O PAPEL DA SEGURANÇA CIBERNÉTICA NAS SOCIEDADES TECNOLÓGICAS

Kevin Benetti de Paula Timmermann – kevintimer@gmail.com
Curso de Graduação em Engenharia Mecânica – UFSC
88030-353 – Florianópolis – SC
Mathias Hinz – mathias_hinz@hotmail.com
Curso de Graduação em Engenharia Mecânica – UFSC
88030-353 – Florianópolis – SC

Resumo: *O presente artigo tem por objetivo apresentar para estudantes e entusiastas os conceitos relacionados à segurança cibernética e discutir o panorama atual da sociedade da informação e os desafios inerentes ao desenvolvimento tecnológico. Para isso, utiliza-se da apresentação de casos reais, bem como análises estatísticas evidenciando o cenário de vulnerabilidade existente. São abordados os planos governamentais de defesa cibernética desenvolvidos em diferentes países, onde buscam acompanhar essa revolução dos meios de comunicação. A leitura do artigo e a reflexão perante tais questões fornece uma base de conhecimento para posteriores aprofundamentos no assunto e suas devidas ramificações.*

Palavras-Chave*: Segurança Cibernética, Tecnologia da Informação, Sociedade Tecnológica.*

Introdução

Com o avanço das tecnologias da informação nas sociedades tecnológicas, não estamos mais limitados por modos de armazenagem de dados meramente físicos. O acesso às informações de forma virtual, se apresenta como uma característica da democratização da tecnologia, facilitando o acesso ao conhecimento em geral. Seu impacto na sociedade pós-moderna é primordial, fazendo parte hoje em dia de praticamente todos os setores (financeiro, governamental, social, etc...), com o papel de armazenar, resgatar, transmitir e manipular dados (que junto com um contexto se tornam informação).

Porém, com esse avanço, alguns alertas começam a surgir. Esses dados passam a não ter barreiras de acesso, estando esta violação de privacidade definida apenas pelas brechas encontradas em algoritmos tecnológicos. Com a evolução do ambiente de ameaças, a proteção à elas também deve evoluir, sendo então necessária uma nova abordagem com relação a segurança cibernética.

Deve-se garantir que os usuários certos tenham acesso a nada a mais nem nada a menos que as informações que lhe foram destinadas de forma íntegra. Quando essa premissa deixa de ser verdadeira, suas consequências podem atingir magnitudes avassaladoras tanto para indivíduos quanto para corporações.

Diversos são os ataques cibernéticos que podem ser listados de grande repercussão e impacto na sociedade atual, desde os trabalhos de Alan Turing na quebra de códigos alemães que influenciaram o rumo da Guerra Mundial até o recente caso de ataque sincronizado à cerca de 100 países, no qual, por exemplo, bancos de informações de hospitais na Inglaterra foram criptografados, impossibilitando o atendimento de pacientes.

O objetivo central desse artigo é expor principalmente a jovens e estudantes de diferentes áreas a origem por trás da segurança cibernética e como/porque a sociedade em que se vive hoje é tão dependente do ramo, uma vez que tal pública alvo tem sua comunicação diária e atividades educativas realizadas majoritariamente no ambiente digital, estando muito vulnerável a ameaças cibernéticas.

Contextualização e Conceitos

Quando deu-se o surgimento dos primeiros computadores, no início do Século XX, o elemento humano se fazia menos importante diante da grandiosidade dos equipamentos existentes até então, realizando operações complexas, porém não tão elevadas como os atuais.

Com o avanço dos meios de comunicação, começam a surgir nas décadas seguintes, máquinas menores e mais sofisticadas, com seu ápice de desempenho ao final do século, com o surgimento de redes locais e longa distância. Em todos esses momentos, sobreveio sempre a importância única da informação. Esta, quando disposta na forma digital, não se resume apenas a um conjunto de bytes reunidos, mas sim a um conjunto de dados classificados e devidamente organizados de modo que um indivíduo ou uma organização possam fazer desse apanhado, uso adequado para dado objetivo.

Neste ramo da informação digital, a definição de Kevin O'Shea a respeito de ataque cibernético é a que melhor engloba a descrição feita nos modelos de segurança cibernética mais conhecidos como os Protocolos AAA e o Modelo da CIA:

> Ataque Cibernético é uma ação de computador-a-computador que debilita a confidencialidade, integridade e disponibilidade de um dispositivo digital ou das informações que nele residem. (Kevin O'Shea, 2003, ISTS, p. 6)

Dentre os responsáveis por estas ações, pode-se destacar indivíduos comuns, mercenários, ativistas, empregados e até mesmo órgãos governamentais. O pesquisador Max Kilger propôs que as motivações para ataques cibernéticos podem ser divididas entre[1]: dinheiro, ego, entretenimento, causa, entrada e status. Seus alvos podem ser visualizados na Figura 1.

[1] Uma explicação mais detalhada para cada motivação pode ser encontrada em detalhes no link http://www.networkworld.com/article/2330885/lan-wan/meeces-to-pieces.html.

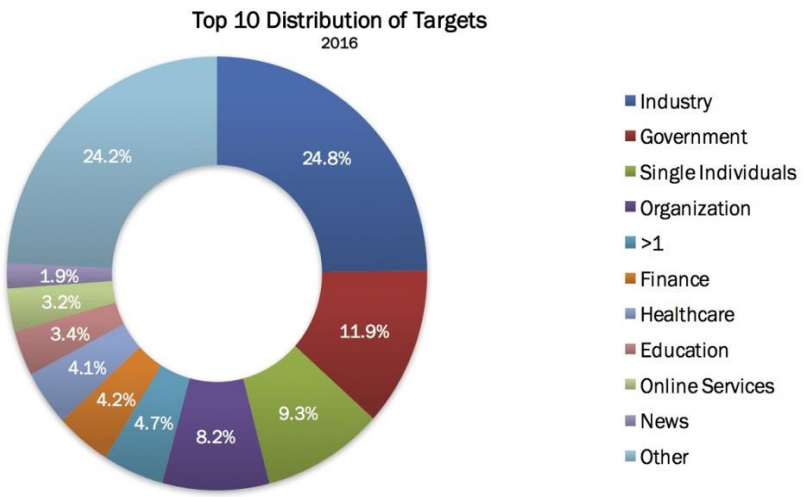

Figura 1 - Distribuição percentual de alvos no ano de 2016

Seus ataques podem ser divididos da seguinte forma:

Comprometimento do Dispositivo
Consiste em obter o controle de um determinado dispositivo sem autorização do usuário, visando a utilização do mesmo para execução de ataques mais elaborados.

Interrupção de Serviço
Tem como objetivo impedir o dispositivo alvo de executar suas funções, podendo ter como finalidade atenção pública, falha de sistemas, etc…

Extração de Dados
Visa apropriar-se de informação e dados do utilizador do dispositivo, adquirindo e muitas vezes expondo informações privadas e potencialmente confidenciais.

Infiltração
Baseia-se em submeter informações incorretas a um sistema sem ser detectado, permitindo por exemplo alterar o comportamento do dispositivo premeditadamente.

Ameaça Persistente Avançada
Procura executar ações extensivas de acesso ao dispositivo, resultando ao fim no total controle do sistema.

Pode-se então afirmar que segurança cibernética engloba todo o escopo e ações destinadas a evitar as ações descritas acima como ataques cibernéticos.

Panorama da segurança cibernética pelo mundo

Atualmente, observa-se que os contornos do espaço cibernético ainda não são definidos para os estados ao redor do planeta, dado o elevado grau de interdependência e interconectividade das redes e tecnologias de informação em termos mundiais. O assunto é recente e possui pouco aprofundamento de conhecimento até nos países com economias mais desenvolvidas. Estratégias nacionais de segurança cibernética estão sendo revisadas ou lançadas no presente momento, com uma sinalização forte do quanto há por fazer, principalmente em termos de cooperação internacional, legislação, normalização e capacitação de recursos humanos especializados. Tal fato não significa que discussões sobre o tema não vinham sendo realizadas no passado. As questões as quais diziam respeito às diretrizes, normalização e metodologias, ao longo dos últimos anos vinham sendo debatidas mundialmente, no escopo da segurança da informação e comunicações.

Pode-se citar como exemplo os Estados Unidos, o qual em 2008 lançou o documento *Securing Cyberspace for the 44th*. Já no Reino Unido a primeira estratégia nacional lançada, foi em 2009 e se denomina C*yber Security Strategy of the United Kingdom: safety, security and resilience in cyber space*. Os tópicos abordados são muito similares, dentre os principais podemos citar: Criação de uma estratégia integrada e detalhada de segurança cibernética; Organização das estruturas nacionais para a segurança cibernética; Parcerias com o setor privado; Treinamento e educação em cibernética, entre outras; Além de estar em debate no congresso estadunidense uma série de novas legislações sobre o tema.

No Brasil, acostumou-se a considerar como regra que as grandes questões latentes no planeta, sejam internalizadas com certo atraso. Porém no presente caso, isso não ocorre. Diferente dos países mais desenvolvidos, que ainda se encontram em uma fase preparatória, no país os desdobramentos da questão cibernética estão sendo acompanhadas constantemente.

Em 2008, após um ano de estudos realizados pelo Gabinete de Segurança Institucional da Presidência da República, o assunto foi apresentado na forma de uma proposta para elaboração de uma Estratégia de Segurança e de Defesa Cibernética para o País. Nessa ocasião a iniciativa foi aprovada por unanimidade na Câmara de Relações Exteriores e Defesa Nacional (Creden). Porém, embora a frente das demais nações, as medidas ainda parecem insuficientes frente a crescente de ataques no país.

Torna-se perceptível um esforço de diversos países para acompanhar essa nova realidade da sociedade globalizada, realizando grandes investimentos em capacitação humana e pesquisas de impactos socioeconômicos gerados. Porém, enquanto os governantes buscam uma ambientação a respeito do tema, o desenvolvimento de tecnologias da informação cresce exponencialmente e os ataques tornam-se cada vez mais frequentes.

História e panorama dos ataques cibernéticos pelo mundo

O avanço dos ataques cibernéticos está diretamente vinculado com evolução obtida no ramo de segurança cibernética, onde os ataques se tornam cada vez mais sofisticados à medida que seus precursores têm seus efeitos atenuados pelas medidas de segurança cibernética.

Um panorama geral pode ser visto na Figura 2, onde os primeiros casos que marcaram o surgimento de um novo tipo de ataque são descritos em sequência.

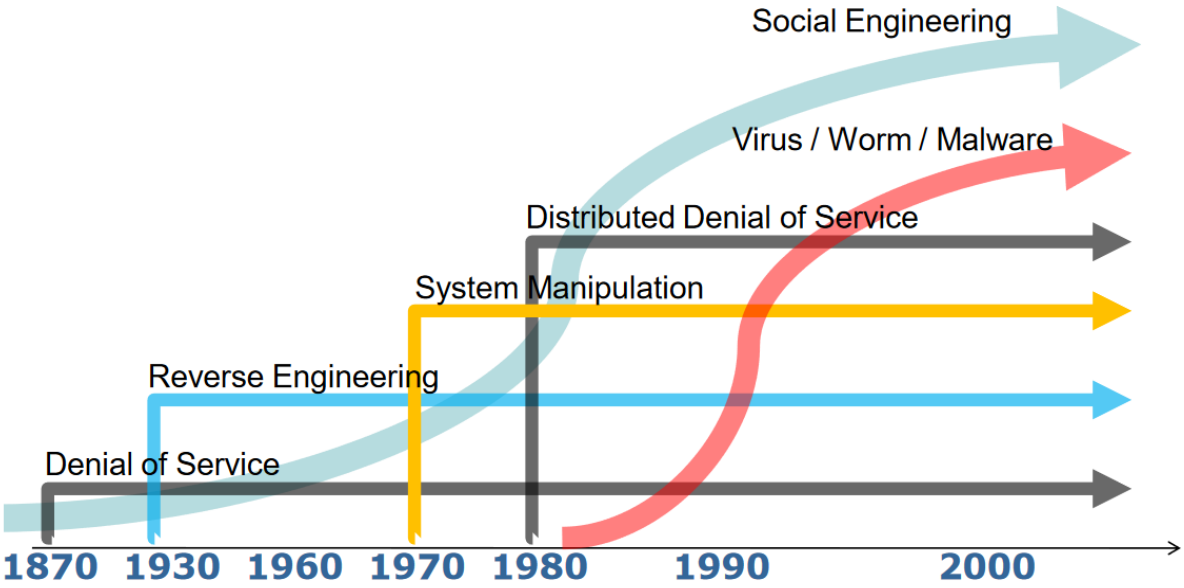

Figura 2 - Evolução dos ataques cibernéticos

(1870) Negação de Serviço - Dois adolescente americanos foram capazes de derrubar o recém implantado sistema eletrônico de telefonia americano.

(1930) Engenharia Reversa - Alan Turing e sua equipe desenvolveram uma máquina automática de decriptografia para a máquina alemã de criptografia Enigma.

(1970) Manipulação de Serviços - John Draper descobriu como realizar ligações de longa distância de graça utilizando um apito de brinquedo da empresa de cereais Cap'n Crunch. Sua descoberta foi de que o apito gerava o tom precisamente necessário para que o sistema de telefonia abrisse uma linha.

(1980) Ataque de Negação de Serviço - David Dennis, um estudante de 13 anos do ensino médio americano, derrubou os terminais do Laboratório de Educação e Pesquisa Computacional da Universidade de Illinois executando apenas um comando no sistema.

Percebe-se pelo gráfico que o grande “boom” na evolução dos ataques ocorreu a partir de 1980, onde começam a ser desenvolvidas ferramentos como virus, malware e worm, visando o maior alcance de ataques. Com o difundimento da tecnologia digital pela sociedade, o acesso ao público se tornou cada vez maior, permitindo que mais pessoas pudessem tanto atacar quanto serem atacadas de diferentes formas.

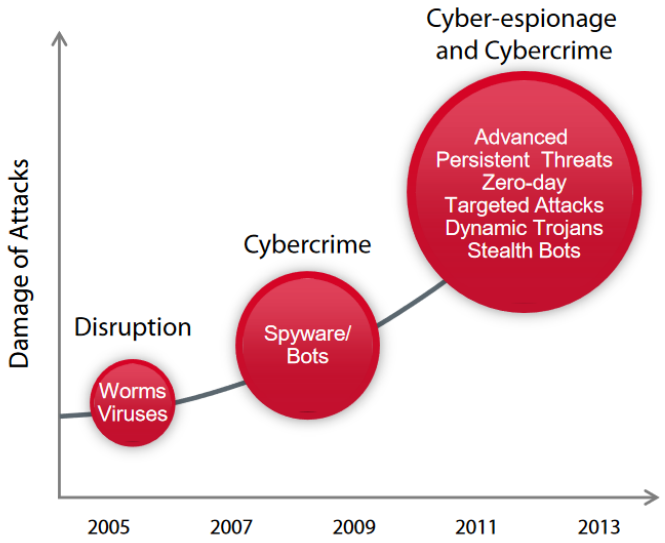

Figura 3 – Complexidade dos ataques com o tempo

Vale-se destacar os ataques que marcaram época e seus impactos. Dentre os *vírus/worms*, que eram os mais comuns pelos anos 2000 à 2005, o *worm* “Red Code” por exemplo utilizava de uma falha do sistema operacional para permitir que seu malfeitor pudesse ter controle total da máquina atacada a partir do acesso remoto.

Já pelos anos a cerca de 2009, o *botnet* começou a assumir o papel prevalecente, inicialmente com casos com o “Rustock”, onde máquinas infectadas podiam enviar mais de 25.000 mensagens de Spams por hora. Hoje em dia, tal ataque se encontra muito mais sofisticado, sendo por exemplo utilizado para infectar a rede de empresas buscando o roubo de informações.

Na atualidade, a principal preocupação das autoridade está voltada ao Ransomware. Este é um tipo de código que quando infecta o computador de um determinado usuário, criptografa todos os dados nele presente, exigindo uma recompensa para que a chave responsável pela decriptografia seja fornecida. Tal processo ainda é chamado de “sequestro de informações”.

Ele atualmente domina o mercado de ameaças digitais e é o tipo de malware mais rentável da história, sendo no ano de 2017 o responsável pelo maior ataque cibernético da história, atingindo bancos, aeroportos e hospitais de mais de 100 países.

Tal ataque leva a reflexão: até ponto a sociedade pode confiar suas tarefas ao ambiente digital? Um exemplo de tal questão trata-se dos hospitais atacados em 12 de maio de 2017, onde 16 hospitais de Londres tiveram suas atividade paralisadas, uma vez que todas as informações foram criptografadas durante o ataque, colocando em risco a vida dos pacientes tratados até que o dinheiro do sequestro de informações fosse pago.

Podemos pensar analogamente aos bancos, onde todo o dinheiro da população pode estar suscetível a ataques cibernéticos. A empresa de segurança eletrônica Kaspersky Lab estima que cerca de R$ 2,8 bilhões tenham sido roubados em ataques entre 2013 a 2015 por uma mesma quadrilha, com 30 países alvos, entre eles Rússia, Estados Unidos, Alemanha, China, Ucrânia e Canadá.

Outro ponto ainda mais preocupante são as informações pessoais as quais os hackers podem ter acesso. Seguro saúde, moradia, registros governamentais, são apenas alguns exemplos de informações armazenadas no ambiente digital que podem estar vulneráveis a ataques.

Considerações finais

Torna-se evidente uma constante preocupação com o crescimento dos ataques cibernéticos vinculadas ao desenvolvimento exponencial da tecnologia da informação. Vive-se hoje em um mundo onde o conceito de segurança da informação é questionável, visto a dificuldade e talvez impossibilidade de se estabelecer demarcações no meio virtual.

Os frequentes ataques ocorridos diariamente levam à reflexão sobre a existência da possibilidade de se garantir segurança de informação de usuários nos meios virtuais, como frequentemente é feito por instituições públicas e privadas. Medidas estão sendo tomadas e estudos estão sendo realizados em todo o planeta, porém ainda de forma embrionária, até mesmo nos países mais desenvolvidos.

Com a tendência da sociedade atual a migrar para o mundo virtual, das sociedades cibernéticas, da crescente no uso da internet, surge uma preocupação com o futuro da informação e da privacidade. Um clima de incerteza se faz presente. Segurança Cibernética se constitui de um assunto complexo e profundo, devendo a sociedade estar em constante busca do seu aprofundamento, a fim de assim, se equiparar às crescentes ameaças.

Referências Bibliográficas

LÉVY, Pierre. *Cibercultura.* Lisboa: Instituto Piaget, 1997.

BRASIL. Gabinete de Segurança Institucional da Presidência da República (GSIPR). Lei n. 10.683 de 28 de maio de 2003. Dispõe sobre a organização da Presidência da República e dos Ministérios, e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/LEIS/2003/L10.683. htm>. Acesso em: 30 junho 2017.

SAYLOR M. ***Evolution of the Cyber Attack.*** **Texas, 2011.**

INGLATERRA e EUA se aliam na Segurança Cibernética. Convergência digital, 26 jun. 2009. Disponível em: . Acesso em: 30 junho 2017.

CABINET OFFICE. Cyber security strategy of the United Kingdom: safety, security and resilience in cyber space. UK Office of Cyber Security (OCS) and UK Cyber Security Operations Centre (CSOC). UK: TSO, Jun. 2017. 25 p.

CANONGIA C.; JUNIOR R.M. ***Segurança cibernética: o desafio da nova Sociedade da Informação.*** **Brasília, 2009.**

CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES. Securing Cyberspace for the 44th. Report of the CSIS Commission on Cybersecurity for the 44th. Washington: Presidency, Jun. 2017. 88 p.

2016 Cyber Attacks Statistics, 19 de Janeiro de 2017. Disponível em: < http://www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/>. Acesso em: 30 junho 2017.