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 2

A Ética e as implicações na cibersegurança

Pedro Veiga

Realizada em 1 de Abril de 2020

ANÁLISE DA 2ª 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 2ª 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 nº2 do ciclo de palestras “Eu, na Engenharia e na Vida” fala da cibersegurança e da ética que vem com ela.

É interessante perceber a importância da ética na cibersegurança que Pedro Veiga expõe com clareza.

Palavras-chave: cibersegurança, ética, dados

1. Introdução

O tema abordado nesta palestra debruçou-se fundamentalmente sobre a ética no mundo da cibersegurança.

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. Ciber ataques

Pedro Veiga começou por elogiar mostrar um roubo de 100 milhões de dólares que houve num banco no Bangladesh em 2016 em que os ladrões queriam fazer um roubo de 870 milhões de dólares que foi interrompido ao ser descoberto o crime. Depois mostrou o maior ataque de ransomware até aos dias de hoje que ocorreu numa fábrica de automóveis, um ataque que roubou emails secretos de uma empresa e um ataque que ocorreu na Equifax fazendo com que o CEO se despedisse. De seguida deu o exemplo do ataque *'make it rain'* em que ao introduzir uma pen USB num multibanco, fazia com que as notas saíssem cá para fora. Referiu que a IBM proibiu o uso de pens USB dentro da empresa, devido a serem instrumentos fáceis para roubar dados.

Pedro Veiga é contra a votação eletrónica porque acha que não há garantias de uma votação segura que garanta a identidade da pessoa, atualmente.

2.2. O termo Ciber

Segundo Pedro Veiga, a convergência tecnológica que foi feita entre Informática, (Tele)-comunicações e os media está presente em grande força nos dias de hoje.

O palestrante apontou que a cibersegurança é associada ao cibercrime e à ciberdefesa, salientando o prefixo "ciber" que está presente no dia a dia com ciberbullying, ciberfraude, etc.

O prefixo Ciber provém de um romance escrito na década de 80 chamado *"Neuromancer"* em que se utiliza o termo *"cyberspace"* , que já falava em blocos de informação a fluírem entre computadores ligados em rede.

O importante a reter no ciberespaço é informação, sistemas e redes de comunicação.

2.3. Dimensões da cibersegurança

As dimensões da cibersegurança residem na técnica e tecnologia, na política organizacional, na legalidade, na economia e no comportamento humano e psicológico.

2.4. Roubo de Informação

O roubo de informação pode subdividir-se em espionagem Industrial, espionagem estatal e espionagem militar.

A espionagem industrial espelha o roubo de propriedade industrial e intelectual. A espionagem estatal faz-se em todo o mundo e é um problema muito atual. A espionagem militar debruça-se nos sistemas de comando e controlo.

Na darkweb vendem-se dados que são roubados. Os dados de cartões de crédito segundo Pedro Veiga estão a 20 cêntimos cada um, já os dados de saúde estão a 50 dólares.

2.5. Roubo da Identidade Digital

Um dos maiores problemas atuais é o roubo da identidade digital. Isto é causado pela engenharia social na dimensão da manipulação de pessoas para obtenção de acesso às redes e aos sistemas de informação como método para cometer cibercrimes. Tudo isto é causado por mensagens de correio eletrónico, links ocultos em mensagens, links quando se visitam sites e executáveis dentro de mensagens.

2.6. Ciber-higiene

Cabe às pessoas evitar os ataques ao fazer uso da ciber-higiene. Não se deve ler mails de origem desconhecida, ter os nossos sistemas atualizados, fazer cópias de segurança., proteger sistemas com password(forte), mudar a password com frequência e ter cuidados com a segurança física.

Pedro Veiga utiliza vários telemóveis como forma de testar aplicações e de não permitir acesso a certas informações por parte aplicações não seguras.

2.7. Ética na cibersegurança

Os Engenheiros Informáticos têm um acesso quase ilimitados aos recursos (em especial à informação) da organização onde trabalho. O uso dos conhecimentos informáticos deve ser usado no estrito respeito às suas funções. Todos os intervenientes têm obrigação de proteger a informação do acesso ilegítimo (dos criminosos, dos trabalhadores da organização e dos dirigentes da organização).

2.8. Rui Pinto

Rui Pinto acabou por ter algum tempo da palestra dedicado a si. Segundo pensa Pedro Veiga, esse hacker utilizou um robot que ataca o IP indicado e tentou ainda extorsão. O palestrante acha ainda um exagero o tempo de prisão que foi imposto a Rui Pinto até à data.

À pergunta elaborada por mim que dizia “Não acha que em Portugal muitas vezes se confunde a mensagem(informação) com o mensageiro (Rui Pinto entre outros) e que muitas vezes são ignoradas provas bem importantes por conveniência? Foi um prazer assistir a esta conferência” não obtive nenhuma resposta porque não foi lida na altura, devido ao timing a que a fiz.

3. Análise Crítica

3.1. Ciber Ataques

Os ataques informáticos são algo que era impensável num passado distante. As tecnologias mudam a forma de acesso à moeda e aos dados em geral e com isto traz uma componente criminal que pode ser explorada em massa.

É importante ter a noção que quando se inova no campo tecnológico, há uma possibilidade forte de haver um desenvolvimento paralelo de métodos de utilização dessa mesma tecnologia para algo negativo.

Assim como Pedro Veiga, também eu não concordo com a votação digital visto não ser segura ao ponto de garantir a identidade do individuo que vota.

Essa forma de voto pode ser alvo de ataques sem que se note qualquer tipo de irregularidades por parte da autoridade competente que neste caso iria analisar a fidedignidade dos votos.

Acredito que no futuro a votação eletrónica seja uma opção, mas atualmente creio que seja uma ideia pouco favorável em comparação com a realidade de hoje.

Cabe aos Engenheiros criar sistemas capazes de aguentar com ataques informáticos agressivos de modo a não comprometer a informação pessoal das pessoas e das empresas. As arquiteturas dos softwares e redes desenhadas têm que ser vistas ao pormenor de modo a evitar a existência de janelas por onde possam haver fugas de informação.

O mundo cada vez mais vê-se forçado a usar tecnologias de ponta e com isso vêm os hackers atrás à procura de algo para enriquecer de maneira rápida e fácil.

É importante formar bons Engenheiros capazes de combater estes problemas de forma trivial para que as pessoas se sintam mais seguras.

3.2. O termo Ciber

A palavra ciber é uma de várias palavras que foram inventadas recentemente. A inovação dos dias de hoje provoca a necessidade da criação de certos termos para que possamos definir um objeto que nos é desconhecido à partida.

Creio que o termo ciber é usado de forma exagerada e que se utiliza com prefixo de algo que esteja diretamente ligado com o uso computacional.

Ao declarar a palavra ciber, vem-me à memoria o termo cibersegurança e ciberbullying. Tudo isto se deve ao uso excessivo dessas palavras ma sociedade atual.

A convergência tecnológica motivada pela inovação constante, fez com que todas as áreas conseguissem tornar os seus processos internos mais eficientes, provocando assim um estado de euforia em torno do prefixo ciber que se tornou uma palavra bastante usual.

3.3. Dimensões da cibersegurança

Ao falarmos de cibersegurança temos que ter em conta na técnica e tecnologia, que é adquirida no curso de Engenharia Informática e que causa grande motivação aos estudantes.

Existe também uma dimensão relativa à política organizacional em que se inclui a ética e deontologia junto da política de utilização dos sistemas. A medida da IBM referida anteriormente que proíbe o uso de Pens USB dentro da empresa para que os funcionários não roubem informação interna, encaixa nesta dimensão.

A legalidade é igualmente uma dimensão extremamente importante. Cabe aos Engenheiros informáticos não se deixarem corromper e utilizar a tecnologia para o bem. É necessário formar homens e mulheres com valores morais que sejam resistentes a vontades imorais.

A dimensão económica insere-se numa visão mais empresarial em que as empresas podem ser afetadas de forma massiva nos seus lucros. Toda esta descida dos lucros se pode dever a um ataque informático que cause posteriormente na empresa uma imagem negativa aos olhos do publico.

O comportamento humano e psicológico é extremamente importante junto das outras dimensões já referidas.

Concordo a cem por cento com Pedro Veiga relativamente às dimensões da cibersegurança.

3.4. Roubo de informação

A espionagem industrial é utilizada de forma massiva nos dias de hoje.

Cabe aos Engenheiros Informáticos proteger de forma segura os dados das empresas em que trabalho e evitar fugas de informação. A construção de sistemas robustos de difícil penetração é também uma forma eficaz de combater este tipo de problema atual.

A par da espionagem industrial, está a espionagem estatal que é igualmente utilizada de forma massiva.

Os países espiam outros países como forma de prever acontecimentos importantes que possam afetar a economia mundial. Muitas vezes os próprios estados tentam influenciar certas decisões de outros países para que haja uma mudança favorável ao seu país seja a nível político ou económico.

A nível militar também existe uma quantidade muito grande de espionagem. As tensões entre os países e o rebentamento de uma guerra são combatidas através deste tipo de espionagem. O facto de haver a flexibilidade e o conhecimento das decisões externas relativamente a algo, possibilita os governos a reagir de uma forma mais capaz a certas ações aparentemente inesperadas.

A espionagem muitas vezes serve para manter um clima controlado no mundo. Se não houvesse espionagem na Coreia do Norte, provavelmente não saberíamos metade das atrocidades que acontecem nesse pais e consequentemente o líder poderia ser ainda mais radical visto não ter tanta pressão externa por parte de todo o mundo.

Claro que fazer espionagem é algo eticamente errado, mas há que extrair algo positivo dessa ação. A espionagem faz com que muitos dos planos secretos e malvados sejam revelados, fazendo com que esses mesmos planos vão por água abaixo.

Atualmente os ataques informáticos são tão comuns e fáceis de fazer que o preço relativo às informações roubadas é bastante barato. Quem diria que um dado bancário de uma pessoa tivesse o irrisório valor de 20 cêntimos e os dados hospitalares estivessem por volta dos 50 dólares por pessoa.

Estes dados são preocupantes e apesar da tendência negativa creio que no futuro se irão encontrar métodos capazes de combater este tipo de ações.

3.5. Roubo da Identidade Digital

Nos dias de hoje o roubo de identidade digital acontece de forma extremamente frequente.

Por vezes são recebidos mails no correio eletrónico que contém informação falsa, que pode causar constrangimentos ao destinatário.

Existem mails com links ocultos que redirecionam o utilizador para locais na internet que pode por em causa o bem-estar do dispositivo ou comprometer a informação pessoal que está gravada nesse objeto.

Existem também executáveis dentro de mensagens que protagonizam efeitos semelhantes aos indicados no parágrafo acima.

No tópico anterior referi a venda de informação pessoal por valores muito pequenos. A verdade é que o roubo da identidade digital é uma preocupação que tem que se ter em conta e é uma das coisas que se deve lutar contra para que o nosso mundo se torne num lugar melhor.

A venda de informação pessoal pode ser bastante lucrativa por isso é muito difícil fazer com que estes tipos de situações acabem de repente.

Para acabar com o roubo da identidade digital, os Engenheiro responsáveis pela segurança das empresas têm que realizar uma construção de arquiteturas completamente fechadas sem brechas para explorar de modo a não haver a mínima possibilidade de hackear um sistema.

As pessoas têm que ter em atenção onde guardam a sua informação de modo a não comprometer a sua identidade digital.

3.6. Ciber-higiene

Para que sejam minimizados os ataques informáticos, há que fazer uso da ciber-higiene.

Cabe aos utilizadores evitar serem vítimas de ciber ataques.

Não se deve ler mails de origem desconhecida no correio eletrónico porque podem conter links ou executáveis maliciosos.

Devemos ter os nossos sistemas informáticos atualizados de modo a estarem preparados para combater as ameaças recentes a que podem ser sujeitos.

A realização de cópias de segurança é extremamente aconselhada às pessoas que possuam dados guardados nos seus dispositivos informáticos de modo a garantir a existência dos dados após um possível acidente com o dispositivo original que guarda as informações.

Os sistemas devem ser protegidos com passwords para que sejam de difícil acesso, fazendo com que os hackers não consigam penetrar o sistema de uma maneira trivial. É aconselhado o uso de carateres incomuns e combinações entre maiúsculas, minúsculas e números.

Deve-se mudar a password de forma regular para melhorar o nível de proteção da conta a proteger. Existem programas que podem tentar entrar numa conta ao estar constantemente a tentar combinações diferentes de senhas. Daí ser aconselhável a dica referida neste parágrafo.

A segurança física não deve ser desprezada. Aliás a segurança física é das coisas mais importantes para garantir a existência e segurança dos dados. Normalmente as grandes empresas possuem servidores que estão em edifícios extremamente seguros normalmente pertencentes a empresas de segurança que fazem a manutenção correta dos servidores.

No dia a dia podemos ter vários cuidados que nos podem ajudar a ter uma vida mais segura e livre de ataques informáticos. Pedro Veiga como foi referido utiliza três telemóveis. Isto é igualmente uma boa opção para as pessoas que não querem comprometer os dados aos hackers que existem na sociedade.

3.7. Ética na cibersegurança

Ao sermos Engenheiros Informáticos iremos acarretar grande responsabilidade na parte da ética de trabalho.

Um bom Engenheiro informático não pode ceder a chantagens que ponham em causa uma ação correta.

Em todas as profissões temos que possuir um sentido de missão e encarar a vida com os valores que nos são ensinados ao longo da juventude. Devemos usar o bom senso como forma de manifestação da nossa honra.

Na realidade um bom Engenheiro é aquele que tem honra e palavra, e que nos momentos mais frios consegue escolher a opção mais acertada apesar de por vezes ser a mais dolorosa ou inconveniente.

Os Engenheiros Informáticos possuem um uso ilimitado a recursos da organização onde trabalham. O uso dos seus conhecimentos deve ser dedicado à função a que o individuo é contratado. Não deve haver uma exploração de modo a extorquir ou prejudicar a empresa ou outra entidade qualquer.

Todos os intervenientes das empresas têm o dever de proteger o acesso ilegítimo dos dados por parte dos criminosos ou das pessoas não autorizadas para tal.

Normalmente os atacantes informáticos não possuem valores compatíveis com uma ética correta que não ponha em causa os direitos das pessoas. Esses tipos de atos merecem ser punidos devido à gravidade dos mesmos.

Após a ameaça de um ataque informático, os Engenheiros não devem reagir de forma agressiva. Devem seguir o código de conduta e realizar os possíveis para parar o ataque e minimizar os danos de modo a conseguir travar a batalha contra o pirata informático que ataca a empresa.

Todo o cidadão deve procurar aprender mais sobre a cibersegurança de modo a prevenir-se contra as ameaças do dia-a-dia fazendo uso das regras usadas no tópico acima relativo à ciber

-higiene.

3.8. Rui Pinto

O caso sensacionalista de Rui Pinto teve também lugar de destaque na palestra que nos foi presenteada.

Infelizmente as grandes instituições Portuguesas muitas vezes sofrem ataques informáticos devido a descuidos e/ou arquiteturas mal concebidas.

Neste caso Rui Pinto atacou o Sport Lisboa e Benfica que é uma Instituição com alguma relevância em Portugal.

Como foi dito anteriormente, Pedro Veiga pensa que Rui Pinto tenho usado um robot que atacou o IP a que foi ordenado atacar.

O suspeito, segundo Pedro Veiga, passou demasiado tempo na prisão por um crime que ainda estava a ser julgado. A meu ver concordo com o senhor Pedro Veiga.

À pergunta elaborada por mim relativamente à distinção entre a mensagem e o mensageiro do hack em questão, creio que haja uma pepita de verdade quando digo que por vezes as informações são ocultadas por comodidade.

Infelizmente o nosso país tem vindo a provar que por vezes fica aquém das espectativas a nível judicial. Na minha opinião acho que não se deve confundir o mensageiro com a mensagem e as provas recolhidas do hack alegadamente feito por Rui Pinto.

Cabe aos Engenheiros Informáticos abrir os olhos à população e de uma maneira legal, e só legal, mostrar a realidade do ciberespaço de modo a que as pessoas tenham noção dos perigos, dos benefícios e das coisas menos boas que possam acontecer na internet.

4. Considerações Finais

A palestra número 2 do ciclo de palestras “Eu, na Engenharia e na Vida” foi bastante interessante e presenteou aos alunos com um testemunho de um caso de sucesso do mundo da cibersegurança.

Foi sem dúvida uma palestra muito enriquecedora que abriu horizontes relativamente a opções a tomar no futuro de modo a atingir o sucesso profissional.