uso de técnicas de Engenharia Social por parte de um funcionário para saber as credenciais de acesso de outro que as tenha e consequentemente ter acesso à *paper wallet*. Neste ataque a principal ameaça, segundo a tabela de ameaças *STRIDE*, é a divulgação de informação confidencial a pessoas não autorizadas.

Na tabela 3.3 está a análise dos ataques através dos parâmetros de avaliação das árvores de ataque selecionados para esta *wallet*.

Ataque	**Dificuldade técnica do ataque**	**Probabilidade de sucesso do ataque**	**Custo do ataque**
1	Baixa	Baixa	Baixo
2	Baixa	Elevada	Baixo
3	Baixa	Baixa	Baixo
4	Elevada	Baixa	Baixo

Tabela 3.3: Avaliação dos Ataques à *Paper Wallet* segundo os Parâmetros de Análise

Na tabela 3.3 estão identificados os ataques que podem comprometer a *paper wallet* (quatro ataques) e a classificação dos três parâmetros escolhidos à priori para analisar cada tipo de ataque. Na tabela o ataque número **(2)** está selecionado a cinzento, pois é o ataque com uma dificuldade técnica baixa e com uma elevada probabilidade de sucesso, logo é com este tipo de ataques que a PJ tem que se preocupar se implementar a *paper wallet* como mecanismo de armazenamento das criptomoedas.

De frisar que este tipo de ataque apenas se concretiza se existirem funcionários fraudulentos dentro das instalações da PJ. Se dentro das instalações da PJ todos os funcionários estiverem satisfeitos com o seu trabalho e acima de tudo forem responsáveis pelas suas atividades, esta ameaça tem uma probabilidade baixíssima de alguma vez representar qualquer tipo de perigo para a implementação da *paper wallet*.

Este tipo de *wallet* é uma boa solução para o armazenamento de criptomoedas, pois a única ameaça de grande relevo é interna (funcionários fraudulentos) e pode ser controlável pela PJ. O facto de este tipo de *wallet* não estar ligado à *Internet* ou a qualquer mecanismo com ligações externas torna muito difíceis os ataques de carisma cibernético e consequentemente garantindo elevados níveis de segurança.

3.3.2. *Mobile Wallet*

A segunda opção para armazenar as criptomoedas confiscadas após uma investigação criminal é a utilização de uma *Mobile Wallet*.

Esta *wallet* funciona como uma aplicação para *smartphone* onde as chaves privadas são guardadas e também é possível movimentar as criptomoedas usando apenas o telemóvel. A *Mobile Wallet* é muito prática, mas apresenta algumas ameaças tendo em conta que está num dispositivo de *hardware* com ligação à *Internet* e consequentemente torna-a suscetível a ataque externos (ex. *hackers*).

Para este tipo de *wallet* o principal objetivo dos atacantes é aceder ao valor de criptomoedas armazenadas nesta *wallet*. Para esta *wallet* vai ser usado um *smartphone* (dispositivo de *hardware* com ligação à *Internet*) como meio de armazenamento.

Para ter acesso à *wallet* serão esquematizados na figura 3.4 os possíveis ataques numa árvore de ataque.

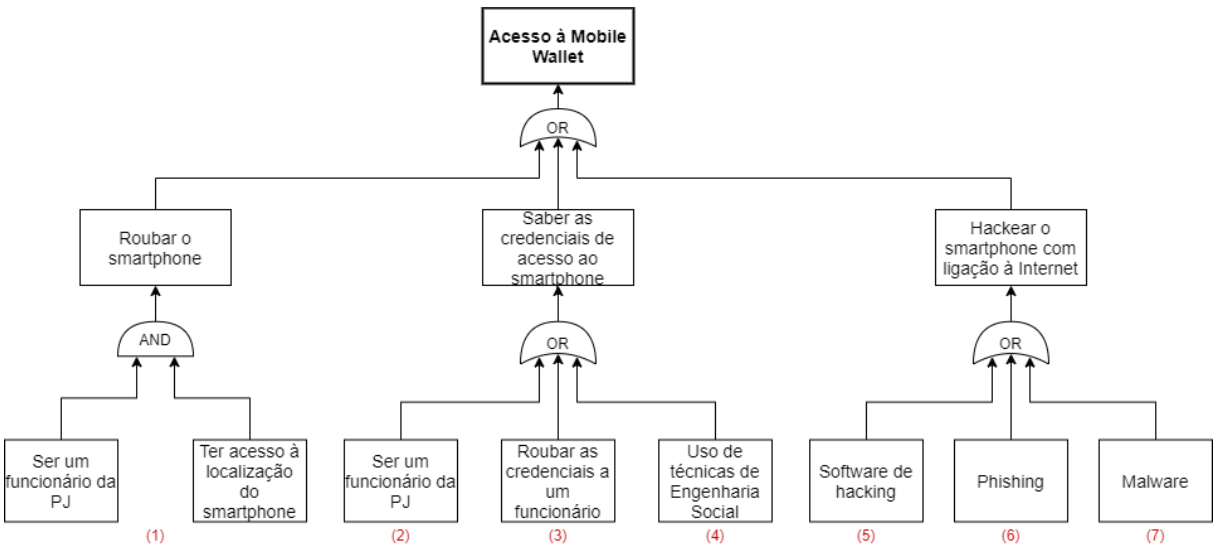

Figura 3.4: Árvore de Ataque ao Acesso à *Mobile Wallet*

Neste tipo de *wallet* as ameaças são tanto de cariz interno como externo, isto é, os atacantes podem ser funcionários da PJ ou pessoas externas com objetivos maliciosos.

Neste tipo de *wallet* existem três formas diferentes de um atacante aceder à *mobile wallet* e roubar as criptomoedas lá armazenadas. A primeira delas é roubar o smartphone onde está a *wallet*, a segunda é, de alguma maneira, obter as credenciais de acesso ao *smartphone* e a última é *hackear* o *smartphone*. De realçar que nesta última o *smartphone* tem que estar ligado à *Internet*, caso contrário não representa qualquer tipo de ameaça para com a *wallet*. Tendo em conta estas três formas de aceder à *mobile wallet*, conseguiu-se, através da árvore de ataque, retirar sete possíveis ataques.

No primeiro ataque **(1)**, se existir um funcionário que tenha em mente atos maliciosos para com a organização e tiver acesso à localização do *smartphone*, pode conseguir roubá-lo e consequentemente aceder à *mobile wallet*. Neste ataque existe uma relação de *"AND",* porque uma pessoa apenas consegue roubar o *smartphone* se for funcionário e tiver conhecimento de onde está guardado o *smartphone* dentro das instalações da PJ. Caso contrário é impossível roubá-lo.

A segunda forma de aceder à *mobile wallet* é ter conhecimento das credenciais de acesso ao *smartphone* onde esta está guardada. Para isto acontecer existem três diferentes possibilidades, sem qualquer dependência entre elas. Usou-se, neste caso, uma relação de *"OR",* pois basta uma delas ser cumprida e são conhecidas as credenciais de acesso ao *smartphone*.

No segundo ataque **(2)**, se existir um funcionário fraudulento na organização e souber as credenciais de acesso ao *smartphone*, muito facilmente consegue aceder à *mobile wallet* e roubar as criptomoedas apreendidas.

No terceiro ataque **(3)**, se um funcionário roubar as credencias de outro que tenha as credenciais de acesso ao *smartphone*, consegue aceder à *mobile wallet*. Neste ataque pode-se concluir, segundo a tabela de ameaças *STRIDE*, que a falsificação é a principal ameaça à segurança da *wallet*.

No quarto ataque **(4)** há o uso de técnicas de Engenharia Social por parte de um funcionário para saber as credenciais de acesso de outro que as tenha e consequentemente ter acesso à *mobile wallet*. Neste ataque à *mobile wallet* a principal ameaça, segundo a tabela de ameaças *STRIDE*, é a divulgação de informação confidencial a pessoas não autorizadas.

E finalmente, a terceira forma de aceder à *mobile wallet* é realizar um ataque cibernético ao *smartphone*, mas só se este estiver ligado à *Internet*. É possível ter acesso à *mobile wallet* se se realizarem, por exemplo, os seguintes três ataques. Usou-se neste caso uma relação de *"OR"* porque não existem dependências entre nodos.

No quinto ataque **(5)** existe o recurso a *softwares* de *hacking*, ou seja, *software* com capacidade de exploração de vulnerabilidades do sistema e consequente violação do mesmo. Neste tipo de ataques é necessário um grande nível de conhecimentos técnicos e um grande

investimento monetário por parte do atacante. Neste ataque pode-se verificar, segundo a tabela de ameaças *STRIDE*, que a principal ameaça é a negação do serviço.

O sexto ataque **(6)** refere-se ao uso de técnicas de *phishing* para tentar obter acesso à *mobile wallet*. Estas técnicas normalmente usam o *email* como fonte de distribuição e são recebidas em formato de anúncios, pedidos de atualizações de dados e *hiperlinks*.

Por fim, no sétimo ataque **(7)**, se um funcionário aceder a *sites* que não são autorizados pela organização ou a sites maliciosos, pode correr o risco de apanhar algum tipo de *malware* e comprometer a segurança total do sistema. Comprometendo a segurança do sistema, dá-se um aumento das possibilidades de ataques externos e consequente acesso à *mobile wallet*.

Na tabela 3.4 segue a análise dos ataques através dos parâmetros de avaliação das árvores de ataque selecionados para esta *wallet*.

Ataque	Dificuldade técnica do ataque	Probabilidade de sucesso do ataque	Custo do ataque
1	Baixa	Elevada	Baixo
2	Baixa	Elevada	Baixo
3	Baixa	Baixa	Baixo
4	Elevada	Baixa	Baixo
5	Elevada	Baixa	Elevado
6	Elevada	Baixa	Elevado
7	Elevada	Baixa	Elevado

Tabela 3.4: Avaliação dos Ataques à *Mobile Wallet* segundo os Parâmetros de Análise

Na tabela 3.4 estão apresentados os sete possíveis ataques à *mobile wallet*, bem como a classificação de cada parâmetro escolhido para a análise. O objetivo destas tabelas é selecionar aqueles ataques com uma maior probabilidade de acontecer, com uma menor dificuldade técnica e com um custo mais baixo, pois são estes os mais prováveis de acontecer. Um ataque que envolva muito conhecimento técnico não vai ocorrer tão recorrentemente como um ataque que envolva conceitos mais básicos.

Nesta tabela podemos ver que existem dois ataques identificados com outra cor, isso significa que são os mais prováveis de acontecer em relação à *mobile wallet*. São estes ataques que a PJ tem que se preocupar caso decida implementar a *mobile wallet* como mecanismo de armazenamento das criptomoedas.

Os ataques **(5) (6) (7)**, embora exijam muitos conhecimentos técnicos e custos elevados de implementação, têm uma probabilidade de sucesso baixa, significando que não vão ocorrer tantas vezes como os outros dois, mas é necessário estar alerta para estes tipos

de ataque e melhorar ao máximo as ferramentas corporativas de proteção contra estes tipos de ataques.

Em relação aos outros dois ataques, **(1)** e **(2)**, estes só ocorrem se existirem na PJ funcionários fraudulentos. Mais uma vez, estes dois ataques têm baixa probabilidade de ocorrer se estiver tudo bem com os funcionários dentro e fora da empresa.

Este tipo de *wallet* já não é tão segura como a *paper wallet*, pois é alocada num *smartphone* com ligação à *Internet*, tornando-se assim mais suscetível a novas ameaças e ataques externos (ex. *hackers*).

Nota: uma *wallet* que esteja num dispositivo com ligação à *Internet* é menos confiável em termos de segurança do que uma que não esteja, pois está suscetível a um maior número de ameaças do ciberespaço.

3.3.3. *Web Wallet*

A terceira opção para armazenar as criptomoedas confiscada após uma investigação criminal é a utilização de uma *Web Wallet*.

Neste tipo de *wallet* as chaves privadas são guardadas nos servidores da organização. Todos os funcionários da empresa têm acesso à *Intranet* da organização, ou seja, algum funcionário com acessos privilegiados, conhecimentos dos sistemas da organização e outros conhecimentos de *hacking* consegue ter acesso à *web wallet*. O mesmo é aplicado a um atacante de fora da organização. O facto de as chaves privadas estarem guardadas em servidores torna estes mais suscetíveis a ataques externos.

Para este tipo de *wallet* o principal objetivo dos atacantes é aceder aos Servidores Corporativos onde se encontram as chaves privadas armazenadas e consequentemente ter acesso à *web wallet*.

Para um atacante ter acesso à *web wallet* serão esquematizados na figura 3.5 os possíveis ataques numa árvore de ataque.

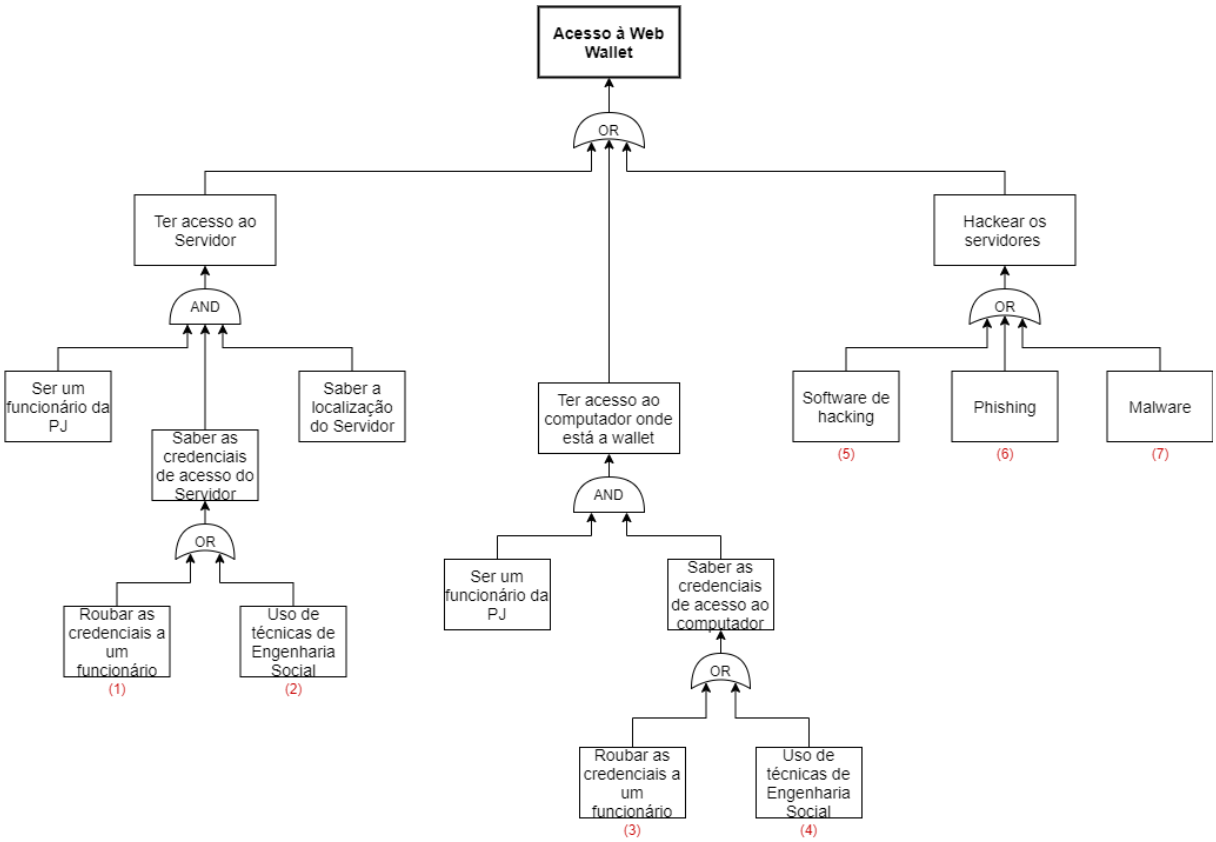

Figura 3.5: Árvore de Ataque ao Acesso à *Web Wallet*

Nota: as *web wallet*s estão guardadas em computadores, mas as suas chaves privadas estão nos servidores corporativos da organização.

Na *web wallet* as ameaças tanto podem ser internas (funcionários fraudulentos), como externas (pessoas externas que têm em mente a realização de atos maliciosos, com o objetivo de prejudicar a organização).

Neste tipo de *wallet* existem três formas diferentes de um atacante aceder à *web wallet* e roubar as criptomoedas lá guardadas. A primeira forma é ter acesso ao servidor que armazena a chave privada da *wallet*, a segunda forma é ter acesso ao computador onde está a *wallet* e a terceira forma é *hackear* o servidor onde está armazenada a chave privada.

Tendo em conta estas três formas de aceder à *web wallet* conseguiu-se, através da árvore de ataque, retirar sete possíveis ataques.

Na primeira forma de aceder à *web wallet* usou-se uma relação de *"AND",* uma pessoa só tem acesso ao servidor corporativo se for funcionário da PJ, se tiver em sua posse as credenciais de acesso ao servidor e souber a sua exata localização física. Se estas três condições não forem cumpridas este ataque não se pode realizar. Posteriormente, no nodo

das credenciais de acesso ao servidor, usou-se uma relação de *"OR",* pois existem duas formas diferentes de obter essas credenciais.

No primeiro ataque **(1)**, se um funcionário fraudulento da PJ conseguir roubar as credenciais de acesso ao servidor e saber a localização exata onde este se encontra, conseguirá ter acesso ao servidor e consequentemente acesso à *web wallet*.

No segundo ataque **(2)** um funcionário fraudulento pode usar técnicas de engenharia social para conseguir saber as credenciais de acesso do servidor e, se souber a localização física do mesmo, consegue aceder à *wallet*.

Em relação à segunda forma de aceder à *web wallet*, é necessário ter acesso ao computador onde está a *wallet* para ser possível ter acesso à *web wallet*. Utilizou-se uma relação de *"AND",* pois só pode ter acesso a um computador quem é funcionário e souber as credenciais de acesso do mesmo. Já no nodo das credenciais de acesso ao computador usou-se uma relação de *"OR",* pois existem duas maneiras diferentes de conseguir obter essas credenciais (roubo ou técnicas de engenharia social).

No terceiro **(3)** e quarto ataque **(4)**, respetivamente, um funcionário da PJ pode roubar as credenciais de outro funcionário ou usar métodos de engenharia social, com o objetivo de saber as credenciais de acesso ao computador onde está a *web wallet*.

E por fim, na última forma de aceder à *web wallet*, é preciso *hackear* o servidor onde estão armazenadas as chaves privadas. Usou-se nesta uma relação de *"OR",* pois existem pelo menos três possíveis maneiras de *hackear* o servidor corporativo (uso de ferramentas de *hacking*, *phishing* e *malwares*).

No quinto ataque **(5)** recorre-se ao uso de ferramentas de *hacking* para aceder aos servidores corporativos e consequentemente obter a chave privada da *web wallet*. Neste tipo de ataques é necessário um grande nível de conhecimentos técnicos e um grande investimento monetário por parte do atacante.

No sexto ataque **(6)** recorre-se ao uso de técnicas de *phishing* para tentar obter acesso ao servidor.

Por último, no sétimo ataque **(7)**, a organização pode ser alvo de um ataque de *malware* nos seus sistemas e este pode comprometer a segurança dos servidores corporativos. Estando comprometidos os servidores, as *web wallet* também estão em risco e por sua vez as criptomoedas também.

Na tabela 3.5 segue a análise dos ataques através dos parâmetros de avaliação das árvores de ataque selecionados para esta *wallet*.

Ataque	Dificuldade técnica do ataque	Probabilidade de sucesso do ataque	Custo do ataque
1	Baixa	Baixa	Baixo
2	Elevada	Baixa	Baixo
3	Baixa	Elevada	Baixo
4	Elevada	Elevada	Baixo
5	Elevada	Baixa	Elevado
6	Elevada	Baixa	Elevado
7	Elevada	Baixa	Elevado

Tabela 3.5: Avaliação dos Ataques à *Web Wallet* segundo os Parâmetros de Análise

Na tabela 3.5 estão apresentados os sete possíveis ataques à *web wallet* e a respetiva classificação de cada parâmetro escolhido para a análise. Dos sete ataques apenas o **(3)** e o **(4)** têm probabilidades de sucesso elevadas, logo vão ser esses que, em caso de implementação da *web wallet*, a PJ tem que se preocupar e proteger. De realçar que estes dois tipos de ataque só acontecem se existirem funcionários fraudulentos dentro das instalações da PJ, caso contrário a probabilidade de alguma vez estes ataques se materializarem é baixa.

Em relação ao ataque **(3)**, ser um funcionário e roubar as credenciais de acesso a outro para ter acesso ao computador onde está a *web wallet* exige poucos conhecimentos técnicos e tem uma probabilidade elevada de sucesso. Entende-se por sucesso o acesso à *web wallet*.

No ataque **(4)**, ser um funcionário e utilizar técnicas de engenharia social para saber as credenciais de acesso ao computador e posteriormente aceder à *web wallet* exige muitos conhecimentos técnicos, ou seja, para além de ser um ataque difícil, tem um custo de execução baixo e uma probabilidade de sucesso elevada o que pode levar a que um funcionário fraudulento com alguns conhecimentos de engenharia social tente executar este ataque.

Os restantes ataques podem vir a acontecer caso a PJ decida implementar este tipo de *wallet*, mas requerem conhecimento técnico e um investimento muito maior, isto é, a organização tem que estar ciente de que estes ataques poderão ocorrer um dia, mas em caso de existirem funcionários fraudulentos os ataques **(3)** e **(4)** poderão ocorrer mais frequentemente.

O facto de este tipo de *wallet* estar em computadores e as suas chaves privadas armazenadas nos servidores corporativos abre as portas para um maior número de ameaças e consequentemente para possíveis ataques à sua segurança.

3.3.4. *Desktop Wallet*

A quarta opção para armazenar as criptomoedas confiscada após uma investigação criminal é a utilização da *Desktop Wallet*.

Este tipo de *wallet* é descarregada e instalada num computador e guarda as chaves privadas no disco rígido. A *desktop wallet* não precisa de terceiros para usar os seus dados, como é o acaso da *Web Wallet* que precisa dos servidores corporativos para armazenar as suas chaves privadas, tornando-se assim uma solução um pouco mais segura. Embora à primeira vista este tipo de *wallet* pareça mais seguro, os computadores podem ser ligados à *Internet* impossibilitando assim uma total confiança no armazenamento de criptomoedas.

Nota: um tipo de *wallet* que esteja num dispositivo com ligação à *Internet* está sempre mais suscetível a um maior número de ameaças do que uma *wallet* que esteja num dispositivo sem ligação à *Internet*.

Para este tipo de *wallet* o principal objetivo dos atacantes é aceder ao computador onde se encontra instalada a *desktop wallet*.

Para um atacante ter acesso à *desktop wallet* serão esquematizados na figura 3.6 os possíveis ataques numa árvore de ataque.

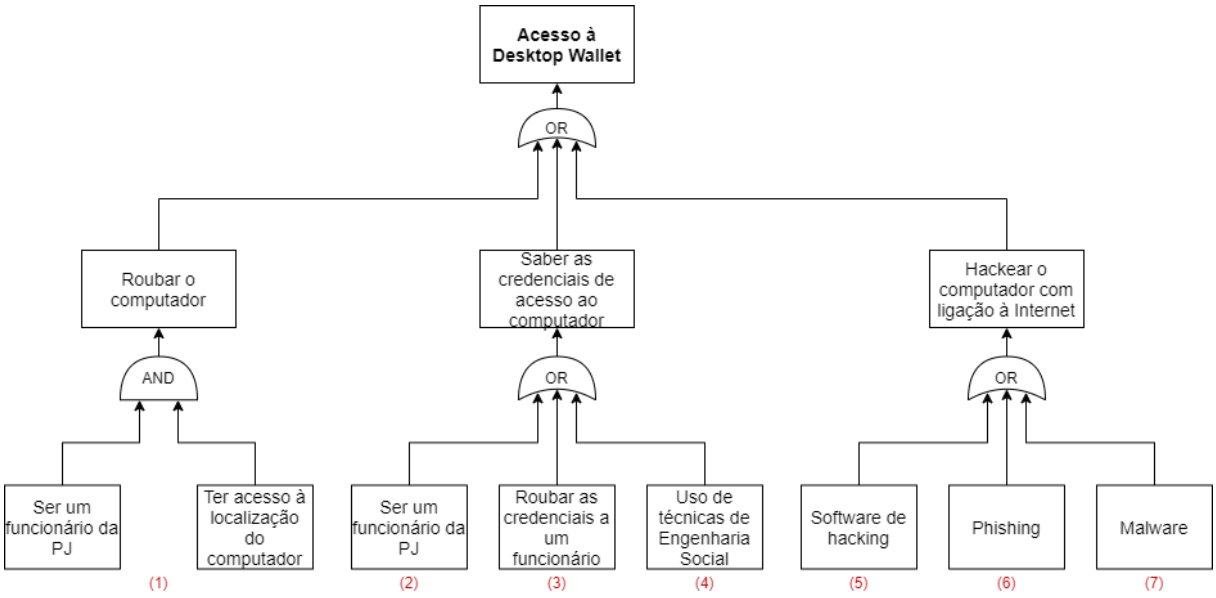

Figura 3.6: Árvore de Ataque ao Acesso à *Desktop Wallet*

Na *desktop wallet* existem tanto ameaças internas como ameaças externas à sua segurança. As três principais formas que podem levar ao acesso indevido à *desktop wallet*

são, por exemplo, o roubo do computador onde está instalada a *wallet*, um funcionário saber as credenciais de acesso ao computador e *hackear* o computador.

Tendo em conta estas três formas de aceder à *web wallet*, conseguiu-se através da árvore de ataque retirar sete possíveis ataques.

O primeiro ataque **(1)**, para aceder à *desktop wallet*, usou-se uma relação de *"AND",* ou seja, uma pessoa só consegue roubar o computador onde está a *desktop wallet* e consequentemente ter acesso à *wallet* se for um funcionário da PJ e souber a localização do computador. Se estas duas condições não forem cumpridas este ataque não se pode realizar.

A segunda forma de aceder à *desktop wallet* é ter conhecimento das credenciais de acesso ao computador onde a *wallet* está guardada. Para isto ocorrer existem três diferentes possibilidades. Usou-se neste caso uma relação de *"OR",* pois basta uma delas ser cumprida que são conhecidas as credenciais de acesso ao computador.

No segundo ataque **(2)**, se existir um funcionário fraudulento na organização e souber as credenciais de acesso ao computador, muito facilmente consegue aceder à *mobile wallet* e roubar as criptomoedas apreendidas. Neste caso estamos a falar da própria pessoa responsável pela *wallet*. Normalmente a pessoa responsável pelas *wallet*s nunca tenta prejudicar a organização, mas se existirem funcionários fraudulentos dentro da PJ esta pode ser um dos ataques possíveis para aceder à *wallet* e roubar as criptomoedas.

No terceiro ataque **(3)**, se um funcionário roubar as credencias de outro que tenha as credenciais de acesso ao computador, consegue aceder à *desktop wallet*. Pode-se verificar novamente que a ameaça principal deste ataque é a falsificação segundo a tabela de ameaças *STRIDE*.

No quarto ataque **(4)** há o uso de técnicas de Engenharia Social por parte de um funcionário para saber as credenciais de acesso de outro e consequentemente ter acesso ao computador onde está a *desktop wallet*. Neste ataque à *desktop wallet* a principal ameaça, segundo a tabela de ameaças *STRIDE*, é a divulgação de informação confidencial a pessoas não autorizadas.

Por fim, a terceira forma de aceder à *desktop wallet* é a realização de um ataque cibernético (*hack*) ao computador. Este ataque só acontece se o computador estiver ligado à *Internet*. Realizando este *hack* é possível ter acesso à *desktop wallet* se forem realizados os seguintes três ataques. Usou-se neste caso uma relação de *"OR"* porque não existe dependências entre nodos.

No quinto ataque **(5)** recorre-se ao uso de ferramentas de *hacking* para aceder ao computador (ligado à *Internet*) e consequentemente aceder à *desktop wallet*. Este tipo de ataque é extremamente difícil e requer muito investimento por parte do atacante.

No sexto ataque **(6)** recorre-se ao uso de técnicas de *phishing* para tentar obter acesso à *desktop wallet*.

E em relação ao sétimo ataque **(7)**, a organização pode ser alvo de um ataque de *malware* nos seus sistemas e este pode comprometer a segurança dos computadores da organização, que por sua vez afetam a segurança da *desktop wallet* que está instalada num desses computadores.

Na tabela 3.6 segue a análise dos ataques através dos parâmetros de avaliação das árvores de ataque selecionados para esta *wallet*.

Ataque	Dificuldade técnica do ataque	Probabilidade de sucesso do ataque	Custo do ataque
1	Baixa	Elevada	Baixo
2	Baixa	Elevada	Baixo
3	Baixa	Baixa	Baixo
4	Elevada	Baixa	Baixo
5	Elevada	Baixa	Elevado
6	Elevada	Baixa	Elevado
7	Elevada	Baixa	Elevado

Tabela 3.6: Avaliação dos Ataques à *Desktop Wallet* segundo os Parâmetros de Análise.

Na tabela 3.6 estão os sete possíveis ataques à *desktop wallet* e a respetiva classificação de cada parâmetro escolhido para a análise.

Nesta tabela visualiza-se que existem dois ataques identificados com cor cinzenta, isso significa que são os mais prováveis de acontecer e aqueles que poderão ter mais sucesso. São estes ataques que a PJ tem que ter em conta caso decida implementar a *desktop wallet* como mecanismo de armazenamento das criptomoedas confiscadas.

Nos dois primeiros ataques, **(1)** e **(2)**, estes só ocorrem se existirem na PJ funcionários fraudulentos. Mais uma vez, estes dois ataques têm baixa probabilidade de ocorrer na realidade se estiver tudo bem com os funcionários dentro e fora da empresa. Por exemplo, este tipo de situações pode ocorrer quando existem funcionários pouco confiáveis em posições hierárquicas de grande importância e por sua vez com acessos privilegiados.

Os ataques **(5) (6) (7)**, embora exijam muitos conhecimentos técnicos e tenham custos elevados de implementação, têm uma probabilidade de sucesso baixa. Significa assim que estes tipos de ataque não vão ocorrer tantas vezes como os outros dois, mas é necessário estar alerta e melhorar ao máximo as ferramentas corporativas de proteção contra este tipo de ameaças.

Este tipo de *wallet* tem muitas parecenças com a *mobile wallet*, pois em ambos os casos as *wallet* são guardadas em dispositivos de *hardware* com ligação à *Internet*, tornando-se assim mais suscetível a novas ameaças e ataques externos.

3.3.5. *Hardware Wallet*

A última opção para armazenar as criptomoedas confiscadas após uma investigação criminal são as *Hardware Wallet*s. Este tipo de *wallet* é uma das opções mais seguras para guardar qualquer tipo de criptomoedas, pois guarda as chaves privadas em dispositivos de *hardware* sem qualquer ligação direta à *Internet*, ou seja, não carece de qualquer tentativa de ataque externo via *Internet*.

Para os atacantes o principal objetivo é ter acesso às criptomoedas que estão dentro da *Hardware wallet*. Este tipo de *wallet* normalmente é guardada em *pen drives* ou em discos externos.

Para ter acesso à *hardware wallet* serão esquematizados na figura 3.7 os possíveis ataques numa árvore de ataque.

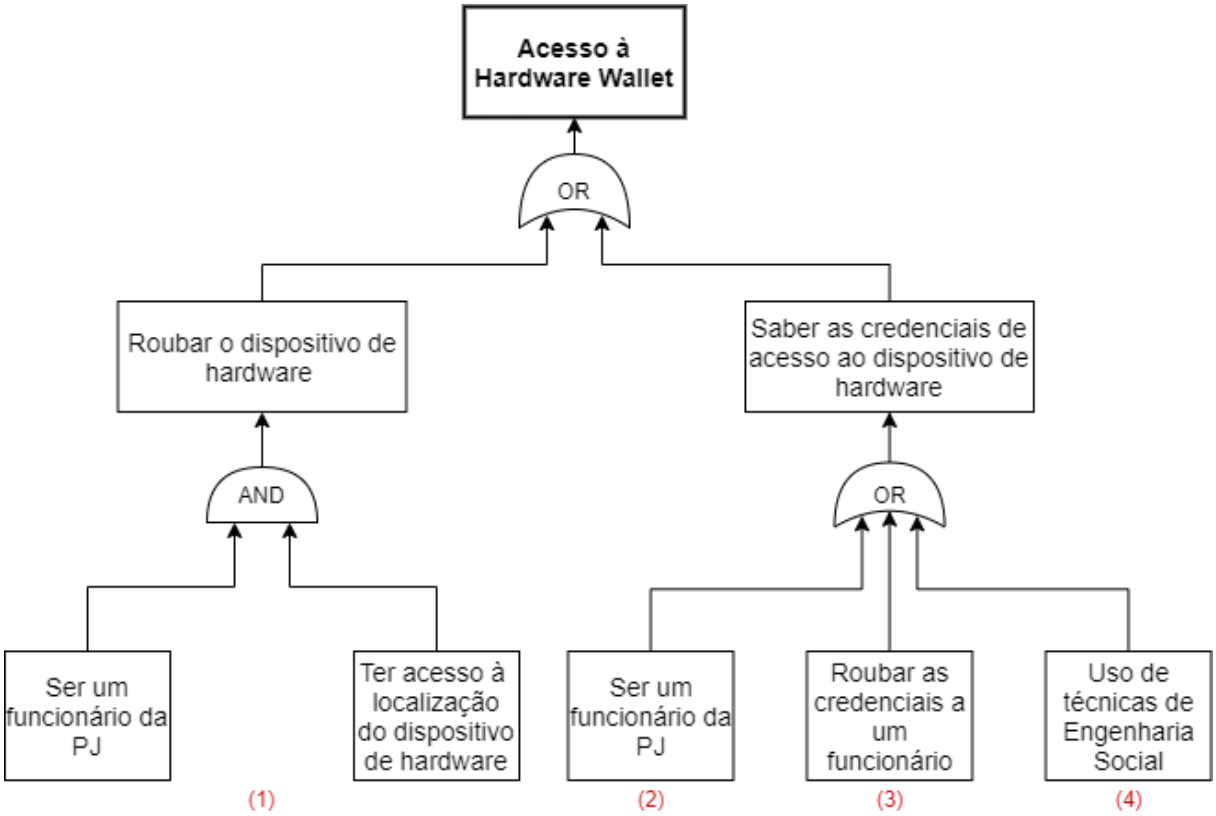

Figura 3.7: Árvore de Ataque ao Acesso à *Hardware Wallet*

Neste tipo de *wallet* as ameaças são apenas de caracter interno, isto é, a única possibilidade de aceder à *hardware wallet* é se o atacante for um funcionário da PJ.

Insatisfação com o trabalho ou rendimentos, pressões emocionais, mau estar familiar são tudo características que podem levar a que os funcionários desempenhem funções de forma incorreta e tentem prejudicar a organização.

Neste tipo de *wallet* existem duas formas de um atacante aceder à *hardware wallet* e roubar as criptomoedas que lá estão guardadas. Uma delas é roubar o dispositivo de *hardware* onde está esta *wallet* e a outra é obter as credenciais de acesso a esse dispositivo. Tendo em conta estas duas formas de aceder à *hardware wallet* conseguiu-se através da árvore de ataque retirar quatro possíveis ataques.

No primeiro ataque **(1)**, se existir um funcionário que tenha em mente atos maliciosos para com a organização e tiver acesso à localização do dispositivo de *hardware*, pode conseguir roubar o dispositivo e consequentemente aceder à *hardware wallet*. Neste ataque existe uma relação de *"AND",* porque uma pessoa apenas consegue roubar o dispositivo de *hardware* se for funcionário e também ter conhecimento de onde fica guardado o dispositivo nas instalações da PJ, caso contrário é impossível a realização deste ataque.

A segunda forma de aceder à *hardware wallet* é saber as credenciais de acesso ao dispositivo de *hardware* onde esta está guardada, para isto acontecer existem três diferentes possibilidades. Usou-se neste caso uma relação de *"OR",* pois basta que uma delas seja cumprida que são logo conhecidas as credenciais de acesso ao dispositivo de *hardware*.

No segundo ataque **(2)** se existir um funcionário que tenha em mente atos maliciosos na organização e souber as credenciais de acesso do dispositivo de *hardware* facilmente consegue aceder à *hardware wallet*.

No terceiro ataque **(3)** se um funcionário roubar as credencias de outro que tenha as credenciais de acesso ao dispositivo de *hardware* consegue aceder à *hardware wallet*. Neste ataque pode-se concluir, mais uma vez, segundo a tabela de ameaças *STRIDE*, que a falsificação é a principal ameaça.

E finalmente no quarto ataque **(4)** há o uso de técnicas de Engenharia Social por parte de um funcionário para ter conhecimento das credenciais de acesso de outro e consequentemente ter acesso à *hardware wallet*.

Nota: as *hardware wallet*s são protegias com um fator de autenticação em que apenas os funcionários com permissões podem aceder-lhe.

Segue-se na tabela 3.7 a análise dos ataques através dos parâmetros de avaliação das árvores de ataque selecionados para esta *wallet*.

Ataque	Dificuldade técnica do ataque	Probabilidade de sucesso do ataque	Custo do ataque
1	Baixa	Elevada	Baixo
2	Baixa	Elevada	Baixo
3	Baixa	Baixa	Baixo
4	Elevada	Baixa	Baixo

Tabela 3.7: Avaliação dos Ataques à *Hardware Wallet* segundo os Parâmetros de Análise.

Na tabela 3.7 estão identificados os quatro ataques que podem comprometer a *hardware wallet* e a respetiva classificação dos três parâmetros escolhidos para analisar cada tipo de ataque. Na tabela os ataques **(1)** e **(2)** estão selecionados com outra cor, porque são os ataques com uma dificuldade técnica baixa e com uma elevada probabilidade de sucesso, logo são estes tipos de ataque que a PJ tem que se preocupar se implementar a *hardware wallet* como mecanismo de armazenamento das criptomoedas.

De realçar mais uma vez que este tipo de ataque apenas se realiza se existirem funcionários fraudulentos dentro das instalações da PJ.

As ameaças à *hardware wallet* são muito semelhantes às da *paper wallet*s, pois ambas são guardadas em mecanismos que não estão ligados da *Internet*. Esta característica torna este tipo de *wallet* muito mais apelativo em termos de segurança das criptomoedas. A *hardware wallet* apenas está sujeita a ameaças internas (funcionários fraudulentos) e estas podem ser controladas pela PJ. Isto faz com que sejam uma ótima escolha para armazenar as criptomoedas confiscadas pela PJ após investigações criminais.

Capítulo 4

4. Secret Sharing na Segurança do Armazenamento de Criptomoedas

O grande objetivo desta secção do trabalho é fazer com que as chaves que dão acesso às criptomoedas não fiquem sob o controlo de uma pessoa única, pois ao contrário de outras apreensões de dinheiro, ouro, prata, jóias, droga, etc., o valor não está no objeto apreendido, mas sim nos dados. O problema que se coloca aqui é que estes dados são triviais de copiar e consequentemente suscetíveis a roubar. Se alguma pessoa fraudulenta deitar as mãos nestes dados, consegue roubar o valor total de criptomoedas apreendidas.

O facto de a chave privada estar sob o controlo de uma pessoa pode levar à perda total do valor de criptomoedas, em caso de destruição da chave, falecimento da pessoa responsável e inexistência de *backups* dos dados.

Em seguimento, teve-se a seguinte ideia, dividir a chave que dá acesso às criptomoedas por um número de *shares* e por um número de participantes (conceito de *Secret Sharing*) de modo a não deixar esta chave sob o controlo de uma pessoa apenas. Isto significa que se torna mais difícil alguém com atividades ilícitas em mente aceder às criptomoedas. Contribuindo assim para uma melhoria significativa dos níveis de segurança das criptomoedas apreendidas.

Tendo e conta este desafio nesta secção do trabalho será elaborado um modelo processual e operacional para o processo de armazenamento de criptomoedas em *wallets* porá a PJ, aplicando conceitos do modelo de Secret *Sharing* de *Shamir* com uma estrutura hierárquica de cargos da PJ. O objetivo desde modelo é melhorar os níveis confidencialidade, integridade e disponibilidade dos dados do processo de armazenamento de criptomoedas.

O *Secret Sharing*, como já foi referido, é um método criptográfico em que um segredo (dados) é distribuído por um *dealer* a um determinado número de participantes. Os dados resultantes são designados *shares* ou partes. Apenas é possível reconstruir o segredo quando são reunidos o número de *shares* necessários para esta reconstrução. Os restantes participantes deste grupo que não estiveram integrados no processo de reconstrução do segredo, não tem qualquer conhecimento do segredo. Estando os *shares* reunidos, o segredo é reconstruído e o acesso à informação é permitido.

No Modelo de *Secret Sharing* de *Shamir* é definido um número de participantes *n* e um número mínimo de *shares k* necessários para a reconstrução de um segredo *s*. Utilizando este conceito de *Secret Sharing* e aplicando a uma organização com uma estrutura hierárquica bem organizada é possível melhorar os níveis de segurança da informação em atividades de elevada importância. Neste caso a atividade de elevada importância é o armazenamento das criptomoedas em *wallets* na sede da PJ.

Após uma investigação da PJ que envolva a apreensão de criptomoedas (fruto de atos maliciosos e criminais) estar terminada é necessário armazenar as mesmas em *wallets*.

Para um maior nível de segurança da informação no armazenamento das criptomoedas nas *wallets* propôs-se o seguinte modelo.

4.1. Modelo

Neste modelo será distribuída pelo *dealer* partes de uma chave privada de uma *wallet* que armazena as criptomoedas. No presente modelo, o *dealer* são os inspetores responsáveis pelas investigações criminais relacionadas com as criptomoedas. A principal tarefa destes inspetores, para além da conclusão da investigação e do respetivo armazenamento das criptomoedas em segurança é não deixar que nenhum funcionário da PJ tenha acesso não autorizado à *wallet* onde estão as criptomoedas. Neste modelo eles distribuem partes de uma chave privada por apenas aquelas pessoas que necessitam mesmo de acesso à informação que está dentro das *wallets*.

A distribuição e reconstrução desta chave privada é feita através de uma estrutura hierárquica. A distribuição do segredo será realizada utilizando um número *k* de *shares* e um número *n* de participantes definidos pelos responsáveis de captura das criptomoedas. Estes valores de *k* e *n* podem variar conforme a criticidade da informação presente nas *wallets*, isto é, o segredo.

Neste caso dar-se-á um exemplo de uma possível implementação deste modelo com todas as regras e operações necessárias para a segurança da informação das chaves privadas durante este processo.

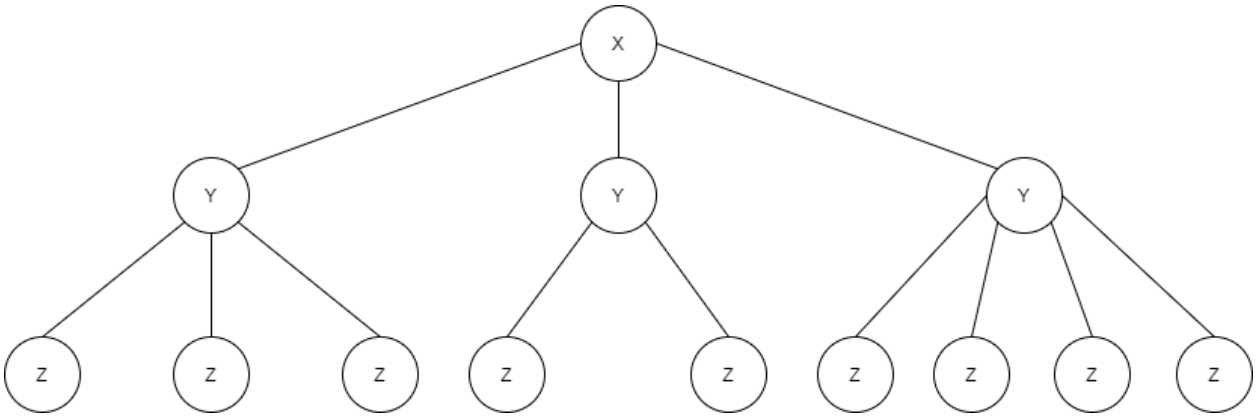

Figura 4.1: Proposta do Modelo com uma Possível Estrutura Hierárquica para a PJ.

Nesta proposta de modelo pode-se constar três níveis hierárquicos (X, Y, Z), sendo que o X é o nível mais alto na hierarquia onde estão incluídos todos os órgãos da direção da PJ, Y o nível intermédio na hierarquia, onde estão incluídas todas as unidades da PJ e Z o nível mais baixo, onde estão incluídas todas as subunidades ou equipas da PJ. Nesta proposta do modelo apenas estão visíveis três níveis hierárquicos, mas podem ser acrescentados novos níveis e novos participantes, depende de organização para organização. Neste caso propôs-se três níveis tendo em conta o organograma da PJ.

O segredo é distribuído pelos inspetores responsáveis da investigação e captura das criptomoedas por um determinado número *k* de *shares* correspondente a um número *n* de participantes. Os *shares* neste modelo podem ser dispositivos eletrónicos como por exemplo: computadores, *pen drives*, discos externos, entre outros. Podem ser também em formato papel, guardado em segurança por cada participante ou até mesmo memorizado na cabeça.

O objetivo dos *shares* é que os participantes tenham guardado cada pedaço do segredo em segurança e que o *share* de cada participante não possa ser corrompido por qualquer fator externo ao mesmo. Quando for necessário realizar uma reconstrução do segredo, para ter acesso à informação, o participante deve estar presente e na posse do seu *share* para este processo ser possível.

4.2. Instanciação do Modelo e Boas Práticas

De seguida vão ser apresentada todas as regras e boas práticas para o bom funcionamento deste modelo. O objetivo destas regras é tornar o modelo versátil a todas as organizações que façam este tipo de apreensões e garantir que os dados estão salvaguardados na ocorrência de algum ato malicioso interno ou externo.

1. Nesta primeira regra, **nenhum funcionário** consegue reconstruir o **segredo sozinho**. A criação desta regra vem ao encontro do objetivo principal deste capítulo do trabalho, que é o facto de não deixar a chave de acesso às criptomoedas sob o controlo de uma pessoa ou funcionário. Não deixar nenhum funcionário sozinho reconstruir o segredo, significa que são minimizados os casos em que um funcionário tem em mente a prática de atividades ilícitas e as violações da segurança dos dispositivos ou área de trabalho do funcionário. Em caso de existir uma violação da segurança as criptomoedas estão salvaguardadas com a utilização desta regra. Esta regra é válida para todos os níveis hierárquicos.

   Exemplo: um funcionário que esteja numas das equipas (Z) não consegue reconstruir o segredo sozinho.

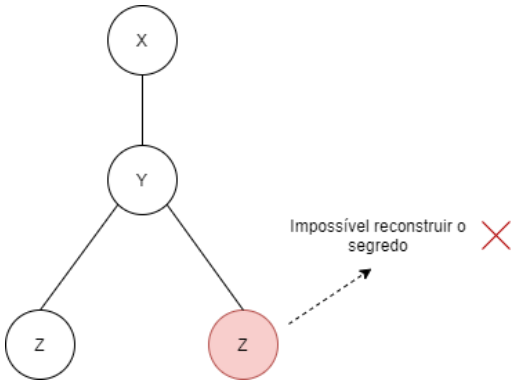

Figura 4.2: Exemplo 1 – Nenhum Funcionário Consegue Reconstruir o Segredo Sozinho.

2. Na segunda regra, são necessários pelo menos **dois funcionários** de **níveis hierárquicos diferentes** para reconstruir o segredo e consequentemente ter acesso à informação da *wallet*. Esta regra vem mais uma vez cumprir com o objetivo desta secção do trabalho (não permitir que a chave de acesso às criptomoedas esteja sob controlo de uma pessoa ou funcionário). Definiu-se que o segredo só pode ser reconstruído, quando estão envolvidos funcionários de níveis hierárquicos diferentes, para haver uma comunicação obrigatória entre os níveis e o segredo não ser reconstruído por uma direção, unidade ou equipa sozinha. Esta necessidade de comunicação com pelo menos outro nível hierárquico leva a que um funcionário *x* saiba o porquê da necessidade do funcionário *y* querer aceder às criptomoedas. Com esta regra, é criado uma espécie de controlo natural ao acesso às criptomoedas, ou seja, se um funcionário *x* perceber que não há necessidade alguma de o funcionário *y* aceder às criptomoedas, este pode reportar a situação à chefia e dar outra alternativa ou conselho ao funcionário *y* para prosseguir com as suas atividades. Aumentando assim os níveis de segurança das criptomoedas apreendidas pela PJ.

Exemplo: um funcionário da unidade Y e um funcionário da equipa Z conseguem reconstruir o segredo enquanto que dois funcionários das equipas Z não o conseguem reconstruir.

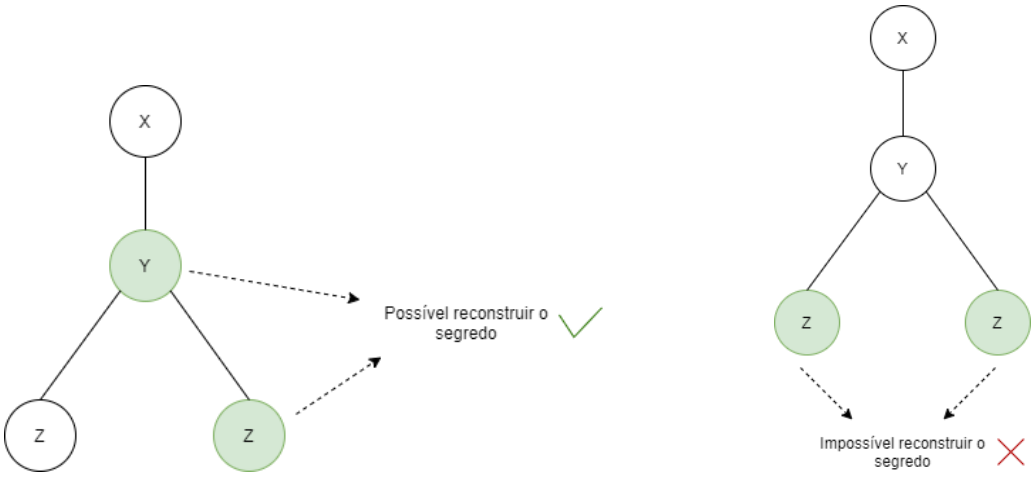

Figura 4.3: Exemplo 2 – Níveis Hierárquicos Diferentes vs Níveis Hierárquicos Iguais.

3. Nesta terceira e última regra, é necessário pelo menos **um funcionário** da subunidade ou **equipa responsável** pela captura e processo de armazenamento das criptomoedas para reconstruir o segredo. Esta regra existe para a equipa que realizou a apreensão saber o porquê de outras equipas, unidades ou direções quererem aceder às criptomoedas. Se a equipa responsável souber a razão pela qual outros funcionários querem aceder às criptomoedas, torna este processo muito mais seguro e à prova de atos maliciosos internos. É de realçar que nenhum funcionário de níveis hierárquicos altos conseguem aceder às criptomoedas sem a presença de um membro da equipa de apreensão das criptomoedas.

Exemplo: o funcionário da equipa Z mais à direita foi o responsável de uma investigação da PJ, isto significa que se não existirem mais funcionários envolvidos na investigação a reconstrução do segredo não vai ser possível sem a presença do funcionário da equipa Z.

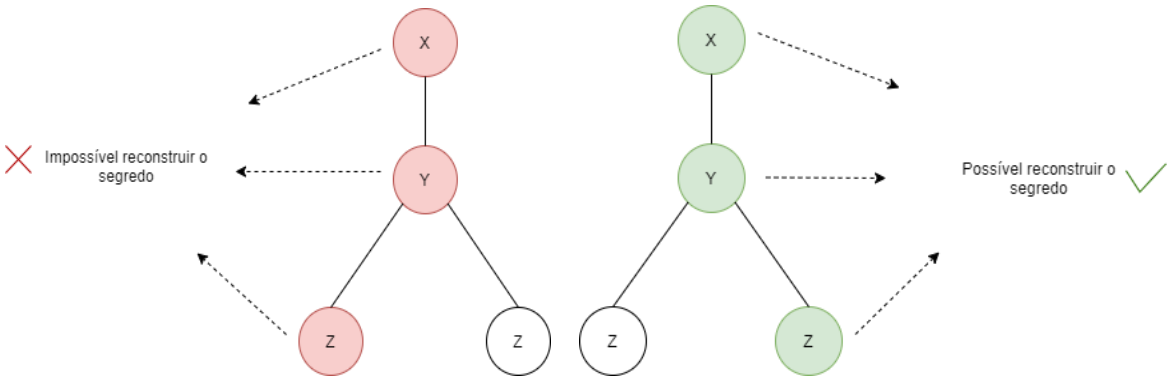

Figura 4.4: Exemplo 3 – Funcionário da Equipa Responsável pela Captura vs Funcionário Não Envolvido na Captura.

Este modelo hierárquico utiliza alguns conceitos de *Secret Sharing* de *Shamir*, nomeadamente, no que toca à definição do número de participantes *n*, número de *shares k* e na relação entre *n, k* e o processo de reconstrução do segredo. Com as regras acima descritas o modelo consegue oferecer uma contínua disponibilidade temporal dos dados, ou seja, qualquer um dos funcionários ao qual foi distribuído parte dos dados da chave, precisar e tiver razões para aceder às criptomoedas, esse acesso é concebido a qualquer altura (com a participação de um dos funcionários da equipa que realizou a apreensão das criptomoedas). Oferece também uma maior confidencialidade e integridade dos dados no processo de armazenamento das criptomoedas.

Em caso de existência de algum funcionário fraudulento, destruição ou corrupção de um *share* de um participante, existe um *backup* de toda a informação que cada funcionário tem. Este *backup* está na posse da equipa responsável pela captura das criptomoedas e só pode ser usado nestes casos em específico. Com este *backup* é a criada a redundância necessária para este modelo aumentar os níveis de segurança contra este tipo de situações.

Usando este modelo a PJ consegue aumentar os níveis de segurança da informação contra possíveis ataques, *malwares*, atos maliciosos, erros humanos e acessos indevidos aos seus sistemas e diminuir os efeitos secundários de uma possível violação de segurança interna ou externa.

Capítulo 5

5. Análise de Resultados e Conclusões

Neste capítulo vão ser analisados os resultados obtidos pelo método da análise de ameaças, que consiste na identificação das ameaças *STRIDE*, construção e classificação dos parâmetros de análise das árvores de ataque de cada tipo de *wallet* e vão ser retiradas conclusões de aplicabilidade do modelo baseado em conceitos de *Secret Sharing* apresentado no capítulo 4.

Em relação ao método de análise de ameaças, numa primeira fase foi desenhado o sistema, isto é, uma representação de como e onde podem ser armazenadas os diferentes tipos de *wallet* na sede da PJ. Numa segunda fase foram identificados todos os ativos e pontos de acesso do sistema, bem como alguns parâmetros referentes aos objetivos e motivações dos atacantes em violar a segurança do sistema. Na terceira e última fase foram identificadas as ameaças aos diferentes ativos e pontos de acesso do sistema e em seguida foram construídas árvores de ataque para cada tipo de *wallet*. Ainda dentro desta fase foram escolhidos parâmetros de análise das árvores de ataque para proceder à avaliação de qual dos tipos de *wallet* é a mais segura para a PJ implementar, sem correr o risco de ser atacada e lhes serem roubadas as criptomoedas apreendidas nas investigações criminais realizadas.

Na análise à *Paper Wallet* pode-se verificar quatro ataques possíveis à violação da sua segurança e consequente roubo das criptomoedas. Desses quatro ataques aquele que apresenta uma maior probabilidade de acontecer é o ataque número dois (ser um funcionário da PJ, ter as credenciais de acesso ao cofre e aceder à *paper wallet*), se e só se existirem funcionários fraudulentos dentro das instalações da PJ. Mas, transportando isto para factos reais, os quatro possíveis ataques identificados para este tipo de *wallet* são todos de carácter interno, ou seja, a PJ consegue controlar todos os fatores à volta para que estes tipos de ataque nunca aconteçam, caso obtém por implementar uma *paper wallet* para o armazenamento das criptomoedas apreendidas. Para a PJ este tipo de *wallet* é uma boa solução, pois para além de não estar ligada a qualquer dispositivo com ligação direta à *Internet*, apresenta menos ameaças e ataques do que os restantes tipos de *wallet*. A única com o mesmo número de ameaças e ataques é só mesmo a *hardware wallet* que será analisada mais à frente.

A *Mobile Wallet* consegue-se verificar a existência de sete possíveis ataques à violação da sua segurança. Desses sete apenas dois têm uma probabilidade de sucesso mais credível em relação aos restantes ataques. Estes dois ataques apresentam níveis baixos de dificuldade técnica e custos, sendo assim podem ser ataques mais recorrentes do que aqueles que envolvem mais conhecimentos técnicos e elevados valores monetários. Este tipo de *wallet* é uma das mais práticas, mas apresenta algumas vulnerabilidades quanto à segurança devido ao facto de estar num dispositivo com ligação direta à *Internet*. Estando num dispositivo desses o número de ameaças sobe como pode ser verificado na tabela de ameaças *STRIDE* e consequentemente o número de ataques também sobe, tornando este tipo de *wallet* menos seguro para o armazenamento das criptomoedas apreendidas.

Em relação à *Web Wallet*, existem sete possíveis ataques para aceder à *wallet* e consequentemente roubar as criptomoedas lá armazenadas. Dos setes possíveis tipos de ataque, os que apresentam maiores probabilidade de sucesso são o número três (roubar as credenciais a um funcionário para ter acesso ao computador onde está a *wallet*) e o número quatro (uso de técnicas de engenharia social para saber as credenciais de acesso ao computador onde está a *wallet*). O facto de neste tipo de *wallet* as chaves privadas serem armazenadas em servidores e o *software* da *wallet* estar num computador ou smartphone (ambos com ligação à *Internet*) leva a que o número de ameaças e ataques seja mais elevado, como pode ser verificado na tabela de ameaças *STRIDE* e na árvore de ataque da *web wallet*. Este tipo de *wallet* é muito parecido com as *mobile wallet* e *desktop wallet*, a única diferença é que as chaves privadas são armazenadas nos servidores da organização. Se o servidor for comprometido todas as criptomoedas guardadas nas *wallets* podem estar em perigo. Esta *wallet* é muito prática no dia a dia, mas a nível de segurança é pouco segura, devido ao facto de estar em dispositivos com ligação direta à I*nternet* e as chaves privadas estarem armazenadas em servidores sob o controlo de outras pessoas que não os utilizadores. Olhando para estes resultados e características a web wallet não é uma boa solução para a PJ armazenas as criptomoedas apreendidas nas suas investigações.

A *Desktop Wallet* funciona basicamente como a *mobile wallet*, só que em vez de *wallet* estar num *smartphone* está num computador. Verificando na árvore de ataque está *wallet* está suscetível a sete possíveis ataques, destes apenas dois têm boas probabilidades de sucesso que é no caso em que o computador com a *wallet* lá instalada é roubado e no caso que um funcionário com as credenciais de acesso ao computador acede à *wallet* e retira todos os seus fundos. De realçar que estes dois ataques têm maiores probabilidades de acontecer quando existem funcionários fraudulentos dentro das instalações da PJ. Este tipo de *wallet* é prática, mas mais uma vez apresenta vulnerabilidades no que toca a segurança. O facto de esta estar instalada num computador com ligação à *Internet* faz com que tenha mais ameaças e consequentemente um maior número de possíveis ataques à sua segurança (verificado na

tabela de ameaças *STRIDE* e na árvore de ataque correspondente). Tendo em conta as informações anteriores, a *desktop wallet* não é uma boa solução para a PJ guardar as criptomoedas apreendidas, fruto de atos ilícitos.

Por fim na *Hardware Wallet* é verificado a existência de quatro possíveis ataques à segurança da *wallet*. Desses quatro ataques apenas dois apresentam uma maior probabilidade de se materializar, é o caso do ataque número um (ser um funcionário da PJ, saber a localização do dispositivo de *hardware* e roubar o dispositivo) e do ataque número dois (ser um funcionário da PJ, saber as credenciais de acesso ao dispositivo de *hardware* e aceder à *hardware wallet*). Estes dois ataques são mais recorrentes se e só se existirem funcionários fraudulentos dentro das instalações da PJ. O número de ameaças e ataques é menor do que as *wallets* com ligações à *Internet*, como pode ser verificado na tabela de ameaça *STRIDE* e na respetiva árvore de ataque. Menos ameaças e menos possíveis ataques revela que esta wallet em termos de segurança é uma boa solução para a PJ. Este tipo de wallet, dentro da categoria das *cold wallets*, é uma boa solução para guardar grandes valores monetários durante longos períodos de tempo. E é isso mesmo que a PJ precisa, de um mecanismo seguro que não tenha qualquer tipo de ligação à *Internet* e que permita armazenar as criptomoedas apreendidas durante muito tempo ou até definirem alguma utilidade para estas.

Em suma, dos cinco tipos de *wallets* analisados neste trabalho, a *Hardware Wallet* em termos de segurança das criptomoedas é a melhor opção para a PJ armazenar as criptomoedas apreendidas após as investigações.

Em relação ao modelo baseado em conceitos de *Secret Sharing*, muitas vezes ativos de elevada importância para uma organização, como é o caso das criptomoedas, encontram-se sob a responsabilidade de uma pessoa apenas. Esta não é uma boa estratégia para preservar a segurança da informação dentro de uma organização. Se este modelo for implementado, significa que os dados estão distribuídos apenas pelas pessoas que precisam de saber ou precisam dela para trabalhar, e que na ausência de uma dessas pessoas é possível ter acesso a essa informação. Evitando desta forma que possíveis funcionários fraudulentos corrompam a informação ou tenham acesso a informação não autorizada.

Este modelo é dado no caso de a PJ quiser aumentar os seus níveis de segurança da informação em relação ao processo de armazenamento das criptomoedas apreendidas.

Se este modelo for aplicado, em conjunto com a utilização da *hardware wallet* para armazenar as chaves privadas, as criptomoedas estarão mais seguras contra possíveis ataques ou atos maliciosos dentro da PJ.

Imaginando que a PJ opta pela utilização de *hardware wallets* para o armazenamento das chaves privadas que consequentemente dão acesso às criptomoedas apreendidas. Para além das criptomoedas estarem protegidas contra os ataques via *Internet*, com a aplicação

deste modelo passam também a estar mais seguras contra os ataques de funcionários de dentro da PJ, tornando o processo de armazenamento de criptomoedas mais seguro.

Com a aplicação do *Secret Sharing* neste modelo, os *shares* (pedaços de dados da chave privada) dos funcionários, distribuídos pelos inspetores responsáveis pelas investigações criminais envolvendo criptomoedas, estão mais protegidos. Apenas é possível aceder à informação quando são reunidas todas as condições para tal, ou seja, o número de *shares* necessários, respeitando as regras hierárquicas impostas pelo modelo. Esta é uma possibilidade de implementação do *Secret Sharing* numa *hardware wallet* para melhoria da segurança no processo de armazenamento de criptomoedas por parte da PJ.

5.1. Trabalho Futuro

O trabalho futuro desta dissertação, passa por comunicar à PJ a análise em relação à segurança dos diferentes tipos de *wallets* usados para armazenar criptomoedas, e a proposta do modelo baseado no *Secret Sharing* para melhoria do processo de armazenamento de criptomoedas apreendidas pela PJ. Para além da apresentação da análise e do modelo, poderá ser perguntado à equipa responsável pelas investigações criminais envolvendo criptomoedas quais são os tipos de wallets que mais usam, e quais são os métodos ou boas práticas que usam para as manterem seguras. Com o objetivo de fazer com que os responsáveis desta área da PJ tenham conhecimento de que a implementação de *hardware wallets* é uma mais valia em termos da segurança das criptomoedas para a organização.

Capítulo 6

6. Referências

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. ResearchGate.

[2] Gennaro, R., Goldfeder, S. & Narayanan, A. (2016). Threshold-optimal DSA/ECDSA signatures and an application to Bitcoin wallet security. International Conference on Applied Cryptography and Network Security, pages 156-174.

[3] Gentilal, M., Martins, P. & Sousa, L. (2017). TrustZone-backed Bitcoin Wallet. Proceedings of the Fourth Workshop on Cryptography and Security in Computing Systems pages 25-28.

[4] Extance, A. (2015). The future of cryptocurrencies: Bitcoin and beyond. Nature, Vol. 526, Issue 7571.

[5] Peck, M. E. (2017). Blockchains: How They Work and why they'll Change the World. IEEE Spectrum Vol. 54, Issue 10.

[6] Li, X., Chen, T., Luo, X. & Yu, J. (2020). Characterizing Erasable Accounts in Ethereum. The Information Security Conference (ISC), pages 352-371.

[7] Goundar, S. (2020). Introduction to Blockchains and Cryptocurrencies. Blockchain Technologies, Applications and Cryptocurrencies, pages ix-xix.

[8] Simonite, T. (2011). What Bitcoin Is, and Why It Matters. MIT Technology Review. Disponível em: https://www.technologyreview.com/2011/05/25/194486/what-bitcoin-is-and-why-it-matters/

[9] Huber, T. A., Sornette, D. (2020) Boom, Bust, and Bitcoin: Bitcoin –Bubbles as Innovation Accelerators. Swiss Finance Institute Research Paper No. 20-41.

[10] Brunton, F. (2019). Digital Cash: The Unknown History of the Anarchists, Utopians, and Technologists Who Created Cryptocurrency. Princeton University Press.

[11] *Cointelegraph*. What is Cryptocurrency. Guide for Beginners. Disponível em: https: //cointelegraph.com/bitcoin-for-beginners/what-are-cryptocurrencies.

[12] *Cointelegraph*. What is Bitcoin? History, characteristics, pros and cons. Disponível em: https://cointelegraph.com/bitcoin-for-beginners/what-is-bitcoin.

[13] *Cointelegraph*. Bitcoin Wallets for Beginners: Everything You Need to Know. Disponível em: https://cointelegraph.com/bitcoin-for-beginners/what-is-bitcoin-wallets.

[14] Das, P., Faust, S. & Loss, J. (2019). A Formal Treatment of Deterministic Wallets. The 2019 ACM SIGSAC Conference on Computer and Communications Security, pages 651-668.

[15] Arapinis, M., Gkaniatsou, A., Karakostas, D. & Kiayias A. (2019). A Formal Treatment of Hardware Wallets. University of Edinburgh. International Conference on Financial Cryptography and Data Security, pages 426-445.

[16] Vijai, C. (2019). Mobile Wallet and Its Future in India. JETIR, Vol. 6, Issue 5.

[17] Chakravaram, V., Ratnakaram, S., Agasha, E. & Vihari, S. (2020). Cryptocurrency: Threat or Opportunity. ICCCE 2020, pages 747-754.

[18] Ciaian, P., Rajcaniova, M. & Kans, D. (2016). The economics of Bitcoin price formation. Applied Economics, pages 1799-1815.

[19] Presidência do Conselho de Ministros, “Decreto-Lei n.º 137/2019”, Diário da República, setembro, 2019.

[20] Marback, A., Do H., He K., Kondamarri S., Xu D. (2009). Security Test Generation using Threat Trees. ICSE Workshop on Automation of Software Test, pages 62-69.

[21] Myagmar, S., Lee A. J., Yurcik W. (2005). Threat Modeling as a Basis for Security Requirements. Symposium on Requirements Engineering for Information Security (SREIS), Vol.2005, pages 1-8.

[22] Stango, A., Prasad, N. R., & Kyriazanos, D.M. (2009). A Threat Analysis Methodology for Security Evaluation and Enhancement Planning. In third International Conference on Emerging Security Information, Systems and Technologies, pages 262-267.

[23] Kohnfelder, L., Garg, P. (1999). The threats to our products. In Microsoft Interface. Microsoft Corporation.

[24] Shostack, A. (2014). Threat Modeling: Designing for Security. John Wiley & Sons: Hoboken, NJ, USA.

[25] Simonjan, J., Taurer S., & Dieber, B. (2020). A Generalized Threat Model for Visual Sensor Networks. Sensors, Vol. 20.

[26] Schneier, B. (1999). Attack Trees. Dr. Dobb's Journal. Disponível em: http://macs.citadel.edu/baniks/427/Homework/attacktrees.pdf

[27] Moore, P. A., Ellison, J. R., & Linger, C. R. (2001). Attack Modeling for Information Security and Survivability. Disponível em: https://apps.dtic.mil/dtic/tr/fulltext/u2/a388771.pdf

[28] Schneier, B. (2000). Secrets and Lies: Digital Security in a Networked Word. John Wiley & Sons.

[29] Shostack, A. (2008). Experiences Threat Modeling at Microsoft. Microsoft. Disponível em: http://ftp.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-413/paper12.pdf

[30] Opel, A. (2005). Design and Implementation of a Support Tool for Attack Trees. Department of Mathematics and Computer Science, Otto-von-Guericke University. Disponível em: https://www.toengel.net/internship/data/report.pdf

[31] Mallick, PK. (2020). Risk Management. Disponível em: https://www.researchgate.net/publication/344737720_RISK_MANAGEMENT

[32] Komargodki I., Naor M., Yogev E. (2016). How to Share a Secret, Infinitely. In Theory of Cryptography - 14th International Conference, pages 485-514.

[33] Beimel A. (1996). Secure Schemes for Secret Sharing and Key Distribution. Israel Institute of Technology. Disponível em: https://www.cs.bgu.ac.il/~beimel/Papers/thesis.pdf

[34] Shamir A. (1979). How to Share a Secret. Communications of the ACM, Vol.22, pages 612-613. Disponível em: https://dl.acm.org/doi/abs/10.1145/359168.359176

[35] Blakley, G. R. (1979). Safeguarding cryptographic keys. International Workshop on Managing Requirements Knowledge, pages 313–318. Disponível em: https://ieeexplore.ieee.org /abstract/document/8817296

[36] Dolev S., ElDefrawy K., Lampkins J., Ostrovsky R. & Yung M. (2016). Proactive Secret Sharing with a Dishonest Majority. 10th Conference on Security and Cryptography for Networks (SCN'16), pages 529-548.

[37] Standler M. (2001). Publicly Verifiable Secret Sharing. International conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology – EUROCRYPT'96, pages 190-199.

[38] Kingsley P. K., Hyunsung K. (2019). Linear (t,n) Secret Sharing Scheme with Reduced Number of Polynomials. Security and Communication Networks, Vol. 2019, ID 5134534. Disponível em: https://www.hindawi.com/journals/scn/2019/5134534/

[39] Harn L., Hsu C-F. (2017). (t,n) Multi_Secret Scheme Based on Bivariate Polynomial. Wireless Personal Communications, Vol. 95, pages 1495-1504.

[40] Harn L., Hsu C.-F., Xia Z., Zhou J. (2017). How to Share Secret Efficiently over Networks. Security and Communication Networks, Vol. 2017, ID 5437403.

[41] Orcutt, M. (2020). How the North Korean hackers behind WannaCry got away with a stunning crypto-heist. MIT Technology Review. Disponível em: https://www.technologyreview .com/2020/01/24/276082/lazarus-group-dragonex-chainalysis/

[42] Saul, J. (2019). New Zealand Crypto Firm Hacked to Death, Seeks U.S. Bankruptcy. Bloomberg Law. Disponível em: https://news.bloomberglaw.com/bankruptcy-law/new-zealand - crypto-firm-hacked-to-death-seeks-u-s-bankruptcy