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 Lectivo de 2022/2023

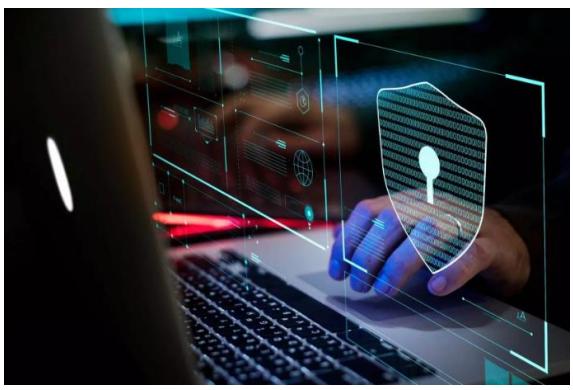
PALESTRA Nº 2

Cibersegurança e Proteção de Infraestruturas Críticas

Eng.º Paulo Moniz Diretor da Área de Segurança da Informação e Risco IT no Grupo EDP

Realizada em 8 de março de 2023

CIBERSEGURANÇA E PROTEÇÃO DE INFRAESTRURAS CRÍTICAS



Paulo Gouveia

Número de Aluno: 2020121705

Coimbra, 14 de março de 2023

Paulo Gouveia

Cibersegurança e Proteção de Infraestruturas Críticas

No âmbito da cadeira de Ética e Deontologia

Coimbra, 14 de março de 2023

Índice

Resumo

Este relatório foi desenvolvido com base na palestra sobre cibersegurança e proteção de infraestruturas críticas, ministrada pelo Eng.º Paulo Moniz, tema abordado durante a segunda aula da Unidade Curricular de Ética e Deontologia no dia 3 de março de 2023, integrada na Licenciatura de Engenharia Informática do Instituto Superior de Engenharia de Coimbra.

Aborda temas como a presença da EDP na cadeia de valor de energia, CiberRisco e como medi-lo,que deu continuação ao tópico de vulnerabilidades, CiberAtaques e CiberPoder. Foram também discutidas tipologias comuns de ataques, como BotNet, “deny of service” e “phishing”, bem como a presençade diferentes recursos nas infraestruturas críticas e como tem que ser feita uma lista de prioridades no que defender.

Palavras-chave:

- Cibersegurança
- Vulnerabilidades
- Recursos
- CiberRiscos
- CiberAtaques

1. INTRODUÇÃO

Este relatório é referente à palestra "Cibersegurança e Proteção de Infraestruturas Críticas", apresentada em 8 de março de 2023. O tema principal da palestra foi o CiberRiscos, vulnerabilidades existentes, CiberAtaques, CiberPoder, e recursos a serem utilizados.

O relatório apresenta uma síntese dos tópicos discutidos na palestra, iniciando por uma breve caracterização da EDP, e a sua presença na cadeia de valor da energia. Iniciando assim o tópico de CiberRiscos e a forma de medi-los. A medição consiste em avaliar os tipos de vulnerabilidades, o perfil do atacante, definido pelo termo CiberAtaque, bem como a magnitude dessa ameaça, definida como CiberPoder, incluindo as tipologias de ataques com exemplos reais. Por fim, destacamos a importância de estabelecer uma lista de prioridades para proteger os recursos críticos das infraestruturas, além da relevância das leis que dão suporte a essa lista.

Será feita uma análise crítica que abordará pontos fortes e fracos da apresentação, bem como uma avaliação dos argumentos e evidências apresentados.

Este relatório tem como finalidade apresentar informações relevantes aos estudantes acerca dos CiberRiscos presentes no mundo, explicando a forma como são medidos e diferentes maneiras de alocar os recursos para combater os ataques. As fontes de informação utilizadas foram o palestrante.

2. Descrição do Tema Abordado na Palestra

2.1. EDP

A EDP (Energias de Portugal) é uma empresa do setor energético português, que atua na geração, distribuição e comercialização de energia elétrica e gás natural.

Além de Portugal, está presente em outros 13 países, empregando cerca de 12.000 trabalhadores. A empresa possui uma base de 8,7 milhões de clientes de energia elétrica e 1,7 milhões de clientes de gás natural. A capacidade de armazenamento da empresa é de 26.753 GW de energia e tem uma produção anual de energia de 70 TWh.

Figura 1 - Países que a EDP opera

2.1.1. A presença da EDP na cadeia de valor d energia

A EDP (Energias de Portugal) está presente em diversas etapas da cadeia de valor de energia, incluindo a geração, distribuição e comercialização de energia elétrica e gás natural, o transporte é feito por outra empresa no caso da energia.

Este capítulo ilustra como isto tudo é um sistema vivo, começando pela produção de energia. Essa imensa energia produzida de seguida é transportada por uma rede, que pode ser visto como uma coluna vertebral que atrevessa diversos países, sendo este tranporte feito pela REN (Redes Energéticas Nacionais).

A EDP é quem faz a distribuição final para a energia chegar às nossas cidades, vilas e casas. Além disso, a comercialização de energia elétrica e gás natural envolve também um fator de marketing e o mercado ibérico de energias.

Como observação final, é realçando como é um sistema que têm que manter sempre um nível mínimo de produção para evitar eventual cenários menos desejados. Essa necessidade de manter o equilíbrio do sistema deu origem aos tópicos mais relevantes da palestra, que abordaram as vulnerabilidades e os riscos de um ataque ciber que poderia desestabilizar a forma como o sistema funciona.

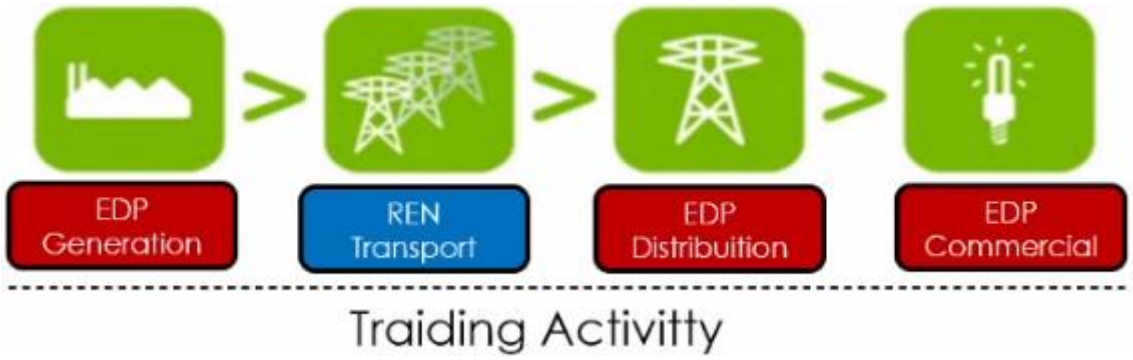


Figura 2- Sequência de como a energia é produzida e distribuída

2.2. CiberRisco

O risco no ciberespaço consiste em ter um recurso tecnológico com eventual vulnerabilidade, sendo explorado por um agente com motivações benignas ou maliciosas. Cabe às organizações fazer tudo o que estiver ao seu alcance para prevenir ocorrências deste tipo, detetar possíveis vulnerabilidades, reagir aos incidentes e recuperar do ataque.

O restante da palestra baseia-se nos diversos pontos acima mencionados, como os diferentes tipos de atacantes e vulnerabilidades, bem como as medidas de prevenção, deteção, reação e recuperação de dados em caso de ciberataques. A avaliação do risco envolve a análise desses pontos em conjunto com a quantidade de recursos necessários para se defender e quais os tipos de ataques que podem explorar essas vulnerabilidades no sistema que têm presente.

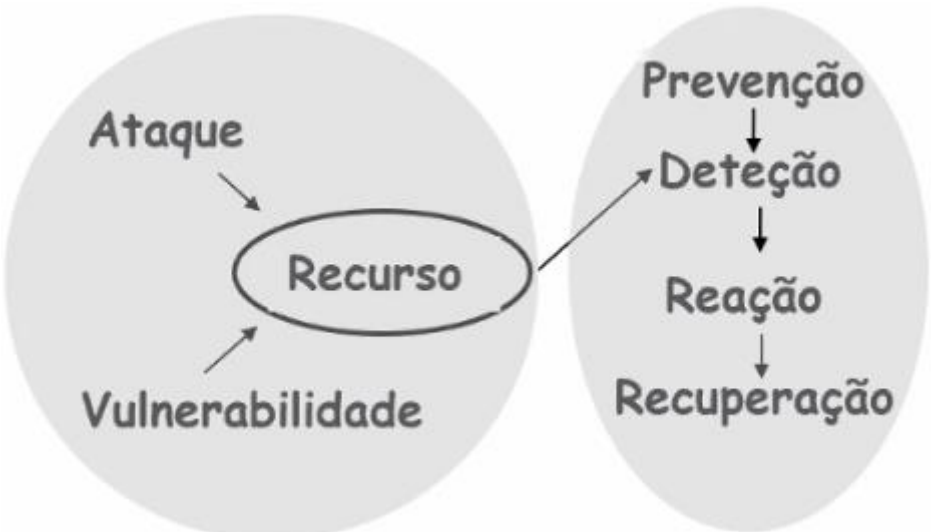


Figura 3 - Exemplo de como um recurso é alvo de exploração, e os passos de resposta que se seguem caso o recurso seja comprometido

2.3. Vulnerabilidades

Vulnerabilidades são falhas que podem ser criadas de forma voluntária ou involuntária, seja no desenho, construção e configuração de aplicações e serviços de TI, bem como nos processos e procedimentos que suportam a sua gestão, tais como a reposição de password sem confirmação da identidade.

Existem também falhas propositadas, tamém conhecidas como “backdoors”, são colocadas intencionalmente nos sistemas para mais tarde serem explorados.

2.3.1. Arquitetura Complexa

No contexto de arquiteturas complexas, como é comum em empresas de grande dimensão, as vulnerabilidades podem ser ampliadas devido à complexidade envolvida. Isso significa que quanto mais complexa é a arquitetura, mais difícil é garantir a segurança, tornando-se um fator crítico na gestão de riscos cibernéticos.

Como disse Bruce Schneider, especialista em segurança, "a complexidade é o pior inimigo da segurança".

2.3.2. Sistemas legados

Sistemas legados, muitas vezes concebidos sem preocupações de segurança, apresentam um elevado número de vulnerabilidades que são introduzidas nas organizações. A remediação dessas vulnerabilidades (por exemplo, patches) é complicada, cara, pouco flexível e nem sempre eficaz, o que representa um risco significativo em termos de cibersegurança. Isso é especialmente preocupante para empresas de grande dimensão e com história, que tendem a possuir muitos sistemas legados em uso.

Muitos destes sistemas foram criados numa época em que ainda não havia a noção de como um sistema poderia ser atacado e explorado de forma malicionasa.

2.3.3. Procedimentos e Configurações

A configuração de sistemas e aplicações, assim como os procedimentos para a sua gestão, são fatores essenciais na cibersegurança, já que vulnerabilidades podem surgir devido a configurações mal feitas ou procedimentos inadequados (como senhas padrão em equipamentos).

Uma exemplo mencionado na palestra é como, a partir do endereço IP de uma impressora, é possível aceder a ficheiros em espera ou em histórico na impressora, que podem conter informações críticas. Embora geralmente seja necessário fazer login para aceder essa página, em muitos casos, senhas padrão não alteradas são deixadas pelo gestor dos equipamentos da empresa, tornando o sistema vulnerável a ataques.

Empresas de grande dimensão enfrentam desafios nesse sentido, pois a heterogeneidade, complexidade e dimensão dos seus sistemas podem resultar em várias configurações e procedimentos vulneráveis, exigindo uma atenção especial a esse aspecto.

2.3.4. Transformação Digital

A transformação digital traz consigo novas formas de funcionamento, tais como a computação em nuvem (que se torna no núcleo das arquiteturas), a Internet das Coisas (IoT), o big data ou a mobilidade (por exemplo, a prática de BYOD - Bring Your Own Device). Como resultado, o conceito de perímetro muda, o acesso e a massificação dos dados aumentam, e os riscos de cibersegurança alteram-se.

Isto leva-nos a ter mais cuidado com os equipamentos que utilizamos para aceder aos sistemas da empresa, de forma a não comprometê-los. Também é importante ter atenção

aos serviços de cloud que utilizamos para armazenar ficheiros da empresa, de forma a garantir a sua segurança.

2.3.5. Prestadores de Seviços

As grandes organizações muitas vezes dependem de prestadores de serviços externos (PSEs), como call centers, equipes de desenvolvimento e manutenção, outsourcing, e equipes de processamento de negócios (BPO). É essencial que haja um envolvimento e alinhamento adequados com esses prestadores de serviços externos, incluindo a qualificação, comunicação, formação e alinhamento dos procedimentos com as políticas da empresa. A contratação também é um fator importante a ser considerado.

2.3.6. Cultura Cibersegurança

Aspetos culturais têm grande importância na cibersegurança, uma vez que muitas vulnerabilidades resultam de engenharia social. É importante que os colaboradores estejam conscientes dos riscos do ciberespaço e que assumam um comportamento adequado neste domínio. Empresas com muita história possuem um elevado número de colaboradores de diversas formações e faixas etárias, o que torna ainda mais crítico este aspecto para a segurança organizacional e pessoal.

Um exemplo claro da diferença de abordagem é a proteção de dados nos Estados Unidos, que é mais orientada para o estado, enquanto na Europa há um foco maior na proteção dos dados pessoais. Além disso, é possível observar casos de falta de conscientização em pessoas mais idosas ou em regiões onde a tecnologia é uma novidade e as vulnerabilidades existentes são desconhecidas, como a não alteração de senhas “default”.

2.3.7. Redes IT/OT

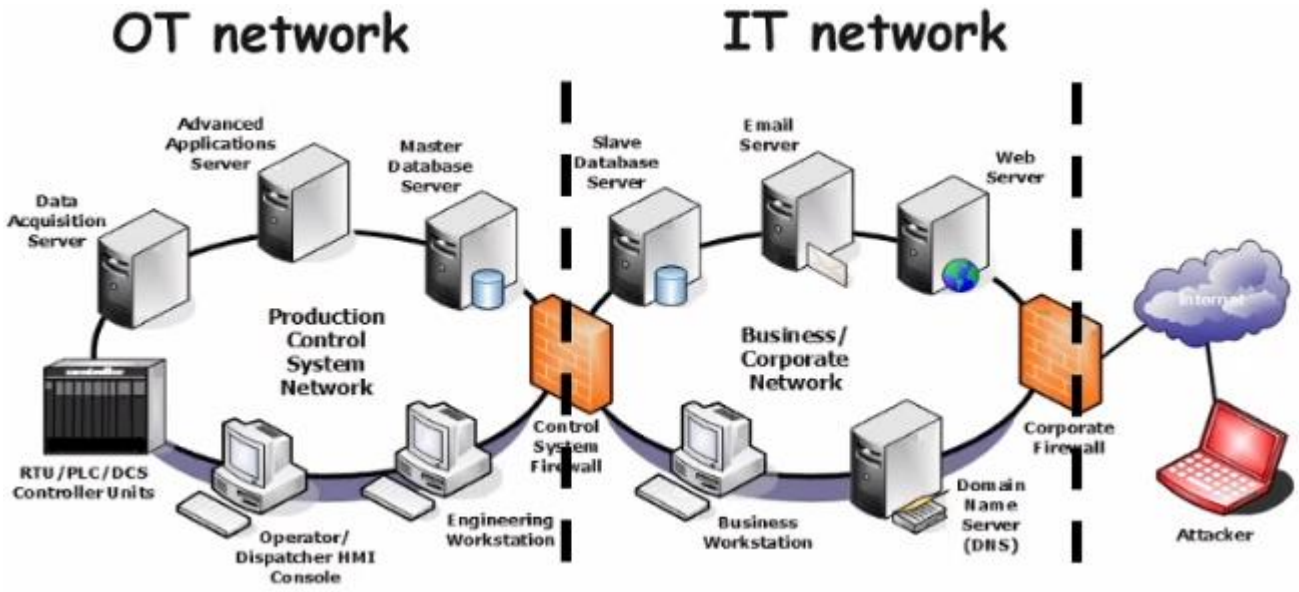


Figura 4 - Como é feita a interação de redes IT e OT

As redes de TI são usadas para gerenciar dados e sistemas de informação em ambientes administrativos, enquanto as redes de OT são usadas para controlar e monitorar processos industriais em tempo real. As redes de TI geralmente têm acesso à internet, enquanto as redes de OT são geralmente isoladas da internet e dos sistemas de TI.

As redes de OT são projetadas para suportar aplicativos industriais, enquanto as redes de TI são projetadas para suportar aplicativos de escritório e de produtividade. As redes de OT enfrentam riscos de segurança cibernética, como ataques de negação de serviço e explorações de vulnerabilidades, o que pode ter consequências graves para a segurança e a produção industrial.

Com a evolução dos serviços e benefícios oferecidos aos clientes e cidadãos, a utilização de soluções tecnológicas requer uma intensificação na troca de dados e interligação de sistemas, como as redes de energia inteligentes.

Antigamente, os sistemas industriais eram isolados e utilizavam protocolos pouco conhecidos, mas atualmente, muitos deles utilizam protocolos IP (Internet Protocol) e seus protocolos legados ficam expostos na internet, tornando-se acessíveis a qualquer pessoa. Essa nova realidade traz consigo novas vulnerabilidades e riscos, exigindo uma abordagem holística para a segurança.

2.4. CiberAtaques

Ciberataques são ações realizadas por indivíduos ou organizações com motivações criminosas diversas, que buscam explorar vulnerabilidades nos recursos tecnológicos das organizações para comprometer suas informações e infraestruturas. Esses ataques podem ter consequências financeiras, legais, de imagem ou operacionais, causando impactos negativos significativos.

2.4.1. CiberPoder

O termo CiberPoder refere-se ao poder que um ator (como um estado-nação ou um grupo de hackers) pode exercer no ambiente cibernético, seja por meio de ataques cibernéticos ou outras atividades relacionadas à segurança cibernética.

Dimensão Física e Virtual do Ciberpoder	Efeitos dentro do Ciberespaço	Efeitos fora do Ciberespaço
Instrumentos do Ciberespaço para o exercício de poder	**Intrusivos:** Ataques de negação de serviços na internet. **Ligeiros:** Estabelecimento de normas e standards para requisitos de segurança.	**Intrusivos:** Ataques aos sistemas que controlam infraestruturas físicas. **Ligeiros:** Difusão de mensagens na internet para a mudança de opinião publica.
Instrumentos "Físicos" para o exercício de poder	**Intrusivos:** Controlo dos Governos sobre as empresas e os serviços de internet que disponibilizam. **Ligeiros:** Disponibilização de plataformas e comunicações para suportar causas ligadas à defesa dos direitos humanos.	**Intrusivos:** Destruição física de recursos tecnológicos. **Ligeiros:** Discriminação seletiva de serviços ou mesmo a difamação de certas localizações na internet.

Figura 5 - Dimensões do ciberpoder com exemplos (fonte: adaptação Nye, 2010)

2.4.1.1. Características do CiberEspaço

Termos como "Low Barriers to entry, Mutable Geography, Opportunity for Concealment, No defined frontiers" refere-se a algumas características do ciberespaço que tornam difícil a atribuição de responsabilidades em caso de ataques cibernéticos. Essas características incluem:

- Baixas barreiras de entrada: qualquer pessoa com conhecimento técnico suficiente pode se envolver em atividades cibernéticas maliciosas, tornando difícil identificar a fonte do ataque.

- Geografia mutável: o ciberespaço não é restrito a uma localização geográfica específica, o que torna difícil determinar onde um ataque foi originado.

- Oportunidade de ocultação: os atacantes podem esconder sua identidade e localização por meio do uso de ferramentas de anonimato e técnicas de ocultação, dificultando a identificação deles.

- Falta de fronteiras definidas: o ciberespaço não possui fronteiras físicas claras, o que significa que os ataques podem cruzar fronteiras internacionais, tornando difícil a aplicação da lei e a responsabilização dos atacantes.

O ciberespaço apresenta assimetrias em termos de poder, já que indivíduos ou grupos com poucos recursos podem causar grandes danos. Um exemplo disso é o caso de Edward Snowden, que com poucos recursos, foi capaz de expor informações altamente sensíveis e impactar a segurança nacional dos Estados Unidos.

No entanto, é importante ressaltar que a difusão de poder no ciberespaço não significa igualdade de poder. Grandes organizações e Estados-nação ainda possuem vantagens em termos de recursos e habilidades técnicas, e podem exercer poder significativo no ambiente cibernético.

2.4.2. Ameaças Híbridas

As ameaças híbridas são caracterizadas pelo uso sincronizado de múltiplos instrumentos de poder adaptados para explorar vulnerabilidades específicas em todo o espectro de funções sociais.

O objetivo é convocar efeitos sinérgicos para surpreender o indivíduo e a sociedade, destruindo a confiança e causando frustração nas instituições sociais e governos, conduzindo a situações de caos social.

Alguns dos métodos que podem ser usados em simultânio podem ser, por exemplo, os que foram utilizados na agressão contra a Ucrânia da parte da Rússia:

• Campanhas de desinformação

• Ataques cibernéticos contra infraestruturas críticas para intimidar a população e enfraquecer a confiança no governo e no sistema político

• Hacking de sistemas de armamento.

2.4.3. Topologias

Os ciberataques podem ser realizados por uma ampla gama de agentes hostis, com diferentes recursos e motivações. Algumas vezes, os ataques são motivados por prazer individual, enquanto outras vezes podem ser parte de ações terroristas.

É importante ressaltar que o ciberespaço é assimétrico na perspectiva do exercício do poder, o que significa que um pequeno ator com poucos recursos pode causar um impacto

muito grande. Diante dessa realidade, é fundamental entender as diferentes tipologias de ciberataques para poder proteger as organizações e indivíduos de possíveis ameaças.

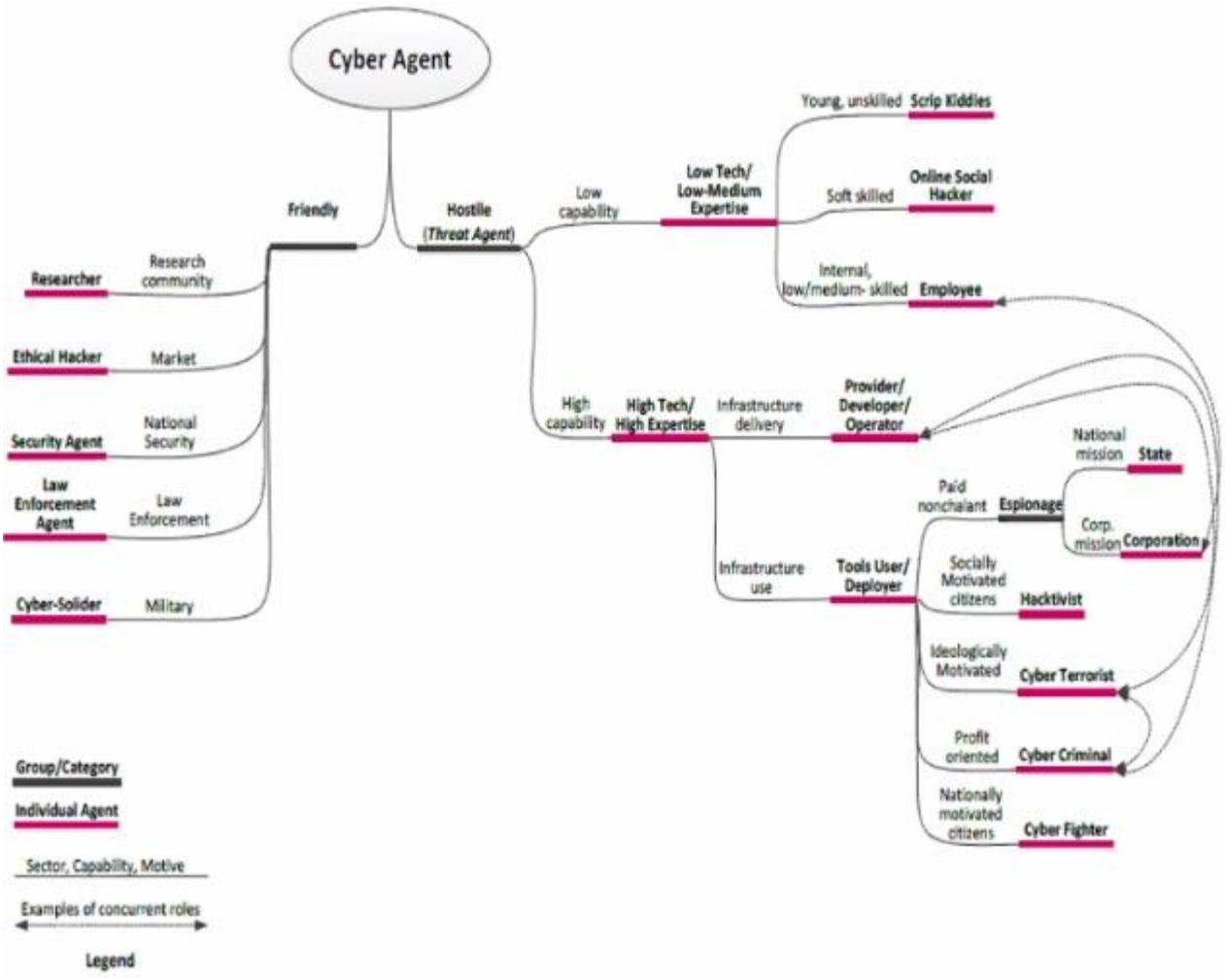


Figura 6 – Topologias de um CiberAgente

2.4.4. Sofisticação das Ameaças

As ameaças mais sofisticadas, conhecidas como APTs (Advanced Persistent Threats), têm produzido efeitos de grande dimensão, como os ataques ocorridos na Ucrânia, Estónia, Sony e TV5.

No entanto, é importante destacar que o conhecimento para lançar esses tipos de ataques não está mais restrito a apenas alguns especialistas, já que atualmente é possível comprar kits ou serviços para realizar ataques.

Nesse cenário, o Grupo EDP, por gerir infraestruturas críticas e manipular informações pessoais de milhões de clientes, é um exemplo de alvo potencial para essas ameaças sofisticadas.

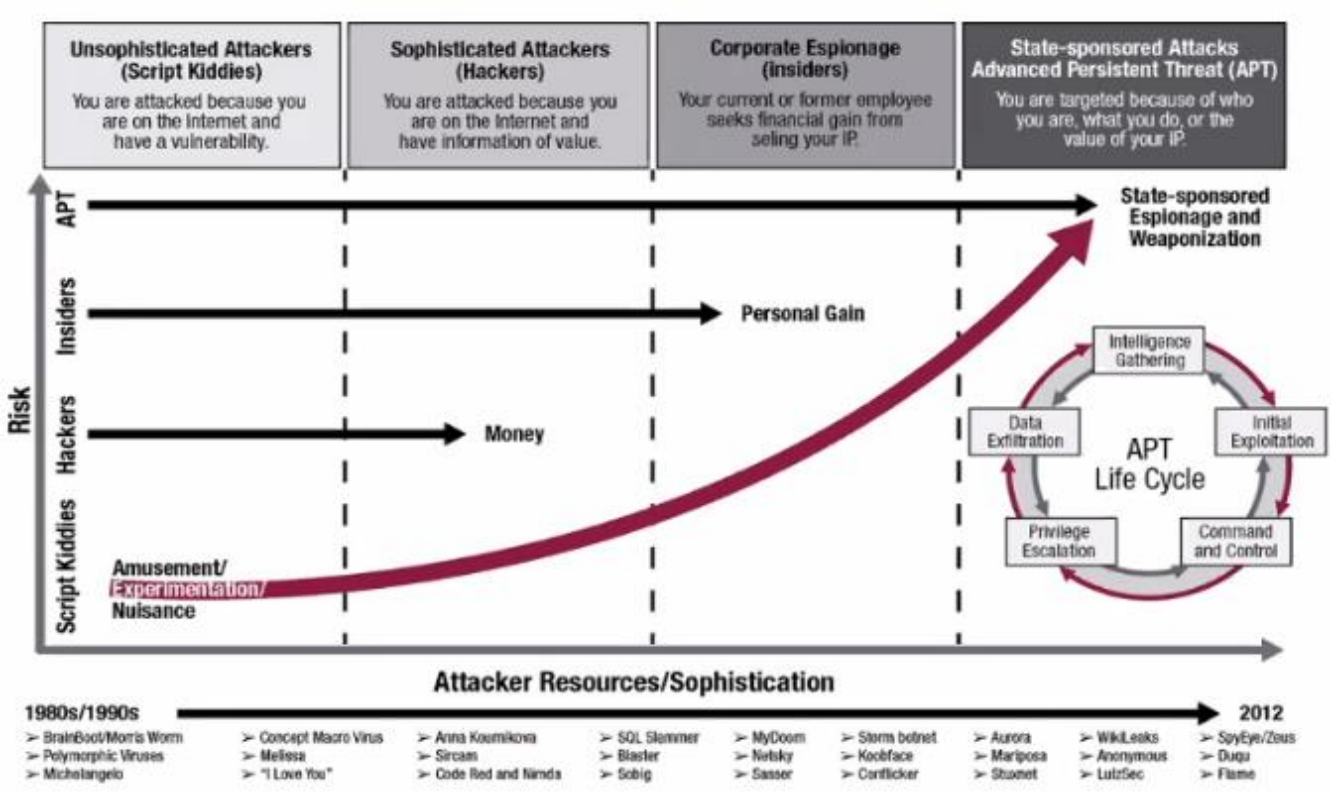


Figura 7 - Gráfico da sofisticação de ataques

2.5. Recursos

O Grupo EDP é uma empresa que possui uma grande quantidade de recursos, mas isso também a torna um alvo atraente para ciberataques. Dentre os riscos que a empresa enfrenta, destacam-se a exposição de dados pessoais de milhões de clientes, o que pode gerar grandes impactos financeiros, na imagem e na operação da empresa, bem como na sociedade como um todo.

Além disso, por gerir infraestruturas críticas, qualquer ataque pode ter um impacto fundamental na imagem e nos resultados financeiros e operacionais do Grupo EDP, e também na sociedade em geral.

As infraestruturas críticas possuem recursos que devem ser protegidos de forma específica de acordo com as leis em vigor. Isso ocorre porque, caso esses sistemas sejam comprometidos, as consequências podem ser desastrosas para a segurança nacional, a estabilidade econômica, a saúde pública, a segurança e outras áreas essenciais.

Portanto, é crucial que esses recursos sejam defendidos adequadamente para garantir o bom funcionamento das infraestruturas críticas e a segurança de seus utilizadores.

3. Análise Crítica

3.1. Presença do CiberRisco no mundo digital e tipos de vulnerabilidades

A palestra aborda vários pontos cruciais relacionados à Cibersegurança, como o conceito de CiberRisco e os tipos de vulnerabilidades existentes.

Em relação ao CiberRisco, concordo com o palestrante ao afirmar que as organizações devem fazer tudo o que estiver ao seu alcance para prevenir ocorrências deste tipo, detetar possíveis vulnerabilidades, reagir aos incidentes e recuperar do ataque. O risco no ciberespaço é uma realidade e deve ser levado a sério pelas empresas, independentemente do seu tamanho ou área de atuação.

As falhas propositadas, sistemas legados e a complexidade das arquiteturas são grandes ameaças à segurança cibernética. Configurações inadequadas e procedimentos incorretos também podem levar a vulnerabilidades. Com a transformação digital, surgem novas formas de funcionamento que aumentam os riscos de cibersegurança, exigindo maior cuidado com os equipamentos e serviços utilizados para acessar e armazenar dados empresariais.

Em resumo, a palestra apresentou uma visão clara e objetiva sobre a presença do CiberRisco no mundo convencional. As informações e exemplos apresentados foram fundamentais para demonstrar a gravidade do problema e a necessidade de medidas de prevenção, deteção, reação e recuperação de dados em caso de ciberataques.

A minha posição é de que a Cibersegurança deve ser uma prioridade para as empresas em todo o mundo, independentemente do seu tamanho ou área de atuação, e que medidas preventivas devem ser tomadas para minimizar os riscos de exposição a ciberataques.

3.2. Defesa dos recuros nas infraestruras críticas

A proteção de infraestruturas críticas é, sem dúvida, um assunto importante e cada vez mais relevante em um mundo cada vez mais conectado e dependente de tecnologia. A palestra abordou com clareza os riscos enfrentados pelo Grupo EDP, bem como os potenciais impactos financeiros, de imagem e operacionais que podem ser causados por CiberAtaques.

É fundamental que as empresas que gerenciam infraestruturas críticas, como o Grupo EDP, possuam medidas de segurança sólidas e eficazes para proteger seus recursos e utilizadores. Essas medidas devem ser estabelecidas com base em leis e regulamentações específicas para o setor e devem ser atualizadas constantemente para acompanhar as novas ameaças.

4. Considerações Finais

Em conclusão, a palestra abordou um tema de extrema importância nos dias atuais: a Cibersegurança e Proteção nas infraestruturas críticas.

Foi apresentado um panorama claro e objetivo sobre a presença do CiberRisco no mundo convencional, com destaque para a exposição de dados pessoais e os possíveis impactos financeiros, na imagem e na operação da empresa, bem como na sociedade em geral.

De acordo com a minha análise crítica, é essencial que as empresas em todo o mundo, independentemente do seu tamanho ou área de atuação, priorizem a segurança cibernética. Medidas preventivas devem ser tomadas para minimizar os riscos de ciberataques e a proteção de dados sensíveis. Além disso, é fundamental que as leis em vigor sejam aplicadas adequadamente para garantir a segurança nacional, a estabilidade econômica, a saúde pública, a segurança e outras áreas essenciais.

Portanto, concluo que a Cibersegurança deve ser uma preocupação constante de todos os setores, e é necessário investir em medidas de prevenção, detecção, reação e recuperação de dados em caso de CiberAtaques. A conscientização sobre o tema e a adoção de boas práticas são fundamentais para garantir a proteção dos recursos nas infraestruturas críticas e a segurança de toda a sociedade.

REFERÊNCIAS

Moniz, P. (2023). Palestra de Cibersegurança e Protecção de Infraestruturas Críticas.