Licenciatura em Engenharia Informática

Curso Engenharia Informática

Ramo de Desenvolvimento de Aplicações

Unidade Curricular de Ética e Deontologia

Ano Letivo de 2023/2024

PALESTRA Nº 8

Ciber Segurança e Protecção de Infraestruturas Críticas

Eng.o Paulo Moniz

Realizada em 24 de abril de 2024

**“Ciber Segurança e Protecção de Infraestruturas Críticas”**

**João Alves Pereira de Carvalho**

**2019131769**

**Coimbra, 25 de abril de 2024**

**João Alves Pereira de Carvalho**

**Relatório da palestra “**Ciber Segurança e Protecção de Infraestruturas Críticas”

Trabalho de avaliação de natureza académica

**Coimbra, 25 de abril de 2024**

Índice

Resumo iii

1. Introdução 1
2. Sobre o palestrante, Engenheiro Paulo Moniz 2

2.1. Percurso Escolar 2

2.2. Carreia Profissional 2

2.3. Atualidade 2

1. EDP - Presença na cadeia de valor da energia 3
2. CiberRisco 4
3. Vulnerabilidades 5
4. CiberAtaques - CiberPoder 7

6.1. CiberAtaques 7

6.2. CiberPoder 7

1. CiberAtaques mais comuns 8

7.1. Ransomware 8

7.2. DoS - Denial of Service 8

7.3. BotNet 8

7.4. Phishing 8

1. Recursos - Infra-estruturas Críticas 9

8.1. Recursos 9

8.2. Cibersegurança 9

8.3. Ciberdefesa 9

1. Análise Crítica 10

Referências 11

Anexos A

# Resumo

A palestra focou-se na cibersegurança e proteção de infraestruturas críticas, destacando a importância da ética na engenharia para construir um mundo mais seguro. O especialista Engenheiro Paulo Moniz falou sobre a complexidade dos sistemas tecnológicos e as vulnerabilidades exploradas por atacantes, como a coordenação de veículos elétricos com senhas padrão.

Destacou a interligação entre sistemas OT (Tecnologia Operacional) e IT (Tecnologia da Informação) e a sofisticação dos ataques cibernéticos, como phishing, botnets e ransomware. Ele também comentou sobre os desafios de trabalhar com sistemas antigos que não foram projetados com segurança cibernética e ressaltou a necessidade de investir em cibersegurança para proteger infraestruturas críticas..

# Introdução

Este relatório resume os principais pontos da palestra, oferecendo uma visão geral sobre as melhores práticas em cibersegurança para proteger infraestruturas críticas. O objetivo é informar sobre a importância da segurança cibernética e a necessidade de investir em medidas de proteção para garantir a resiliência dos sistemas que sustentam a sociedade moderna. A palestra do Engenheiro Paulo Moniz, especialista em cibersegurança do grupo EDP, destacou os desafios e práticas para proteger infraestruturas críticas. A ética na engenharia, associada à proteção cibernética, é chave para criar um mundo mais seguro e sustentável.

# Sobre o palestrante, Engenheiro Paulo Moniz

## 2.1. Percurso Escolar

O Engenheiro Paulo Moniz formou-se em Engenharia Eletrotécnica e de Computadores pelo Instituto Superior Técnico em 1995. Posteriormente, concluiu uma Pós-Graduação em Sistemas de Informação na mesma instituição. Além disso, possui um mestrado em Segurança Informática pela Faculdade de Ciências da Universidade de Lisboa e um MSc em Information Security pela Universidade de Carnegie Mellon.

## 2.2. Carreia Profissional

Com uma experiência de cerca de 25 anos no setor das tecnologias de informação, Paulo Moniz iniciou a sua carreira como administrador de sistemas na EDP Distribuição. Mais tarde, passou para a EDINFOR, onde participou em vários projetos internacionais de desenvolvimento de soluções, atuando como analista, programador e formador. Em 2008, assumiu a liderança da Security Practice na Logica Iberia, marcando o início da sua dedicação à área de segurança.

## 2.3. Atualidade

Atualmente, Paulo Moniz é Diretor da área de Segurança da Informação e Risco IT na Digital Global Unit Security & IT Risk do Grupo EDP. Tem uma vasta experiência em gestão de projeto e desempenha um papel crucial na supervisão e proteção das infraestruturas críticas da empresa. Com sua formação e experiência, Paulo Moniz contribui significativamente para a segurança cibernética no setor energético..

# EDP - Presença na cadeia de valor da energia

A EDP (Energias de Portugal) é uma das maiores empresas de energia em Portugal, sendo também uma das principais prestadoras de serviços de energia a nível internacional. A EDP está presente em várias áreas do setor energético, incluindo a geração, distribuição e comercialização de energia elétrica. O grupo tem investido significativamente em energias renováveis e na transição para fontes mais sustentáveis de produção de energia.

A segurança das infraestruturas críticas é uma prioridade para a EDP, uma vez que a empresa é responsável pela distribuição de energia elétrica em Portugal. As infraestruturas da EDP são vitais para garantir a estabilidade do fornecimento de energia e, consequentemente, o funcionamento seguro e contínuo de diversos setores da sociedade

A EDP enfrenta desafios constantes relacionados à cibersegurança, especialmente devido à interligação entre seus sistemas de Tecnologia Operacional (OT) e Tecnologia da Informação (IT). Essas interconexões tornam a empresa mais vulnerável a ataques cibernéticos, o que exige uma abordagem proativa para identificar e prevenir ameaças.

# CiberRisco

O CiberRisco refere-se aos riscos associados à segurança cibernética em um ecossistema interdependente, onde organizações de diferentes tamanhos se apoiam umas nas outras para componentes críticos e serviços de negócios. Esta interdependência torna o sistema mais complexo e interconectado, criando desafios para a gestão de riscos

À medida que as redes de energia se tornam mais descentralizadas, com o surgimento de geradores em pequena escala, os ataques cibernéticos nesses geradores podem impactar a sociedade de forma significativa, tal como os ataques a entidades maiores. Portanto, é crucial que todas as organizações, independentemente de seu tamanho, colaborem para gerir e mitigar os riscos associados à interdependência do sistema e garantir a segurança cibernética e a resiliência da sociedade como um todo.

A gestão do CiberRisco requer uma abordagem abrangente, envolvendo prevenção, deteção, reação e recuperação para proteger as infraestruturas críticas, com destaque para a interdependência entre os diferentes setores e a necessidade de colaboração e responsabilidade entre todos os envolvidos.

# Vulnerabilidades

As vulnerabilidades em segurança cibernética são falhas ou lacunas nos sistemas, aplicações ou procedimentos que podem ser exploradas por atacantes. Estas falhas podem surgir durante o desenho, construção ou configuração de aplicações e serviços de TI, bem como em processos que suportam a sua gestão, como a reposição de senhas sem confirmação da identidade.

Empresas de grande dimensão costumam lidar com um elevado número de aplicações, o que leva a uma arquitetura complexa. Esta complexidade é um dos principais desafios para a segurança, como destaca Bruce Schneider, especialista em segurança, ao afirmar que "complexidade é o pior inimigo da segurança”.

Os sistemas legados, mais antigos, foram muitas vezes concebidos sem as preocupações de segurança modernas. Como resultado, há um grande número de vulnerabilidades nestes sistemas, que são introduzidas nas organizações ao longo do tempo. Remediar estas vulnerabilidades pode ser uma tarefa desafiadora, cara, e nem sempre eficaz, especialmente quando se trata de aplicar patches em sistemas complexos.

Empresas com uma longa história e grande dimensão enfrentam um risco significativo em termos de cibersegurança devido à presença de muitos sistemas legados, que requerem atenção e gestão cuidadosa para proteger contra possíveis ataques cibernéticos.

A configuração de sistemas e aplicações, bem como os procedimentos para a sua gestão, são fatores essenciais para garantir a segurança cibernética. Por exemplo, o uso de senhas padrão nos equipamentos pode criar portas abertas para atacantes.

Empresas de grande dimensão, devido à sua heterogeneidade, complexidade e tamanho, possuem muitos procedimentos e configurações que podem gerar vulnerabilidades nos sistemas. Isso requer uma atenção especial para evitar que falhas de configuração ou procedimentos inadequados comprometam a segurança cibernética. Portanto, é fundamental que essas organizações implementem boas práticas de segurança para proteger seus sistemas contra ameaças potenciais.

A transformação digital traz consigo novos paradigmas, como a computação em nuvem (que se torna central nas arquiteturas), Internet das Coisas (IoT), big data e mobilidade (como o conceito de BYOD - Bring Your Own Device). Esses avanços alteram o conceito de perímetro de segurança, ampliando o acesso aos dados e massificando o fluxo de informações.

Nas grandes organizações, é comum a dependência de prestadores de serviços externos (PSEs), tais como call centers, desenvolvimento, manutenção, outsourcing e equipas de BPO. Para garantir a segurança cibernética, é essencial envolver e alinhar esses prestadores de serviços com políticas e procedimentos de segurança, qualificação, comunicação e formação adequadas.

Os aspetos culturais desempenham um papel crucial na cibersegurança. Muitas vulnerabilidades resultam de engenharia social, por isso é importante que os colaboradores estejam conscientes dos riscos do ciberespaço, mesmo que não sejam facilmente perceptíveis em termos de avaliação de risco. A formação dos colaboradores para reconhecer e evitar esses riscos é fundamental para proteger a organização.

Empresas com uma longa história tendem a ter um grande número de colaboradores com diferentes formações e idades, o que torna essencial promover um comportamento adequado e consistente em relação à segurança cibernética. A conscientização de todos os colaboradores sobre a importância da segurança digital é vital para a proteção da organização contra ameaças cibernéticas.

# CiberAtaques - CiberPoder

Empresas com uma longa história tendem a ter um grande número de colaboradores com diferentes formações e idades, o que torna essencial promover um comportamento adequado e consistente em relação à segurança cibernética. A conscientização de todos os colaboradores sobre a importância da segurança digital é vital para a proteção da organização contra ameaças cibernéticas.

## 6.1. CiberAtaques

Os ciberataques são ações maliciosas que visam sistemas cibernéticos com diversos objetivos, como roubo de dados, interrupção de serviços ou obtenção de informações confidenciais. Os ataques podem ser perpetrados por agentes com variados recursos e motivações, desde a busca por prazer individual na demonstração de poder até ações terroristas bem elaboradas.

A sofisticação das ameaças cibernéticas evoluiu com o tempo, resultando em ataques mais avançados, como as APTs (Advanced Persistent Threats), que podem causar grandes impactos, como nos casos dos ataques na Ucrânia, Estónia, Sony e TV5. A disponibilidade de kits ou serviços para a realização de ciberataques facilita a participação de mais pessoas nessas atividades maliciosas.

A EDP, por gerir infraestruturas críticas e manipular informações pessoais de milhões de clientes, é um alvo potencial para esses ataques sofisticados, exigindo uma abordagem cuidadosa e proativa para lidar com essas ameaças.

## 6.2. CiberPoder

O ciberpoder é o uso do ciberespaço para exercer poder político ou militar. Atualmente, todos os conflitos políticos e militares têm uma dimensão cibernética, com atacantes usando uma variedade de estratégias e táticas para alcançar seus objetivos.

O ciberpoder pode ser um recurso vantajoso para partes mais fracas em conflitos contra nações mais fortes, especialmente devido ao domínio dessas nações em TI. Além disso, os ataques cibernéticos podem causar danos significativos a infraestruturas críticas, como serviços de internet, sistemas de controle de infraestruturas físicas e informações confidenciais.

Os efeitos do ciberpoder se manifestam tanto dentro do ciberespaço, com ataques de negação de serviço e difusão de mensagens, quanto fora do ciberespaço, com ações intrusivas contra sistemas de controle de infraestruturas físicas.

Os principais desafios na utilização do ciberpoder são a deteção, atribuição e enquadramento de resposta. Muitas vezes, é difícil identificar a atividade maliciosa, atribuir sua origem ou responder de maneira adequada sem ultrapassar os limites de um conflito internacional.

# CiberAtaques mais comuns

## 7.1. Ransomware

Este tipo de ataque envolve a encriptação dos dados de um sistema, bloqueando o acesso do utilizador até que seja pago um resgate (ransom) para a recuperação dos dados. É uma forma de extorsão digital que pode afetar tanto empresas como indivíduos.

## 7.2. DoS - Denial of Service

Um ataque de negação de serviço (DoS) tem como objetivo sobrecarregar um sistema ou rede com tráfego excessivo, tornando-o indisponível para os utilizadores legítimos. Pode ser feito através de uma única máquina ou de uma rede coordenada de dispositivos (ataque DDoS).

## 7.3. BotNet

Uma botnet é uma rede de dispositivos infetados por malware que podem ser controlados remotamente por um atacante. Os dispositivos da botnet são usados para realizar vários tipos de atividades maliciosas, como ataques DDoS, envio de spam ou mineração de criptomoedas.

## 7.4. Phishing

O phishing é uma técnica de ataque que visa enganar os utilizadores para que revelem informações sensíveis, como senhas ou dados de cartão de crédito. Os atacantes geralmente usam e-mails falsos ou sites fraudulentos para se passarem por entidades confiáveis e induzirem os utilizadores a fornecerem suas informações pessoais.

# Recursos - Infra-estruturas Críticas

As infraestruturas críticas são os ativos, sistemas e redes, físicos ou virtuais, que são tão essenciais que a sua incapacidade ou destruição teria um efeito debilitante na segurança nacional, estabilidade económica, saúde ou segurança públicas, ou qualquer combinação destes.

## 8.1. Recursos

No ciberespaço, as organizações, especialmente aquelas que detêm infraestruturas críticas como a EDP, desempenham um papel fundamental na cibersegurança e ciberdefesa. Mesmo em cenários de guerra, ao contrário dos campos convencionais de conflito, estas organizações são essenciais para manter a segurança e proteger o bem-estar e os direitos dos cidadãos.

## 8.2. Cibersegurança

A cibersegurança refere-se às atividades de prevenção, monitorização e resposta a ameaças no ciberespaço que coloquem em risco a segurança das pessoas ou organizações. Cabe às forças policiais e serviços de informação garantir a cibersegurança, protegendo as infraestruturas críticas e dados sensíveis.

## 8.3. Ciberdefesa

A ciberdefesa, por sua vez, está relacionada com as atividades de prevenção, monitorização e reação a ameaças que coloquem em risco a soberania nacional. Esta missão é assegurada pelas forças armadas, que trabalham para proteger o país de ataques cibernéticos que possam comprometer sua segurança e estabilidade.

# Análise Crítica

A palestra sobre cibersegurança e proteção de infraestruturas críticas aborda um tema extremamente relevante para a sociedade moderna, destacando os desafios enfrentados pelas organizações que lidam com infraestruturas críticas, como a EDP. O enfoque na ética e sustentabilidade na engenharia é especialmente importante, pois enfatiza a necessidade de adotar abordagens que garantam não apenas a segurança, mas também o bem-estar social e ambiental.

O conteúdo da palestra oferece uma cobertura abrangente dos diversos aspectos da cibersegurança, desde as vulnerabilidades e ciberataques até o conceito de ciberpoder e seus impactos nas infraestruturas críticas. A utilização de exemplos práticos, como os ataques à rede elétrica, ajuda a ilustrar a gravidade das ameaças cibernéticas e a necessidade de estar preparado para enfrentá-las.

Além disso, a palestra ressalta a importância da prevenção, monitorização e resposta eficaz às ameaças cibernéticas, bem como a colaboração entre forças policiais, serviços de informação e organizações responsáveis por infraestruturas críticas. A interdependência entre os diferentes setores da sociedade e a necessidade de manter a soberania nacional também são aspectos-chave abordados.

Em suma, a palestra oferece uma visão clara dos desafios e responsabilidades associados à cibersegurança e proteção de infraestruturas críticas, destacando a necessidade de estratégias eficazes para mitigar riscos e garantir a resiliência das organizações e da sociedade como um todo.

# Referências

Nota de imprensa da palestra acerca do palestrante, Moodle - Unidade Curricular de Ética, consultado a 25 de abril de 2024  
  
Notas tomadas acerca da palestra.

# Anexos

Nada a anexar