



IPBeja
INSTITUTO POLITÉCNICO
DE BEJA

INSTITUTO POLITÉCNICO DE BEJA
Escola Superior de Tecnologia e Gestão
Mestrado em Engenharia de Segurança Informática
Fundamentos de Cibersegurança

Trabalho Individual

Paulo António Tavares Abade - 23919



Beja, outubro de 2025

INSTITUTO POLITÉCNICO DE BEJA
Escola Superior de Tecnologia e Gestão
Mestrado em Engenharia de Segurança Informática
Fundamentos de Cibersegurança

Trabalho Individual

Paulo António Tavares Abade - 23919

Orientadores: Rui Silva & Rogério Bravo

Beja, outubro de 2025

Resumo

Resolução do trabalho

Keywords: cibersegurança

Abstract

Work Resolution

Keywords: cybersecurity

Índice

1 Grupo I - Professor Rui Silva	1
1.1 Pergunta - Apresentação de duas áreas do MITRE ATT&CK	1
1.1.1 Malware Protection	1
1.1.2 Incident Coordination	2
1.2 Pergunta - MITRE - Projeto de ATT&CK - Night Dragon	2
1.3 Pergunta - MITRE - Projeto ATT&CK - Tática de Initial Access	3
2 Grupo II - Professor Rogério Bravo	4
2.1 Pergunta - Os 4 Pilares da Cibersegurança	4
2.1.1 Tecnologias	4
2.1.2 Pessoas	4
2.1.3 Organizações	5
2.1.4 Segurança Física	5
2.1.5 O pilar na intervenção digital forense	5
2.2 As três dimensões da segurança da informação	6
2.2.1 Segurança Física	6
2.2.2 Segurança Lógica	6
2.2.3 Segurança Humana	6
2.3 O Conceito de Governança	7

Índice de Figuras

1 Grupo I - Professor Rui Silva

Nesta secção serão respondidas as questões do Grupo I, focando-se na áreas do MITRE ATT&CK lecionadas pelo professor Rui Silva.

1.1 Pergunta - Apresentação de duas áreas do MITRE ATT&CK

Em resposta à questão 1.1, foram escolhidas para apresentar as áreas de *Malware Protection* e *Incident Coordination*, que podem ser consideradas como mutualismo/simbiose, uma vez que ambas as áreas trabalham em conjunto para fortalecer a defesa contra ameaças. Caso uma ameaça seja detectada, pela área de *Malware Protection*, a área de *Incident Coordination* entra em ação para coordenar a resposta ao incidente, assegurando que as medidas adequadas sejam tomadas para mitigar o impacto da ameaça.

1.1.1 Malware Protection

A proteção contra malware envolve a implementação de medidas e tecnologias para prevenir, detectar e remover software malicioso que possa comprometer a segurança dos sistemas informáticos. No entanto, esta proteção não é infalível, podendo ser contornada por *malwares* que esteja camouflado ou que nunca tenha sido identificado, no caso do último, é conhecido como *Zero-Day Malware*. Esta proteção funciona através da análise de padrões comuns em ataques (CAPE), sendo que estes padrões foram identificados através do MAEC (Malware Attribute Enumeration and Characterization), que é um padrão para a representação de informações sobre malware, permitindo a troca estruturada de dados entre diferentes ferramentas e sistemas de segurança. O objetivo principal do MAEC é facilitar a detecção, análise e resposta a ameaças de malware, promovendo a interoperabilidade entre diferentes soluções de segurança. Este é utilizado pelo Incident Coordination para ajudar a prevenir novos ataques com base no que a proteção de malware não conseguiu impedir.

1.1.2 Incident Coordination

A coordenação de incidentes envolve a gestão e resposta a incidentes de segurança informática que não tenham sido superados pela proteção de malware, garantindo que as ameaças sejam tratadas de forma eficaz e eficiente. Isto inclui a identificação, análise, contenção, erradicação e recuperação de incidentes de segurança. A coordenação eficaz de incidentes é crucial para minimizar o impacto das ameaças e garantir a continuidade das operações. Integrando e correlacionando informação de multiplicas fontes estáticos e dinâmicas, mais conhecidamente como IODEF (Incident Object Description Exchange Format), que é um padrão para a troca estruturada de informações sobre incidentes de segurança informática, sendo que isto permite detetar com cada vez mais qualidade a presença de malware através da análise da sua assinatura. Isto fica automatizado com o RID (Realtime Inter-network Defense), que é um protocolo que permite a troca automática e segura de informações sobre ameaças. Existem ainda outros protocolos como o *TAXII* (Trusted Automated eXchange of Indicator Information) que é um protocolo para a troca automatizada de indicadores de ameaças, e o *STIX* (Structured Threat Information eXpression) que é uma linguagem padronizada para a representação de informações sobre ameaças cibernéticas, e estes são complementares sendo que o STIX é o formato que passa pelo TAXII para ser transmitido entre sistemas.

1.2 Pergunta - MITRE - Projeto de ATT&CK - Night Dragon

O projecto *Night Dragon* foi uma campanha de ciberespionagem que visou várias empresas de energia, petróleo e os seus derivados, sediadas no Cazaquistão, Taiwan, Grécia e Estados Unidos da América, e a campanha foi descoberta em novembro de 2009 pela McAfee. O objetivo principal desta campanha era roubar informações confidenciais e proprietárias relacionadas com a indústria de energia. Primeiramente, os atacantes compraram serviços para alojar os servidores que iriam controlar as vítimas e usavam os protocolos HTTP como meio de comunicação, pois estes ficavam disfarçados entre o tráfego legítimo. A partir de SQL Injection para obter os dados, era utilizado o software *Cain & Abel* para realizar ataques de brute-force para decifrar os hashes das palavras-passe dos administradores de sistemas, conseguindo assim aceder remotamente aos sistemas das vítimas, e com o *zwShell* implantado os atacantes podiam executar comandos remotamente.

Com isso, os atacantes começaram a obter ficheiros e outras informações sensíveis de sistemas comprometidos, enviando-os para os servidores que tinham sido comprados anteriormente.

Ainda utilizaram um RAT (Remote Access Trojan), usando os servidores afetados para fazer ataques a alvos internos através de e-mails de *spear-phishing* que continham anexos maliciosos que, quando abertos, instalavam o RAT nos sistemas das vítimas. O alvo principal desta parte do ataque eram portáteis que tinham contas de VPN e que permitiam obter ainda mais acesso aos sistemas internos. A estratégia baseava-se em usar ferramentas de roubo de palavras-passe e, ao entrar, deixar um RAT.

Após a investigação, a McAfee concluiu que o grupo responsável pelo *Night Dragon* tinha ligações à China, trabalhava entre as 9h e as 17h no horário de Pequim, e que o grupo tinha como alvo empresas específicas, sugerindo que a campanha era motivada por interesses económicos e estratégicos.

1.3 Pergunta - MITRE - Projeto ATT&CK - Tática de Initial Access

A tática de *Initial Access* tem o objetivo de conseguir o primeiro ponto de entrada numa rede e/ou alvo. Existem várias técnicas para alcançar este objetivo, sendo a mais conhecida o *Phishing/Spear-Phishing*, que envolve o envio de e-mails, SMS ou aplicações que aparecem ser legítimos, mas que contêm links ou anexos maliciosos. No caso do *Enterprise*, qualquer funcionário da empresa pode ser alvo deste tipo e-mails, enquanto que no *Mobile*, o alvo costuma ser o utilizador final e pode ser vítima através de SMS, aplicações ou chamadas telefónicas. Por fim, no *ICS*, o alvo vai ser o funcionário ou grupo de funcionários de uma organização que possua acesso a sistemas industriais, e estes podem ser vítimas através de e-mails ou chamadas telefónicas.

Existem diversas variantes de *Phishing/Spear-Phishing* porque cada ambiente tem as suas particularidades, e o atacante deve adaptar-se a cada um deles, maximizando as chances de sucesso para cada situação, onde cada alvo tem os seus próprios hábitos e rotinas.

2 Grupo II - Professor Rogério Bravo

Nesta secção serão respondidas as questões do Grupo II, focando-se na parte da teoria da cibersegurança, variando desde os pilares da cibersegurança, intervenção digital forense, os padrões *ISO 27000*, as três dimensões da cibersegurança, entre outros tópicos lecionados pelo professor Rogério Bravo.

2.1 Pergunta - Os 4 Pilares da Cibersegurança

Os quatro pilares da cibersegurança são as tecnologias, as pessoas, as organizações e a segurança física. Estes pilares sustentam a base em que as *ISO 27000* são construídas, e cada um deles desempenha um papel crucial na proteção dos sistemas informáticos e dos dados contra ameaças cibernéticas.

2.1.1 Tecnologias

As tecnologias referem-se às ferramentas, softwares e infraestruturas utilizadas para proteger os sistemas informáticos. Isto inclui firewalls, sistemas de deteção de intrusões, antivírus, criptografia e outras soluções de segurança que ajudam a prevenir, detectar e responder a ameaças cibernéticas.

2.1.2 Pessoas

As pessoas é o pilar com mais impacto na cibersegurança, uma vez que representam o elo mais fraco da cibersegurança, pois são quem utilizam as tecnologias e quem tem acesso a sistemas e dados sensíveis. E se não forem devidamente treinadas e conscientes das ameaças, podem inadvertidamente comprometer a segurança dos sistemas. A formação e a sensibilização dos utilizadores são essenciais para garantir que eles compreendam os riscos e adotem práticas seguras.

2.1.3 Organizações

As organizações são responsáveis por estabelecer políticas, procedimentos e práticas de cibersegurança. Isto inclui a definição de normas de segurança, a implementação de controles de acesso, a realização de auditorias de segurança e a gestão de incidentes. As organizações devem criar uma cultura de segurança que envolva todos os colaboradores e garanta a conformidade com as regulamentações e melhores práticas.

2.1.4 Segurança Física

A segurança física refere-se à proteção dos ativos físicos, como servidores, *data centers* e dispositivos de rede, contra acessos não autorizados, roubos e danos. Isto inclui medidas como controlo de acesso físico, vigilância por vídeo, sistemas de alarme e proteção contra desastres naturais. Ou seja, é fundamental que os dispositivos estejam num local seguro e com acesso restrito apenas a pessoas autorizadas. Se possível também devem estar protegido contra falhas de energia ou falhas de *hardware*, como por exemplo, um disco rígido com defeito.

2.1.5 O pilar na intervenção digital forense

No contexto da intervenção digital forense, o pilar das pessoas é particularmente crucial, uma vez que os profissionais forenses são responsáveis por coletar, analisar e preservar evidências digitais de forma ética e legal. Eles devem possuir um profundo conhecimento técnico, bem como uma compreensão das leis e regulamentos relacionados com a cibersegurança e a privacidade. Além de que devem seguir rigorosos protocolos para garantir a integridade das evidências e evitar contaminação ou adulteração, como por exemplo, ao iniciar uma análise forense, impedir que o antivírus faça alterações nos ficheiros, ou seja, colocar o sistema em modo de *read-only*, entrando na parte do pilar das tecnologias e ao mesmo tempo no pilar das organizações, onde estas devem ter políticas e procedimentos claros para a condução de investigações forenses, garantindo a conformidade com as leis e regulamentos aplicáveis.

2.2 As três dimensões da segurança da informação

Existem três dimensões principais para garantir a segurança da informação, sendo elas a segurança física, a segurança lógica e a segurança humana. Todas estas dimensões estão ligadas entre si, e estão de acordo com a *SEGNAC4*, sendo esta a *Resolução do Conselho de Ministros 5/1990*, onde são estabelecidas normas e procedimentos que visam garantir a segurança da informação em sistemas informáticos, especialmente aqueles utilizados por entidades públicas.

2.2.1 Segurança Física

A segurança física envolve a proteção dos dispositivos físicos, como servidores, *data centers* e dispositivos de rede, contra acessos não autorizados, roubos e danos. Isto inclui medidas como controlo de acesso físico, vigilância por vídeo, sistemas de alarme e proteção contra desastres naturais. No contexto da *SEGNAC4*, a segurança física é fundamental para garantir o acesso restrito a áreas sensíveis e a proteção dos equipamentos contra ameaças que possam roubar ou danificar a informação armazenada.

2.2.2 Segurança Lógica

A segurança lógica baseia-se na proteção dos sistemas informáticos e das redes contra acessos não autorizados digitalmente, onde as medidas incluem autenticação, criptografia, *firewalls*, entre outros métodos que possam limitar o acesso a estes sistemas. No âmbito da *SEGNAC4*, é essencial implementar estas medidas para garantir a confidencialidade e integridade da informação classificada que está armazenada ou a ser transmitida através de sistemas informáticos.

2.2.3 Segurança Humana

A segurança humana refere-se à formação e sensibilização dos utilizadores para garantir que compreendam os riscos aos quais estão expostos e adotem práticas seguras, como a criação de palavras-passe fortes, o reconhecimento de tentativas de *phishing* e não partilhar informações sobre o trabalho, especialmente em ambientes de acesso público. No contexto da *SEGNAC4*, a segurança humana é crucial para prevenir vulnerabilidades que possam ser exploradas por atacantes, já que o fator humano é frequentemente a maior fraqueza dos sistemas informáticos.

2.3 O Conceito de Governança

A Governança, ao ser apresentada neste curso, refere-se a saber **quando e como** alguém acedeu a um sistema informático e a partir de que utilizador e com que permissões foi feito esse acesso, sendo uma monitorização que permite injeção de informação nos *SIEM* (Security Information and Event Management) para permitir assim identificar mais facilmente os ataques e os seus padrões, permitindo ainda uma reconstrução de como foi realizado o ataque. Mantém ainda uma gestão de dispositivos e registo de logs. Estes logs devem conter o endereço IP, a data e hora do acesso (em hora, minuto, segundos e fuso horário) e o porto de comunicação utilizado. A Governança deve ainda incluir assinaturas de ataques, segmentação de redes para evitar a propagação de incidentes e segregação de funções para impedir o comprometimento de dados.

Este conceito coincide com a *Resolução do Conselho de Ministros 41/2018*, que promove o reforço das capacidades de monitorização, deteção, resposta a incidentes e incentiva a implementação de medidas técnicas para aumentar a resiliência das infraestruturas críticas e a promoção de uma cultura de segurança transversal em todos os setores, sejam estes públicos, privados ou académicos.

É possível afirmar, com toda a certeza, que a Governança apresentada no curso está perfeitamente alinhada com os objetivos estratégicos da *Resolução do Conselho de Ministros 41/2018*, no que diz respeito ao reforço das capacidades de monitorização, deteção e resposta a incidentes, tal como definido nas normas ISO 27000, onde todos estes conceitos e normas são complementares entre si e visam o mesmo objetivo final, que é a proteção dos sistemas informáticos e dos dados contra ameaças cibernéticas em Portugal.