Departamento de Engenharia Informática e de Sistemas
Instituto Superior de Engenharia de Coimbra
Instituto Politécnico de Coimbra

Licenciatura em Engenharia Informática
Curso Diurno
Ramo de Sistemas de Informação
Unidade Curricular de Ética e Deontologia
Ano Letivo de 2022/2023

***PALESTRA Nº** 2*
***Título da Palestra:** Cibersegurança e Proteção de Infraestruturas Críticas*
***Palestrante:** Eng.º Paulo Moniz*
***Realizada em** 08 **de** Março **de** 2023*

Relatório da Segunda Palestra de Ética e Deontologia

Luís Henrique Pessoa Oliveira Travassos
Número de Aluno: 2021136600
Coimbra, 08 de março de 2023

Luís Henrique Pessoa Oliveira Travassos

Cibersegurança e Proteção de Infraestruturas Críticas

Relatório da Segunda Palestra de Ética e Deontologia

Coimbra, 08 de Março de 2023

Índice

Resumo

A palestra sobre “Cibersegurança e Proteção de Infraestruturas Críticas” destacou a importância de proteger as redes e sistemas que sustentam as **infraestruturas críticas**, como energia, água, transporte e saúde, contra-ataques cibernéticos. O palestrante, Eng.º Paulo Moniz, abordou também as **principais ameaças cibernéticas**, como ransomware e ataques de negação de serviço (DDoS), e discutiu as melhores **práticas de segurança** cibernética para mitigar essas ameaças, assim como também enfatizou a importância de manter toda a tecnologia indispensável atualizada e de acordo com as regulamentações de segurança, de forma a garantir a resistência e a confiabilidade das infraestruturas críticas. No geral, a palestra foi informativa e relevante para a formação de um engenheiro informático responsável pela segurança dos sistemas e redes de infraestruturas críticas.

1. Introdução

Neste relatório irei abordar os conteúdos da palestra sobre “Cibersegurança e Proteção de Infraestruturas Críticas”, seguindo a mesma ordem de temas que a palestra, sendo esta:

- **Vulnerabilidades**
  - Arquitetura Complexa – Número de aplicações e Serviços IT;
  - Sistemas legados;
  - Procedimentos e considerações;
  - Transformação Digital – Novos Desafios;
  - Número de prestadores de serviços externos;
  - Cultura Cibersegurança;
  - Interligação de redes IT/OT;
- **Ciberataques - Ciberpoder**
  - Características do ciberespaço – Global Common;
  - Características do CiberPoder;
  - Características das Ameaças Híbridas;
  - Exemplos de Ameaças Híbridas;
  - Tipificando as ameaças – um espaço assimétrico;
  - Sofisticação das ameaças e recursos;
  - Perspetiva histórica dos Ciberataques;
  - Ataques mais comuns;
- **Recursos**
  - Infraestruturas críticas – Dependência dos sistemas informáticos;
  - Missão da CiberSegurança e CiberDefesa;
  - Riscos e impactos;

No final do relatório haverá ainda uma análise critica da palestra onde irei referenciar alguns temas que achei mais interessante e dar o meu parecer sobre eles.

2. Descrição do Tema Abordado na Palestra

2.1. Vulnerabilidades

Um dos pontos mencionados pelo palestrante em relação ás vulnerabilidades foi a arquitetura complexa, que pode aumentar, por vezes, o número de aplicações e serviços de TI. Isso pode resultar em possíveis vulnerabilidades em uma rede, pois cada aplicação pode ter sua própria vulnerabilidade e, em um ambiente complexo, pode ser difícil de gerenciar e garantir a segurança de todas elas.

Outro ponto de vulnerabilidade mencionado foi a questão dos sistemas legados, que geralmente são mais antigos e podem ser vulneráveis a ataques cibernéticos devido à falta de atualizações de segurança. O palestrante ainda destacou a importância de avaliar regularmente esses sistemas e aplicar patches de segurança para protegê-los contra vulnerabilidades conhecidas.

Foi também mencionado a importância de ter procedimentos e considerações claras para garantir a segurança dos sistemas e redes. Isso inclui ter políticas de segurança claras, planos de resposta a incidentes e sistemas de monitoramento para detetar possíveis ataques. Também foi destacada a importância de avaliar cuidadosamente os riscos de segurança de qualquer nova tecnologia adotada e garantir que ela seja configurada de forma segura.

O grande número de prestadores de serviços externos também foi apontado como um risco, uma vez que pode aumentar o número de pontos vulneráveis na rede que é importante avaliar cuidadosamente a segurança desses prestadores de serviços e garantir que eles cumpram os padrões de segurança exigidos.

Por fim, a interligação de redes IT/OT foi mencionada como um ponto crítico, pois pode permitir a propagação de ataques entre as redes e sistemas de controle industrial. A palestra destacou a importância de adotar medidas de segurança específicas para proteger as redes OT, que geralmente são mais vulneráveis do que as redes IT convencionais sendo assim importante que todos os envolvidos na segurança das redes estejam conscientes e adotem boas práticas de segurança, desde a alta gerência até os funcionários do nível operacional.

2.2 Ciberataques - Ciberpoderes

Na palestra foi enfatizado que o ciberespaço é um ambiente virtual que não conhece fronteiras geográficas e é possível aceder a este por meio de diversas tecnologias, tais como computadores, smartphones e tablets, e por ser um ambiente global, as informações compartilhadas nele podem ser acessadas por pessoas de qualquer lugar do mundo.

Já o CiberPoder é a capacidade de controlar ou influenciar ações no ciberespaço, podendo essa capacidade ser utilizada para diversos fins, como espionagem, sabotagem ou extorsão e exercida por governos, grupos ou mesmo indivíduos.

Também foram mencionadas as ameaças híbridas, sendo estas aquelas que combinam elementos de diferentes tipos de ameaças, tais como ameaças cibernéticas, terroristas e/ou militares, havendo diversos exemplos destes, como o ataque cibernético à central nuclear ucraniana em 2015, no qual os invasores combinaram um ataque cibernético com sabotagem física, ou o uso de drones para ataques terroristas, que combina tecnologias aéreas com armas.

Em relação a este assunto o palestrante também afirmou que é costume partes envolvidas nestes conflitos terem recursos muito diferentes. Os atacantes podem ser pequenos grupos de hackers com recursos limitados, enquanto os defensores podem ser grandes empresas ou governos com muito mais recursos, o que torna este problema algo mais complexo e avançado que os conflitos habituais.

Foi nos também dito que entre os ataques mais comuns estava o “phishing”, que é uma técnica de engenharia social para obter informações pessoais, senhas e dados bancários, e o ransomware, que é um tipo de malware que criptografa os arquivos do computador e exige um resgate para liberá-los.

Para terminar foi também discutido sobre a necessidade de existirem investimentos em pesquisa e desenvolvimento para aprimorar a segurança cibernética e que é fundamental que os profissionais da área de Engenharia Informática estejam sempre atualizados e capacitados para enfrentar os desafios da segurança cibernética e contribuir para a proteção de infraestruturas críticas e a segurança da sociedade como um todo.

2.3. Recursos

O palestrante também apresentou alguns pontos importantes sobre a importância dos sistemas informáticos para as infraestruturas críticas, a missão da Cibersegurança e Ciberdefesa e os riscos e impactos associados a essa dependência.

As infraestruturas críticas, tais como as de energia, transporte, comunicações e financeiras, dependem cada vez mais dos sistemas informáticos para garantir seu funcionamento adequados e qualquer falha nesses sistemas pode ter graves consequências para a sociedade, como por exemplo a interrupção do fornecimento de energia elétrica ou até a paralisação de sistemas de transporte público.

Foi nos explicado que a missão da Cibersegurança e Ciberdefesa é garantir a proteção destes sistemas, identificando e mitigando as possíveis ameaças cibernéticas que podem colocar em risco as infraestruturas críticas, envolvendo também a implementação de medidas preventivas, tais como o monitoramento constante dos sistemas, a análise de vulnerabilidades e a implementação de políticas de segurança cibernética.

Na palestra foram também explicados os riscos e impactos associados à dependência dos sistemas informáticos para as infraestruturas críticas, sendo estes diversos e com a capacidade de ter consequências graves para a sociedade, sendo bem capazes de interromper o fornecimento de serviços essenciais, prejudicar a economia, causar perda de vidas e gerar caos social.

Além disso, os recursos necessários para proteger esses sistemas são cada vez mais complexos e caros, requerendo profissionais altamente capacitados, tecnologias avançadas e recursos financeiros significativos para garantir a eficácia da proteção.

3. Análise Crítica

A palestra sobre "Cibersegurança e Proteção de Infraestruturas Críticas" relevou-se extremamente atual, tendo em vista o crescente número de ciberataques que ocorrem atualmente e o conjunto de pontos abordados que são fundamentais para entender e proteger infraestruturas críticas de possíveis ameaças cibernéticas.

Uma das questões mais importantes que foram discutidas na palestra foi a questão das vulnerabilidades de sistemas, sendo nos ensinado que todas as infraestruturas de TI são suscetíveis a vulnerabilidades e que elas podem ser exploradas por hackers mal-intencionados, tendo o palestrante fornecido uma visão geral das vulnerabilidades mais comuns que podem ser encontradas em sistemas, bem como técnicas para identificar e corrigir essas vulnerabilidades.

Outro ponto fundamental abordado na palestra foi a questão dos ciberataques, uma vez que este número está a aumentar a cada ano e que a complexidade desses ataques está a se tornar cada vez maior e foi também destacado os diferentes tipos de ataques que podem ocorrer, bem como os impactos que esses ataques podem ter em uma infraestrutura crítica.

Além disso, a palestra também abordou a questão dos recursos necessários para proteger infraestruturas críticas, sendo preciso um grande investimento em tecnologia, treinamento de pessoal e recursos financeiros. Foi ainda nos mostrado pelo palestrante, em geral, os recursos necessários para garantir a proteção adequada de infraestruturas críticas e ainda foi destacada a importância de se investir em segurança cibernética.

Por fim, acredito que a palestra foi muito informativa e relevante, tendo sido bastante benéfico todos os exemplos dados e a atualidade da informação, assim como a grande diversidade de temas centrados na Cibersegurança.

4. Considerações finais

A minha consideração final à palestra “Cibersegurança e Proteção de Infraestruturas Críticas" acaba por ser bastante positiva. A apresentação foi muito boa, abrangendo de forma clara e concisa os principais pontos relacionados à segurança cibernética e a proteção de infraestruturas críticas e ainda ofereceu uma visão geral sobre vulnerabilidades, ciberataques e recursos de proteção, sendo estas informações essenciais para compreender a importância da segurança cibernética e os desafios que as infraestruturas críticas enfrentam.

Além disso, a palestra foi bem organizada, usando exemplos relevantes para tornar os conceitos mais acessíveis e fáceis de compreender. O palestrante, Eng.º Paulo Moniz, foi bastante claro e objetivo, transmitindo de forma clara e coerente as informações relevantes.

Por fim, acredito que a palestra foi uma excelente oportunidade para aprimorar os meus conhecimentos em segurança cibernética e para refletir sobre a importância da proteção das infraestruturas críticas.

Referencias

- Centro Nacional de CiberSegurança;
- Pesquisa sobre o tema da palestra;