Universidade de Aveiro
Mestrado em Cibersegurança | Mestrado de Engenharia Informática
Código: 44153 - Segurança e Gestão de Risco
Docente responsável: Luís Miguel de Noronha Pessoa de Amorim

Relatório Pós-FRAAP
Grupo E

Thursday 13th June, 2024

Ricardo Covelo (102668) - Filipe Silveira (97981) - Telmo Sauce (104428)

Contents

1 Sumário executivo

1.1 Lista de Participantes

Equipa Responsável pela reunião FRAAP:

- Luís Amorim (Professor)
- Telmo Sauce (Aluno)
- Ricardo Covelo (Aluno)
- Filipe Silveira (Aluno)

Equipa da SCUBIC:

- Miguel Oliveira (COO)
- Carlos Oliveira (Senior Software Engineer)
- Dorin Bosii (Software Engineer)

1.2 Resumo do âmbito e princípios estabelecido

O primeiro passo na implementação da metodologia FRAAP foi a reunião Pré-FRAAP no dia 31/05/2024. Na reunião, foram discutidos os objetivos da empresa, as suas principais preocupações e os motivos para realizar a análise de risco. Aqui foram encontrados alguns riscos do sistema e informações básicas do fluxo de informação do sistema, tanto por explicação verbal quanto por apresentação de diagramas posteriormente. Além disso, a metodologia de classificação de riscos, os níveis de impacto e probabilidade, bem como um meio de comunicação entre os alunos e a pessoa responsável pela avaliação de risco, foram acordados.

A reunião FRAAP aconteceu no dia 07/06/2024 com o responsável da análise de risco assim como um responsável pelo backend do sistema. A reunião demorou à volta de 3 horas sendo acordado por todos que os alunos iriam posteriormente completar até dia 11 a avaliação dos riscos estimando a probabilidade e o impacto e estes iram ser aprovados/remodelados pelo responsável.

A produção deste relatório e análise de resultados é o resultado da terceira fase do processo FRAAP.

1.3 Resumo da metodologia

Para o desenvolvimento do nosso projeto, utilizamos a metodologia FRAAP (Facilitated Risk Analysis and Assessment Process) que assenta numa avaliação de risco eficiente, que se destaca

pela avaliação de um sistema/processo em termos de dias em vez de semanas ou meses. Esta metodologia assenta em 3 fases principais.

A fase de Pré-FRAAP tem como objetivo definir as bases de trabalho para a análise de risco. Nesta fase inicial, realizamos uma reunião inicial com os responsáveis de negócio, Miguel Oliveira e Carlos Oliveira, durante cerca de 1 hora e 30 minutos para definir o *scope* do projeto.

A fase do FRAAP envolve uma reunião, no máximo de 4 horas com a participação de uma equipa robusta da empresa constituída por Carlos Oliveira e Dorin Bosii. Durante a reunião, através de um *brainstorm*, são identificadas e avaliadas as ameaças, vulnerabilidades, impactos e controlos existentes.

A fase final, Pós-FRAAP, concentra-se na análise dos resultados das fases anteriores e a elaboração de um relatório final.

1.4 Resumo das principais conclusões da avaliação

Durante a avaliação os riscos que foram identificados como mais críticos foram:

- Intrusões externas, Reutilização de Passwords, Acesso por terceiros a dados ou recursos confidenciais.
  - Controlo: Uso de MFA e rotação de passwords.
- Resposta ineficiente a um incidente, Falta de um processo/politicas de resposta a incidentes, Incapacidade de Identificar e Mitigar Incidentes Rapidamente.
  - Controlo: Criação de um processo de resposta a incidentes
- Malware, Atacantes de Fishing, Má configurações de Router, Disrupção de Operações.
  - Controlo: Conta por staff na rede, redes separadas por Empresa.

Após a implementação destes controlos, estes riscos diminuem drasticamente, apesar de ainda serem riscos que requerem atenção.

1.5 Referenciação á restante documentação

Tabela de Riscos

1.6 Controlos a considerar e um plano de ação/prioritização

De forma a mitigar os riscos identificados nós aconselhamos a mitigar os riscos de maior nível e com controlos de mais fácil e rápida implementação assim mitigando as ameaças mais criticas. De forma a mitigar os riscos identificados os controlos que consideramos de maior importância são:

- Utilização de um IDS e IPS.
- Uso de um Antivírus.
- Uso de MFA e rotação de passwords.
- Sensibilização do Staff para ataques de social engineering.
- Organização do sistema de logs
- Criação de processos de resposta a incidentes e para report de bugs.
- Uso de ferramentas de SAST(SonarCloud) e DAST.

1.7 Conclusões

A análise de risco realizada permitiu nos identificar e avaliar os principais riscos que a organização continha.

O processo incluiu uma avaliação detalhada das ameaças e vulnerabilidades, assim como uma análise das probabilidades e do impacto potencial no serviço e na conformidade contratual.

Para alem disto foi possível identificar controlos para mitigar alguns dos riscos identificados.

Consideramos que nesta avaliação alcançamos os objetivos necessários determinados na Pré-FRAAP.

2 Metodologia

Para o nosso projeto, de acordo com as guias do trabalho, levamos a cabo a metodologia de FRAAP (Facilitated Risk Analysis and Assessment Process) de forma a realizar uma avaliação eficiente e detalhada dos riscos, identificando ameaças, vulnerabilidades e impactos, e propondo controlos e medidas de mitigação adequadas.

O FRAAP é constituído por **três** fases iniciais, descritas por:

2.1 Pré-FRAAP

A primeira reunião, Pré-FRAAP, decorreu a 31 de Maio de 2024, com uma duração próxima de 1 hora e 30 minutos, com o objetivo de definir o âmbito da avaliação, identificar os sistemas e processos a serem analisados e preparar a documentação necessária para a fase FRAAP propriamente dita.

Os participantes do reunião eram constituídos por:

- 3 Alunos (Ricardo Covelo, Telmo Sauce, Filipe Silveira)
- O professor Luís Amorim
- O Responsável da infraestrutura Carlos Oliveira
- O responsável do negócio Miguel Oliveira

No decorrer da reunião fomos explicando a metodologia FRAAP, o intuito da reunião e também os nossos objetivos a cumprir.

Durante a reunião iniciamos com uma breve introdução de todos presentes, uma *overview* do âmbito da SCUBIC e a sua história até ao momento. De seguida explicamos o processo de FRAAP, e concordamos na seguintes tabelas para definições de principio.

Nível	Probabilidade	Descrição	Valor
1	Muito Baixo	Muito Improvável que aconteça	< 1
2	Baixo	Não é provável que aconteça	1 a 2
3	Médio	Pode acontecer raras vezes	3 a 4
4	Alto	Pode acontecer algumas vezes	5 a 6
5	Muito Alto	Praticamente certo que irá acontecer, e vai repetir-se	> 7

Table 1: Níveis de Probabilidade

Nível	Impacto	Descrição do Impacto
1	Baixo	Reposição de serviço < 1h
2	Médio	Reposição de serviço < 4h
3	Alto	Reposição de serviço < 1 dia
4	Muito Alto	Reposição de serviço > 1 dia

Table 2: Impacto no Serviço

Nível	Impacto	Descrição do Impacto
1	Baixo	Falha pontual que pode comprometer o serviço
2	Médio	Falha repetida no cumprimento do serviço, sem penalização
3	Alto	Falha repetida no cumprimento do serviço, com penalização
4	Muito Alto	Falhas graves no cumprimento do serviço, com penalização e/ou que comprometam o contrato

Table 3: Impacto na Conformidade Contratual ou Legal

		Impacto			
		1	2	3	4
Probabilidade	1	1	2	3	4
	2	2	4	6	8
	3	3	6	9	12
	4	4	8	12	16
	5	5	10	15	20

Table 4: Matriz de Risco

	O risco é aceitável
	Não é obrigatório fazer o tratamento, mas deve ser analisado
	Devem ser encontradas medidas de mitigação

Table 5: Legenda dos Riscos

De seguida, foi realizada uma *review* das estratégias de negócio e objetivos propostos pela SCUBIC, com adição do *scope* do projeto e dependências impostas sob a empresa. Daqui aprendemos sobre a arquitetura onde a empresa assenta, as suas restrições atuais e as mudanças que estão a ocorrer de forma interna.

Desta forma, foi possível realizar uma triagem inicial da arquitetura atual, obter um diagrama geral da arquitetura atual para ser estudado posteriormente e , a partir de um Mini-Brainstorming, identificar ameaças e vulnerabilidades iniciais que serviram como ponto de partida da próxima reunião.

Finalmente concordamos os requisitos da próxima reunião, FRAAP , e também os participantes da mesma, bem como a sua data.

2.2 FRAAP

A segunda reunião, decorrida dia 07 de Junho de 2024, foi realizada com 5 membros sendo estes:

- 3 Alunos (Ricardo Covelo, Telmo Sauce, Filipe Silveira)
- O professor Luís Amorim

- O Responsável da infraestrutura Carlos Oliveira
- Responsável pelo Backend Dorin Bosii

Os membros da equipa começaram por esclarecer algumas dúvidas que os alunos ficaram sobre o sistema após a análise dos diagramas apresentados.

De seguida cada um dos membros citou algumas das vulnerabilidades e riscos que se foram lembrando durante o tempo entre as duas reuniões. Quando estes acabaram de expor os riscos identificados pelos mesmos, os alunos expuseram algumas vulnerabilidades comuns a muitas infraestruturas para verificar se se aplicavam à situação da empresa e se já tinham controlos implementados relativamente a essas vulnerabilidades.

Por último os 10 primeiros riscos identificados foram classificados em probabilidade e impacto pelos membros da SCUBIC, para que assim os alunos pudessem classificar o resto dos riscos sozinhos sendo que, os responsáveis iriam depois verificar os valores atribuídos.

De forma sucinta, conseguimos atingir os objetivos da nossa reunião de forma clara e identificamos vários riscos para os nossos resultados finais.

2.3 Pós-FRAAP

Na Terceira fase do FRAAP, foram debatidas as principais conclusões e desenvolvido o relatório atual com uma lista os riscos que a empresa deve ter em conta bem como os controlos mais importantes. Por fim foi desenvolvido uma plano de ação para tornar esta implementação o mais eficaz possível.

3 Avaliação de Risco

Como objetivo de projeto, a partir dos resultados das duas primeiras fases do FRAAP, desenvolvemos a nossa avaliação dos riscos presentes na SCUBIC.

Nas figuras abaixo pode se ver o risco antes e depois da implementação dos controlos sugeridos.

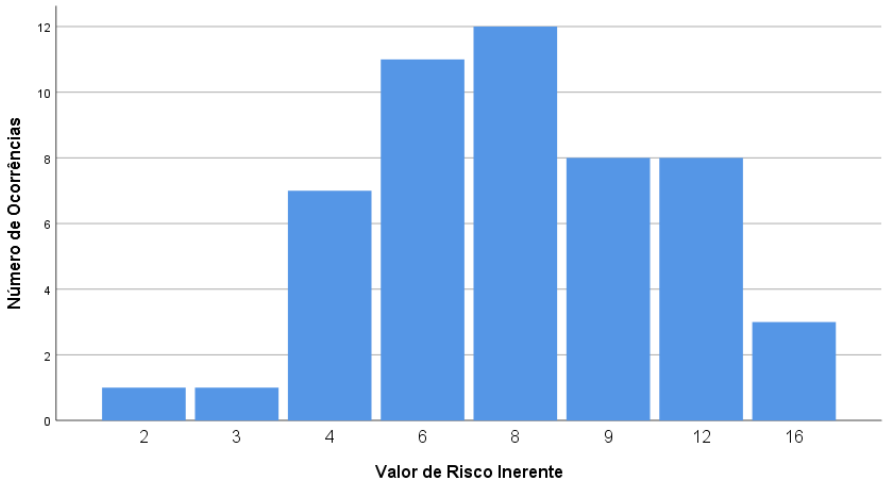

Figure 1: Risco antes do controlos sugeridos

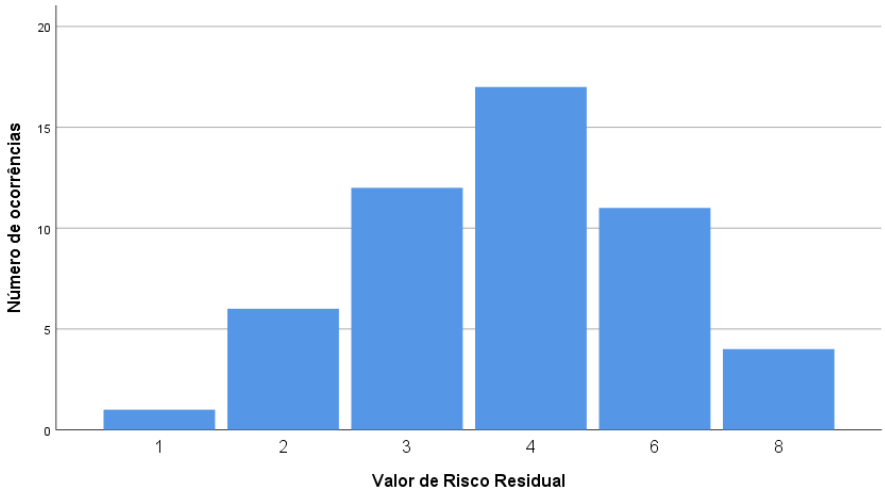

Figure 2: Risco depois do controlos sugeridos

A partir dos resultados, podemos concluir que existem até ao momento existem 3 Riscos graves e 31 riscos médios, sendo que a maior parte deles apenas se irá concretizar se um grupo organizado de hackers se focar na organização, e tendo em conta a maturidade e o tamanho da mesma seria pouco provável. Embora muitos deles sejam médios com um número tão grande

seria sensato mitigar alguns deles uma vez que uma combinação destas vulnerabilidades poderia dar uma oportunidade fácil de um ataque.

3.1 Riscos e Controlos

Apresentados abaixo encontramos os riscos médios e superiores encontrados na empresa e os controlos sugeridos para cada uma delas:

1. Vulnerabilidades associadas a versões antigas, Falta de controlo de versões de bibliotecas/frameworks, Injeção de código, Denial of Service, Acesso ao sistema
    - Control: Ferramenta de controlo de versões de livrarias, Ferramentas
2. Vulnerabilidades associadas a versões antigas, Falta de Controlo de versões dos sistemas, Breach do sistema
    - Controlo: Ferramenta de analise de versões
3. Roubo algoritmos, Access Control , Danos financeiros, Perda de credibilidade
    - Controlo: MFA, Auditorias de Segurança
4. Elevação de Privilégios, Ma configuração do Access Control da API, Acesso não Autorizado
    - Controlo: MFA(CC/SmartCards), JTW
5. Exposição de Serviços Internos a Ameaças Externas sem o conhecimento da empresa, Portos Abertos Desconhecidis (local), Exploração de vulnerabilidades, Exfiltração de Dados
    - Controlo: Auditoria
6. Malware, Atacantes de Fishing, Má configurações de Router, Disrupção de Operações
    - Controlo: Conta por staff na rede , redes separadas por Empresa
7. Atacante bruteforce autenticação, GitLab Autenticação insuficiente, Acesso não autorizado a recursos
    - Controlo: IDS, IPS
8. Atacante troca chave pública e fazer-se passar por alguém, Não Uso de Um Certifica e validação do mesmo, Roubo de Identidade
    - Controlo: Criação de um Certificado e validaçao do mesmo quando se usa a chave publica

9. Falha na Resposta Automatizada a Ameaças, Não prevenção de intrusões (LOCAL), Interrupção dos Serviços, DOS

    - Controlo: IPS

10. Falta de Monitoramento, Registro de Atividades Suspeitas e Incapacidade de Detectar Ataques, Falta de deteção de Intrusões (LOCAL), Atividades Suspeitas indetetaveis

    - Controlo: IDS

11. Falha na Resposta Automatizada a Ameaças, Não prevenção de intrusões (AWS), Interrupção dos Serviços, DOS

    - Controlo: IPS

12. Falta de Monitoramento, Registro de Atividades Suspeitas e Incapacidade de Detectar Ataques, Falta de deteção de Intrusões (AWS), Atividades Suspeitas indetetaveis

    - Controlo: IDS

13. Exposição a ataques externos, Nem Todos os serviços estão em subnets privadas (APIS subnet pub), DOS

    - Controlo: IPS, Firewall, criar subnet privada para servicos que não necessitam de estar numa subnet publica

14. Falha de backups, Perda de informação, Perda de dados, danos à reputação

    - Controlo: Check Regular de ficheiro de backups e mecanismos de recuperação

15. Download de malware malicioso, Falta de deteção de malware (Nas máquinas ubunto AWS), Perda de dados, DDOS, Acesso a dados

    - Controlo: Uso de um antivirus, Sensibilização do Staff para ataques como fishing

16. Obtenção de credenciais por pessoal não autorizado, Credenciais Hard-Coded (GItLab)-Terraform , Exfiltração de dados, perda de confidencialidade

    - Controlo: Utilização de AWS kms com criptografia

17. Utilizador com acesso a máquinas AWS ficar com keys indevidamente, Credencias Task Defenicion AWS, Acesso não autorizado a recursos, Disrupção de operações

    - Controlo: Uso de Tools como AWS Secrets Manager ou HashiCorp Vault

18. Atacante com acesso ao gitlab roubar as keys, Credenciais Hard-Coded da (AWS- no gitlab), Acesso não autorizado a recursos, Disrupção de operações

- Controlo: Uso de MFA para acesso ao gitlab, Uso de Vault para guardar AWS keys

19. Atacante com acesso ao gitlab roubar as keys, Credenciais nas Instâncias EC2 do SuperUser, Acesso não autorizado a recursos, Disrupção de operações

    - Controlo: Uso de Tools como AWS Secrets Manager ou HashiCorp Vault

20. Roubo de Chaves de Acesso, Fixed API Keys(Para Backend), Credentials stolen can be used Indefinitely causing unauthorized access

    - Controlo: Uso de JWT

21. Falha de deteção de anomalias , Sistema não organizado de logs, Não deteção de intrusões, falha de ativação de planos de disaster-recovery

    - Controlo: Organização do sistema de logs (uso de tags, e alertas)

22. Bugs no software, Falta de ferramentas de deteção de bugs, Software instavel e insatisfação do cliente

    - Controlo: Uso de ferramentas de SAST/DAST (SonarQube)

23. Desconhecimento de possíveis entry-points do sistema, Falta de listagem de vulnerabilidades previamente descobertas, Ataques por vulnerabilidades desconhecidas, Mau desaster recovery

    - Controlo: Diminuir nº de pontos de entrada de cada serviço

24. Resposta ineficiente a um incidente, Falta de um processo/politicas de resposta a incidentes, Incapacidade de Identificar e Mitigar Incidentes Rapidamente

    - Controlo: Criação de um processo de resposta a incidentes

25. Obtenção de informações do sistema por pessoal não autorizado, Elementos de debug presentes no código, Perda de credebilidade da instituição, Multas

    - Controlo: Uso de testes unitários e utilização de software como SonarCloud para bug sniffing

26. Intrusões externas, Reutilização de Passwords, Acesso por terceiros a dados ou recursos confidenciais

    - Controlo: Uso de MFA e rotação de passwords

27. Consumo de recursos excessivos, Envio de Dados sem restrições, Perda financeira, Consumo de recursos

- Controlo: Criação de alertas de consumo na AWS. Criação de limitações para o utilizador

28. Intrusões externas, Falta de alertas de down APIS/Services, Desconhecimento do não funcionamento do sistema

    - Controlo: Implementação de Healtchecks e Horizontal Scaling

29. Serviço de API indisponivel ao ser atualizado, Falta de redundância de Backend, Erro de funcionamento do produto.

    - Controlo: Implementação de blue green deployment

30. Intrusões externas e mau funcionamento do sistema, Falta de Testes Unitários para verificar o funcionamento correto do sistema, Erro de funcionamento do produto.

    - Controlo: Criação de testes unitários

31. Developers mal intencionados, Falta de verificação de packages do VScode, Exposição de código confidencial.

    - Controlo: Criação de uma whitelist de extenções para vsCode

4 Planeamento / Priorização

Para assegurar uma implementação dos controlos aconselhamos a seguir o seguinte plano.

- Identificação dos controlos sugeridos que são realisticamente implementáveis no âmbito da empresa.
- Identificar os controlos que já estão parcialmente implementados ou estão atualmente a implementar.
- Dos controlos escolhidos ordena-los por ordem de facilidade, rapidez e custos de implementação.
- Fazer uma lista com os controlos planeados de implementar, ordenando-os entre implementação em curto,médio e longo prazo.
- Implementação dos controlos na ordem listada.
- Teste e monitorização dos controlos implementados.
- Melhoria continua dos controlos com base nos resultados obtidos.

5 Conclusões

Com esta análise nos conseguimos compreender melhor como aplicar os métodos ensinados e perceber a eficácia dos mesmos.

Na nossa opinião tivemos resultados bastantes positivos, onde conseguimos identificar mais de 50 ameaças para a organização bem como controlos que diminuiriam drasticamente o risco destas mesma ameaças.

Este projeto poderia ter alcançado melhores resultados se na reunião de FRAAP houvesse uma equipa mais variada que pudesse apresentar objetivos tais como os clientes e shareholders.

Os engenheiros SCUBIC desempenharam um papel crucial na análise, facilitando o processo de obtenção de informações sobre a empresa. Identificando vulnerabilidades importantes, mas também sugeriram controlos eficazes tiveram um papel muito importante nesta avaliação. Mostraram se disponíveis ao longo de toda a avaliação para esclarecer qualquer dúvida ao longo da análise sobre o sistema e o seu funcionamento.