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 Desenvolvimento De Aplicações

Unidade Curricular de Ética e Deontologia

Ano Letivo de 2019/2020

PALESTRA Nº 9

Centro Nacional de Cibersegurança, CNCS e o CSIRT Nacional – CERT.PT

Rogério Raposo

Realizada em 27 de Maio de 2020

ANÁLISE DA 9ª PALESTRA DO CICLO DE PALESTRAS "EU, NA ENGENHARIA E NA VIDA"

Daniel Moreira Ribeiro

2017013425

Coimbra, 5 de Junho de 2020

Daniel Moreira Ribeiro

Análise da 9ª palestra do ciclo de palestras “Eu, na Engenharia e na Vida”

Trabalho realizado no âmbito da avaliação da unidade curricular de Ética e Deontologia

Coimbra, 5 de Junho de 2020

Índice

Resumo

A palestra nº9 do ciclo de palestras “Eu, na Engenharia e na Vida” fala do centro nacional da cibersegurança, CNCS e o CSIRT Nacional.

É interessante perceber a importância da ética nestas organizações nacionais que protegem o nosso país.

Palavras-chave: cibersegurança, Portugal, crime, cooperação

1. Introdução

O tema abordado nesta palestra debruçou-se fundamentalmente sobre as organizações que estão no título da palestra.

O Relatório segue uma linha temática independente da linha temporal da palestra e é escrito na 1ª pessoa do singular.

Com a elaboração deste mesmo relatório espero facultar conhecimento e esclarecer alguns temas que foram transmitidos pelo palestrante.

O Relatório é composto por um resumo da conferência e a respetiva análise da minha parte.

2. Descrição do Tema Abordado na Palestra

2.1. Marcos da construção social da cibersegurança

Rogério Raposo define 5 marcos da construção social da Cibersegurança.

- O primeiro ocorreu em 1988 - Morris Worm que consistiu no mapeamento de uma rede Universitária que fez com que se espalhasse de ponta a ponta e consequentemente fez com que as organizações se apercebessem que têm que ter em atenção a cibersegurança.
- O segundo 1990 – 1998 – vírus polimórficos onde começaram a haver pessoas a explorar o ciberespaço.
- O terceiro em 2007/2008 nos ciberataques na Estónia e Geórgia onde se assiste pela primeira vez à utilização do ciberespaço como uma arma como uma demonstração de poder contra o estado.
- O quarto ocorreu em 2013 com as revelações feitas por Edward Snowden.
- O quinto ocorreu em 2018 com o escândalo da Cambridge Analytica que tem a haver com o poder de algumas informações sobre os dados e a possível manipulação de modo a influenciar por exemplo eleições presidenciais.

2.2. Discursos da cibersegurança

Segundo Rogério Raposo os discursos da cibersegurança são:

- Defesa através da soberania, mission assurance e exploração.
- Segurança Interna no combate ao cibercrime e proteção nomeadamente de infraestruturas críticas.
- Mercado através do mercado único digital, do crescimento económico e da confiança dos consumidores.
- Direitos e Liberdades através da privacidade, da liberdade de expressão e dos direitos humanos.

2.3. Conflitos na cibersegurança

As entidades devem criar pontes entre si de modo a resolver conflitos.

Os conflitos nem sempre são maus. Por vezes pode-se olhar para um conflito como forma de aprendizagem.

Ao fazer a análise aos conflitos percebemos que existe sempre um atacante com uma motivação, que utiliza uma determinada ferramenta ou técnica de modo a atingir um alvo.

É a partir desse tipo de raciocínio que se tenta descobrir a razão e o caminho do ataque informático.

Atualmente as ameaças não possuem fronteiras e os ataques podem chegar de todos os cantos do mundo.

2.4. Áreas funcionais da cibersegurança

A coordenação nacional são os bombeiros da internet segundo Rogério Raposo.

Atua na Proteção IC, Soberania, Situational Awareness, Combate Cibercrime, defesa, normas e políticas públicas, investigação (R&D), Treino e Educação, incidente response, sensibilização, cooperação (inter)nacional e cooperação público-privada.

2.5. Estrutura de governação da cibersegurança

O Centro Nacional de Cibersegurança e o Departamento de Operações CERT.PT responde ao Gabinete Nacional de Segurança que junto do Conselho Superior de Segurança do Ciberespaço responde ao Ministério da Presidência que por sua vez responde ao Primeiro-Ministro.

2.6. Ecossistema da cibersegurança

O CNCS convive num ecossistema junto do CERT.PT, UNC3T, Centro de Ciberdefesa, Intel, PGR Gabinete Cibercrime, Diplomacia, Centro Internet Segura, Reguladores Setoriais, ANPC/SSI, Exercícios, indústria, academia, ISAC Banca e Rede Nacional CSIRT.

2.7. A Cibersegurança na comunidade através da cooperação

O centro de cibersegurança trabalha sob uma perspetiva de apoio à comunidade e existe cooperação entre as várias entidades que defender a segurança na internet.

Esta cooperação existe porque geralmente quantos mais cabeças pensarem num problema, mais rapidamente esse mesmo problema pode vir a ser resolvido.

A cooperação é útil. Cabe às entidades entreajudarem-se de forma correta de modo a solucionar os problemas.

2.8. Modelos e práticas de cooperação

Normalmente as entidades aprendem umas com as outras e treinam umas com as outras de modo a melhorarem a sua prestação na resolução de problemas realmente graves.

São formados círculos de confiança que acabam por ser cruciais na troca de informação através da troca de discussão sobre um determinado assunto.

2.9. Centro Nacional de Cibersegurança (CNCS)

O centro foi estabelecido em 2014 como sendo a Autoridade Nacional de Cibersegurança.

Possui treino, sensibilização e criação de capacidades. Existem normas e regulação obrigatórias a seguir.

Há uma grande cooperação a nível nacional e internacional.

O CERT.PT é o CSIRT Nacional de jure e está na coordenação da resposta a incidentes e coordenação da gestão de vulnerabilidades e alertas.

O CNCS possui uma unidade de desenvolvimento e inovação, um departamento de operações e um departamento de serviços técnicos.

2.10. Departamento de Operações

O departamento de operações atua no panorama, na análise de informação e na coordenação da reação a incidentes no ciberespaço.

2.11. CERT.PT

O CERT:PT atua na coordenação da Resposta a Incidentes, na análise Forense, na gestão de vulnerabilidades, na cooperação (inter)nacional e na capacitação de CSIRT.

A sua missão é *"(…) implementação das medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais."* – fonte: Decree-Law Nª3/2012(16th Jan).

As entidades do estado relacionam-se com os operadores de infraestruturas críticas que por sua vez se relacionam com o ciberespaço nacional.

O CERP.PT dá atenção à coordenação resposta a incidentes de entidades do estado, Operadores IC e o ciberespaço Nacional. Tem ainda em atenção os alertas das entidades do estado, dos Operadores IC e do ciberespaço nacional. Chega ainda a dar suporte On-Site das entidades do estado e dos Operadores IC, da mesma forma que dá atenção à criação de capacidades nas entidades do estado e aos Operadores IC.

Nos dias de hoje, existe uma reação e notificação a incidentes, bem como partilha de informação desses mesmos casos muito rápida com entidades parceiras.

2.12. Desafios

Alguns dos desafios que se pões à frente da cibersegurança são a ubiquidade do domínio digital e como afeta as nossas vidas, a soberania digital e "militarização" do ciberespaço, o

“valor” dos dados, o desenvolvimento continuo do quadro jurídico, a cibersegurança enquanto Política pública e a falta de recursos humanos.

3. Análise Crítica

3.1. Marcos da construção social da cibersegurança

A cibersegurança surgiu como resposta a problemas que foram causados ao longo do tempo.

Temos que ter em atenção que ao inovar tecnologicamente, irão surgir sempre brechas nas versões mais recentes das novas novidades informáticas.

Os exemplos dados como marcos da construção social da cibersegurança são acontecimentos que de certa forma influenciaram a criação e a performance das unidades que respondem à cibersegurança.

3.2. Discursos da cibersegurança

A defesa do é um dos discursos da cibersegurança através da soberania como foi dito acima.

Também a segurança interna no combate ao cibercrime é extremamente importante e constitui um dos discursos de cibersegurança porque os dados governamentais do estado devem permanecer seguros sob vigilância 24 horas por dia.

Relativamente ao Mercado que também é um dos discursos da cibersegurança, há que ter em atenção que as transações monetárias são extremamente importantes e as entidades competentes têm que garantir o bom funcionamento deste tipo de serviços.

Por último, mas não menos importante, os direitos e liberdades através da privacidade da liberdade de expressão e dos direitos humanos não pode ser desrespeitada no ciberespaço, constituindo assim outro pilar no discurso da cibersegurança.

3.3. Conflitos na cibersegurança

Vivemos numa aldeia global e como tal as entidades têm que cooperar entre si não só para resolver conflitos internacionais, mas também para se aprenderem certas técnicas de modo a derrotar os “maus da fita” no futuro.

Cabe às entidades competentes fazer o esforço de interagir com outras unidades de modo a criar e trocar conhecimento, enriquecendo assim os escudos contra o inimigo.

Em todos os conflitos existem atacantes, podendo eles ser: criminosos, grupos apoiados por estados, script kiddies e coders.

Existem também motivações/razões por trás do ataque, podendo ser: enriquecimento financeiro, político ou religioso, interferência, reputação, vantagem estratégica, garantias de confiança e destruição.

É obvio que para o ataque se realizar também têm que existir ferramentas ou técnicas que possibilitam essa ação, das quais se destacam: ataques físicos, hacking, roubo de informação, denial of service, engenharia social, exfiltration, APT ou um trabalhador desapontado.

Por fim, é claro que para haver um ataque tem que haver um alvo, dos quais podem ser: segredos de estado, segredos de empresas, contas bancárias, negócios, informação pessoal ou infraestruturas críticas.

Ao ter em conta estas razoes e personas consegue-se apurar e direcionar o foco para a forma mais eficiente de resolução do problema.

Atualmente os ataques podem ser oriundos de qualquer lugar visto que vivemos numa aldeia global.

3.4. Áreas funcionais da cibersegurança

Há que proteger o país dos ataques informáticos diários a que é sujeito. Cabe à cooperação nacional tratar desse assunto e resolver os problemas que acontecem no dia-a-dia.

O combate ao cibercrime é extremamente importante para garantir o bom funcionamento da economia Portuguesa.

Tanto a defesa como as normas e políticas publicas são áreas funcionais da cibersegurança que têm que estar protegidas a todo o custo.

Atualmente os países têm uma dependência brutal no que toca a dados informáticos. Quem conseguir proteger os dados ganha uma guerra silenciosa que acontece no dia-a-dia.

Existe uma cooperação a nível nacional e internacional que garante a proteção através da partilha de formas de segurança eficazes para evitar ataques que podem evidentemente causar muitas consequências negativas para determinada empresa ou pessoa.

3.5. Estrutura de governação da cibersegurança

Em Portugal existe uma estrutura em forma de árvore que responde ao Primeiro Ministro. Como foi referido anteriormente o Centro Nacional de Segurança está muito próximo do Primeiro Ministro.

Na minha opinião não poderia ser de outra forma, visto que esta entidade é extremamente importante e crucial para o bom funcionamento do país tendo assim um papel relevante na política do dia-a-dia que nos é aplicada. Arrisco-me a dizer que muitas vezes o Centro Nacional de Segurança pode ser menosprezado no que toca à sua importância.

3.6. Ecossistema da cibersegurança

Existem “N” entidades que cooperam entre si. É extremamente normal isto acontecer e ocupar uma grande parte do ecossistema da cibersegurança.

É de dar os parabéns às entidades competentes por se relacionarem de forma tão saudável de modo a protegerem os Portugueses dos hackers e dos ataques maliciosos que com eles se arrastam.

3.7. A cibersegurança na comunidade através da cooperação

O apoio à comunidade não falta no centro de cibersegurança. A tão referida cooperação também é aplicada aqui de modo a solucionar os problemas que acontecem todos os dias.

A utilidade de uma cooperação saudável pode ter efeitos muito positivos na resolução e formação dos agentes de proteção da população Portuguesa.

3.8. Modelos e práticas de cooperação

Este tópico talvez seja o mais falado ao longo deste relatório. Em todos os assuntos conseguimos observar que existe uma grande cooperação em torno da resolução dos problemas existentes causados pelos ataques informáticos que acontecem ao longo do dia-a-dia em todo mundo e em especial em Portugal.

Como já foi dito, a aprendizagem parte muito da relação entre entidades que se ajudam mutuamente de modo a melhorar a sua eficácia.

Os falados círculos de confiança são um componente importante para que haja esta troca de relações e informações com fontes fidedignas e leais.

3.9. Centro Nacional de Cibersegurança (CNCS)

O Centro Nacional de Cibersegurança luta contra as ameaças do dia-a-dia provocadas pelos piratas informáticos que põe em causa os sistemas também eles informáticos das empresas e entidades que possuem nomeadamente dados que muitas vezes são valiosos e servem de extorsão, para que esse atacante possa ganhar bastante dinheiro.

O CNCS é extremamente eficiente e até à data não creio que haja um marco significativamente negativo que manche esta entidade.

3.10. Departamento de Operações

O departamento de operações espelha exatamente o sentido que é atribuído ao seu nome. Portanto, este departamento está responsável pela atuação no panorama da cibersegurança.

A análise de informação e a coordenação da reação a incidentes do ciberespaço são então conduzidas por este departamento que reflete um rigor capaz de desempenhar um trabalho excecional na área em que atua.

3.11. CERT.PT

O CERT.PT atua mais na parte da resposta a incidentes, na análise forense, na gestão das próprias vulnerabilidades e na tão falada cooperação existente na defesa do ciberespaço.

Pessoalmente, irei pesquisar mais sobre a cibersegurança porque é efetivamente algo que me poderia suscitar interesse como trabalho(emprego) no futuro.

3.12. Desafios

A ubiquidade do domínio digital é um desafio em peras. Vejamos o que o futuro nos reserva e como irá este campo evoluir.

Pessoalmente, pensa que a restrição de uso do ciberespaço deve ser feita. Se as margens de liberdade neste local forem encurtadas, haverá um espectro maior entre o inicio da navegação proibida até aos dados que se pretendem roubar, ou seja, haverá uma área restrita que fará com que seja mais fácil encontrar os atacantes devido ao longo caminho que estes têm que percorrer até chegar ao alvo do ataque.

Os dados valem bastante dinheiro. Para que se minimizem os ataques as pessoas poderiam consciencializarem-se de modo a não fabricarem enormes quantidades de dados.

A nível judicial penso que as leis terão que ser adaptadas segundo esta realidade atual. Penso que atualmente o nosso sistema judicial não respeita a exigência que é requerida pela cibersegurança, havendo certamente falhas na legislação devido a esta tecnologia ser relativamente recente bem como os perigos que nela se manifestam.

Existe falta de Engenheiros capazes de preencher os requisitos pedidos por estas entidades que protegem os cidadãos dos perigos do ciberespaço.

A meu ver, no futuro grande parte da população (se não toda) irá ter formação nesta área. Parece absurdo, mas a realidade é que a informática está cada vez mais presente no nosso dia-a-dia e a dependência que dela advém é manifestada com grande intensidade.

Cabe também ao ministério da educação fazer com que os Portugueses possam estar bem informados para as ferramentas que certamente usam e irão usar para o resto das suas vidas.

Assim como antigamente, as pessoas aprendiam na escola a trabalhar certas artes, penso que hoje é extremamente importante a geração atual aprender mais sobre a cibersegurança.

4. Considerações Finais

A palestra número 9 do ciclo de palestras “Eu, na Engenharia e na Vida” foi bastante interessante e presenteou aos alunos uma perspetiva de emprego possivelmente interessante.

Foi sem dúvida uma palestra muito enriquecedora que abriu horizontes relativamente a opções a tomar no futuro e ao ambiente que nos rodeia no mundo da informática.

Em suma, o tema relativo às entidades que protegem o ciberespaço foi extremamente enriquecedor.