ACADEMIA MILITAR DAS AGULHAS NEGRAS

ACADEMIA REAL MILITAR (1811)

Lucas Hyppolito Gasparini

O USUÁRIO COMO O ELO MAIS FRÁGIL DA SEGURANÇA DA INFORMAÇÃO: UMA ANÁLISE PARA OS BATALHÕES DE COMUNICAÇÕES EM 2018

Resende

2018

O USUÁRIO COMO O ELO MAIS FRÁGIL DA SEGURANÇA DA INFORMAÇÃO; UMA ANÁLISE PARA OS BATALHÕES DE COMUNICAÇÕES EM 2018

Projeto de Pesquisa apresentado à Academia Militar das Agulhas Negras como parte integrante do Trabalho de Conclusão do Curso de Bacharel em Ciências Militares.

Orientador: 1º Ten COM **Miquelângelo** de Souza Dias.

COMISSÃO AVALIADORA

_____
Miquelângelo de Souza Dias 1º Ten COM – Orientador

_____
Avaliador

_____
Avaliador

Resende
2018

Ao meu pai, José Nilson, à minha mãe, Ana Maria, à minha irmã, Amanda, à minha noiva, Juliana e a todas as pessoas que me apoiaram e me incentivaram a seguir em frente nesses cinco anos de formação

AGRADECIMENTOS

Agradeço primeiramente a Deus, que me deu saúde e força para concluir a formação na Academia Militar das Agulhas Negras, ao longo de difíceis cinco anos. Agradeço também aos meus pais, José Nilson e Ana Maria, que são as grandes bases e os motivadores da minha vida, e à minha irmã, Amanda Gasparini, cujo apoio incondicional me fez seguir em frente em toda essa jornada.

Agradeço também à minha noiva Juliana pois sempre me apoiou em todas as minhas dificuldades. Ao meu orientador 1º Ten Miquelângelo, pelo suporte no escasso tempo que lhe coube, por suas correções e incentivos.

Finalmente, agradeço a todos que direta e indiretamente fizeram parte da minha formação militar e pessoal, o meu muito obrigado.

RESUMO

GASPARINI, Lucas Hyppolito. **O USUÁRIO COMO O ELO MAIS FRÁGIL DA SEGURANÇA DA INFORMAÇÃO: UMA ANÁLISE PARA OS BATALHÕES DE COMUNICAÇÕES EM 2018**. Resende: AMAN, 2018. Monografia.

O presente trabalho parte do princípio que o ser humano como qualquer outra máquina apresenta vulnerabilidades e pontos críticos, fatores estes que podem ser explorados para comprometer as atividades e missões de suas organizações, neste trabalho o Batalhão de Comunicações do Exército Brasileiro. Apresenta também as consequências dos principais erros cometidos pelo usuário apontando-o como o elo mais frágil da Segurança da Informação sob o estudo de caso de três dos maiores ataques cibernéticos da atualidade. A partir desta análise é possível evidenciar a importância da capacitação e especialização do usuário no tratamento de informações, e de segurança nacional para uma organização sensível como é o Exército Brasileiro.

Palavras chaves: Segurança da informação; erro humano; capacitação; Batalhão de Comunicações.

ABSTRACT

GASPARINI, Lucas Hyppolito. **THE USER AS THE MOST FRAGILE LINK OF INFORMATION SECURITY: AN ANALYSIS FOR THE SIGNALS BATTALIONS IN 2018**. Resende: AMAN, 2018. Monograph.

The present work assumes that the human being like any other machine presents vulnerabilities and critical points, which can be exploited to compromise the activities and missions of its organizations, in this work the Brazilian Army Signals Battalion. It also presents the consequences of the major mistakes made by the user by pointing to it as the most fragile Information Security link under the case study of three of today's biggest cyber attacks. From this analysis it is possible to highlight the importance of the training and specialization of the user in the treatment of information, and of national security for a sensitive organization such as the Brazilian Army.

Keywords: Information security; human error; training; Signals Battalion

SUMÁRIO

1. INTRODUÇÃO

O trabalho estará contido na grande área Defesa/Ciências Militares, na área 3. Cibernética, na subárea 3.1 Segurança da Informação com o tema 3.1.2 Política de Segurança da Informação.

1.1 DELIMITAÇÃO DO TEMA

A delimitação do tema ocorre à medida que passamos a analisar o comportamento humano nos recentes ataques cibernéticos ocorridos entre 2007 e o presente momento, observando as necessidades pessoais, a ganância, a tendência das pessoas a se livrarem dos problemas a qualquer custo e a ingenuidade em querer ajudar, disponibilizando a informação acarretando assim graves falhas de segurança, consequentemente demonstrando a importância da capacitação pessoal, especificamente, dentro do Exército Brasileiro, para que estes ocorridos não se repitam.

1.2 FORMULAÇÃO DO PROBLEMA

No contexto dos conflitos do século XXI e dos conflitos no amplo espectro cresceu de importância a utilização dos meios de Tecnologia de Informação e Comunicação (TIC) bem como o Comando e Controle, as decisões precisaram ser tomadas mais rapidamente, aumentando a demanda por informações rápidas e precisas. Estas informações passaram a circular nos meios informatizados e a internet tomou espaço no campo de batalha. Tais meios de fluxo de informação adquiriram valor estratégico nacional e internacional e suas vulnerabilidades passaram a ser exploradas.

Diante desses fatores formula-se o seguinte problema: **Qual a importância da capacitação pessoal dos militares para as Operações Militares do Exército Brasileiro?**

1.3 JUSTIFICATIVA

As Políticas de Segurança da Informação adotada por grandes organizações negligenciam a principal fonte de risco aos sistemas de

tecnologia: os próprios usuários, mostra estudo da Flipside, empresa responsável por eventos de cibersegurança.

> *A pesquisa mostra que 27% das violações de segurança são causadas por falha humana. "Na prática, a gente acaba vendo que o usuário é o elo mais fraco", diz Anderson Ramos (2017), diretor da companhia.*

Um comportamento de usuário específico tem gerado inúmeros problemas, e ocasionando acessos indesejados aos sistemas de segurança, trata-se da dificuldade que a maioria das pessoas encontram para memorizar senhas. Não há material literário suficiente que forneça procedimentos claros, passo a passo, que auxiliem na geração e recordação de senhas. Desta forma, os usuários são obrigados a conviver com um dilema entre a segurança e a conveniência, e acabam por compartilhar senhas ou anotá-las em locais de fácil acesso. (BROWN e colaboradores, 2004)

Conforme afirma MITNICK (2005), as organizações que continuam a usar apenas senhas estáticas precisam fornecer treinamento e lembretes ou incentivos frequentes para encorajar práticas seguras de senha. A política efetiva de senha exige que os usuários utilizem senhas seguras com, pelo menos, um numeral e um símbolo ou letras maiúsculas e minúsculas e que elas sejam alteradas periodicamente.

Outra etapa requer certificar-se de que os funcionários não terão dificuldade em memorizar a senha, anotando-a e colocando-a em seu monitor ou escondendo-a embaixo do teclado ou numa gaveta da mesa de trabalho — lugares onde qualquer ladrão de dados experiente sabe que deve procurar primeiro. A boa prática de senha também requer que nunca se use a mesma senha ou senhas parecidas em mais de um sistema (MITINICK, 2005, p. 78).

Baseado nos fatores acima citados, faz-se necessário um estudo mais abrangente e aprofundado no comportamento que os usuários adotam dentro de seus ambientes de trabalho que culminam no comprometimento de todo o sistema de segurança da informação.

1.4 QUESTÕES DE ESTUDO

A proposta do estudo consiste em analisar as características psicológicas do comportamento humano, para que seja possível verificar os aspectos mais relevantes que ocasionam vulnerabilidades no sistema e assim comprometem a segurança das informações.

A pesquisa que desenvolveremos está vinculada à premissa de que as pessoas possuem hábitos e comportamentos que acarretam em vulnerabilidades nos meios de informação e estas podem ser exploradas por pessoas mal-intencionadas. A intenção desta monografia é identificar estas características e comportamentos para que sejam tomadas atitudes eficazes a fim de combatê-las e incentivar a capacitação dos recursos humanos envolvidos nos sistemas de segurança.

Pode-se enunciar alguns comportamentos e hipóteses segundo Marcelo R. Câmara (2009) para nortear os estudos:

a) na perspectiva do usuário:

- Falta de treinamento em segurança.
- Falta de classificação de informação sob sua posse.
- Falta de reporte e resposta a incidentes.
- Distraído.
- Desinformado.
- Emocionalmente fraco.
- Bem intencionado.
- Fantasia vantagem, principalmente financeira.

1.5 OBJETIVOS

1.5.1 *OBJETIVO GERAL*

Demonstrar a importância da capacitação dos recursos humanos, principalmente no Exército Brasileiro, instituição estratégica deste país, para que seja possível a detecção, a resposta, a investigação e a prevenção de acidentes envolvendo o vazamento de informações dentro dos Batalhões de Comunicações.

1.5.2 *OBJETIVOS ESPECÍFICOS*

Analisar os principais ataques cibernéticos da atualidade, citando algumas contextualizações, técnicas e táticas utilizadas no ataque em si, evidenciando a importância da capacitação dos recursos humanos, por fim, apresentar as conclusões a respeito do ocorrido, descrevendo as possíveis soluções e procedimentos que adotados, evitariam tal acontecimento, elucidando, desta forma, a importância em capacitar recursos humanos dentro das frações no Exército Brasileiro.

A presente monografia está assim estruturada:

O primeiro capítulo apresenta alguns métodos e tipos de pesquisas utilizados nesta monografia, com algumas breves citações como forma de elucidar o caminho lógico percorrido para que os objetivos pudessem ser alcançados.

No segundo capítulo é abordado o Batalhão de Comunicações, sob a ótica do manual C-11-20, algumas considerações sobre o emprego, segurança nas operações e a utilização do comando e controle dentro do Exército Brasileiro.

Permitir-se-á, assim, contextualizar, a doutrina militar com os principais aspectos ligados a segurança da informação e a cibernética.

No terceiro capítulo são apresentadas de forma hierarquizada as ameaças humanas dentro da segurança da informação partindo das ameaças externas com os Crackers e Hackers chegando no ambiente interno com os funcionários, ex-funcionários e fornecedores contratados.

No quarto capítulo, são abordados os princípios da segurança da informação: a integridade dos dados, a disponibilidade e a confidencialidade. Estes princípios nortearão o entendimento dos ataques e defesas que os militares do Exército Brasileiro estão sujeitos dentro de um Batalhão de Comunicações.

O quinto capítulo, de acordo com o Cybersecurity Essentials, apresenta as principais técnicas e táticas utilizadas pelas ameaças internas e externas no comprometimento da informação, bem como as possíveis defesas e linhas de ação para combatê-las

O sexto capítulo trará os principais ataques cibernético que culminaram no vazamento de informações sigilosas, no caso o Flame, e o sequestro de milhares de máquinas e servidores, no caso o Wannacry. Entre as fontes de pesquisas, foram utilizados o blog da Kaspersky e as matérias dos principais jornais do mundo que relaram os acontecimentos.

O sétimo capítulo fará uma análise comentada dos ataques citados no capítulo anterior, abordando aspectos da conduta humana como a negligência e imprudência dos funcionários, que permitiram o êxito do ataque.

Por fim, diante das análises, a conclusão apresenta a importância da capacitação dos recursos humanos como forma de proteger concomitantemente com outros sistemas de segurança a informação sensível dos Batalhões de Comunicações do Exército Brasileiro.

2 PROCEDIMENTOS METODOLÓGICOS

Para a execução da pesquisa e, consequentemente, para atingir o objetivo geral da mesma é necessário a adoção de um método, que pode ser definido como:

> [...]o conjunto das atividades sistemáticas e racionais que, com maior segurança e economia, permite alcançar o objetivo - conhecimentos válidos e verdadeiros -, traçando o caminho a ser seguido, detectando erros e auxiliando as decisões do cientista. (LAKATOS; MARCONI, 2003, p.83)

‘ Para a investigação foi utilizado o método indutivo baseado no que define Cervo (1973) a Indução é um processo mental por intermédio do qual, partindo de dados particulares, suficientemente constatados, infere-se uma verdade geral ou universal, não contida nas partes examinadas. Portanto, o objetivo dos argumentos indutivos é levar a conclusões cujo conteúdo é muito mais amplo do que o das premissas nas quais se basearam.

2.1 Tipos de pesquisas realizadas

A pesquisa realizada foi principalmente bibliográfica buscando-se diversos artigos e livros que abordassem o tema da segurança de redes visando acúmulo de conhecimento técnico para desenvolvimento das teorias da metodologia adotada. Ao mesmo tempo da pesquisa bibliográfica foi realizado um curso na Plataforma de Ensino Cisco, o Cybersecurity Essentials,

para um melhor aprofundamento e entendimento dos conceitos técnicos, possibilitando uma grande quantidade de material para uso referencial.

Foi realizada, de maneira concomitante à pesquisa bibliográfica, um estudo de caso com objetivo de identificar os principais fatores que possibilitaram o comprometimento da segurança da informação nos recentes ataques cibernéticos

2.1.1 Técnicas de Pesquisa

A pesquisa foi realizada através diversas técnicas de maneira sucessivas. Inicialmente, foi realizada uma revisão de literatura com objetivo de selecionar as fontes que poderiam ser utilizadas no decorrer da execução desta monografia. Em seguida foi utilizada a técnica de pesquisa exploratória para que fossem levantados os possíveis problemas e falhas técnicas que pudessem comprometer um Batalhão de Comunicações do Exército Brasileiro deste modo, pôde ser possível realizar um comparativo com os principais ataques cibernéticos da atualidade a fim de apresentar uma possível linha de ação para o tratamento dos fatores críticos descobertos.

3 O Batalhão de Comunicações

Segundo o manual de Campanha C -11- 20, o Batalhão de Comunicações tem por missão instalar, explorar e manter a estrutura de Comunicações que dê suporte às necessidades dos sistemas operacionais do Grande Comando (G Cmdo) enquadrante, realizando a integração de meios e processos necessários ao pleno funcionamento do sistema operacional e Comando e Controle (C2).

Dentro das atribuições citadas acima, faz-se necessário um melhor conhecimento do Sistemas de Comando e Controle.

3.1 O emprego

O mesmo manual cita o que o avanço tecnológico impõe a necessidade de constantes evoluções doutrinárias com reflexos na concepção de emprego do material e na estrutura de pessoal, de forma a bem atender às características específicas de cada missão.

Ainda no contexto do emprego das Comunicações (Com), o Batalhão de Comunicações (B Com) é a unidade (U) onde se concentra o maior volume de meios em pessoal e material, os quais, por constituição, possibilitam cumprir os mais variados tipos de missões. O seu emprego deve estar voltado para atender, com eficiência e eficácia, às diversas missões balizadas pelos parâmetros doutrinários vigentes.

Diante de tais características, nas quias o B Com se encontra: grande volume de materiais e pessoal e ao sigilo das informações processadas e armazenadas a segurança da informação deve ser levada como um fator primordial para o sucesso das atividades.

3.2 A segurança nas operações

A segurança inclui as medidas tomadas por um comando para proteger a unidade da espionagem, sabotagem, observação, inquietação ou ataques surpresa. Podendo ser ativas ou passivas.

As medidas passivas incluem a observação, cobertura, dispersão, camuflagem, o aproveitamento do terreno e medidas de proteção eletrônica (MPE).

As medidas ativas envolvem o poder de fogo e o emprego de tropa. O B Com, normalmente, emprega uma combinação de medidas ativas e passivas.

A possibilidade de atuação do inimigo deve ser sempre considerada, quer por sua presença, física e/ou no espectro eletromagnético, quer pelo alcance de suas armas, causando danos a pessoal, material e aos sistemas de comunicações. Tal consideração, entretanto, não deve implicar predominância de uma mentalidade defensiva.

3.3 Comando e Controle

Dentro dos sistemas operacionais que compõe o Comando e Controle faz se necessário algumas considerações acerca da segurança da informação, esta, de fundamental importância para o processamento de informação e sigilo das operações militares.

O Sistema Operacional Comando e Controle (C2) permite aos comandantes de todos os escalões visualizar o campo de batalha, apreender a situação e dirigir as ações militares à vitória.

Ainda de acordo com o manual, o C2 permite ao comandante tático o acesso às informações disponíveis e necessárias à decisão e ao controle das operações. Desta maneira, este sistema integra os demais sistemas operacionais, valendo-se para isso, da infraestrutura de comunicações e informática (telemática) instalada ou apropriada.

3.4 Guerra Centrada em Redes

Devido as características e definição das Guerras Centradas em Rede (GCR), presentes no manual MD31 - M-03 a Guerra Centrada em Redes é uma forma de atuar na guerra com a visão específica oriunda da era da informação. Caracteriza-se pelo estabelecimento de um ambiente de compartilhamento da consciência situacional, de modo a contribuir para a obtenção da Superioridade de Informação e da iniciativa, mesmo que as peças de manobra estejam dispersas geograficamente.

A GCR enfoca o espaço de batalha como uma rede integrada e escalonada em outras redes, concorrendo para aumentar a mobilidade das peças de manobra, a coordenação entre elas e a utilização do conhecimento mútuo.

A GCR não mudará a essência da guerra e não substituirá a força militar em si. O efeito desejado é o incremento relativo do poder de combate em relação ao oponente, aumentando a rapidez nas decisões e na identificação de alvos, a precisão das armas e a letalidade dos ataques.

Devido a estes fatores O B Com deverá estar sempre preocupado com as medidas de proteção dos seus sistemas táticos de Comando e Controle (C2) e de informação, fundamentando ainda mais a necessidade deste trabalho, com o intuito de apresentar quais as principais vulnerabilidades e riscos que as Operações do Batalhão de Comunicações estão suscetíveis.

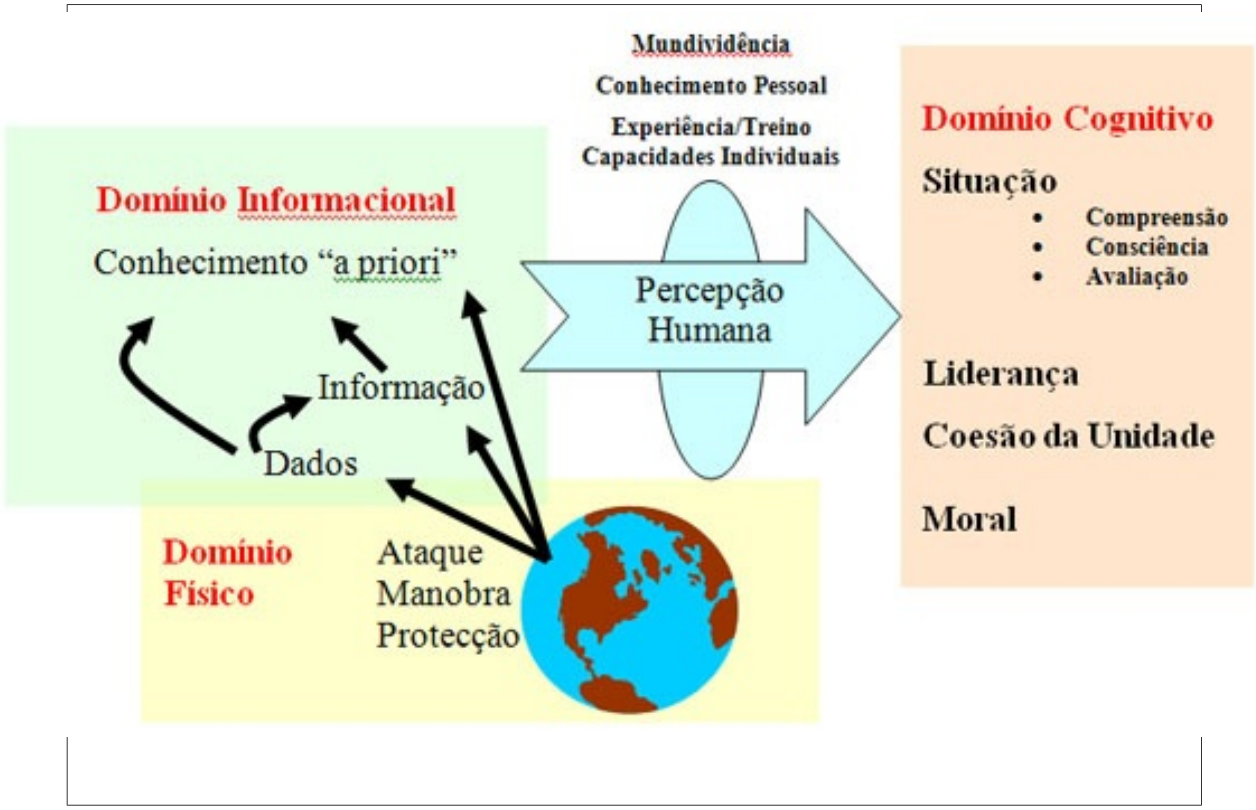

Figura 1: Os domínios da Guerra Centrada em Redes

4 AS AMEAÇAS

Este capítulo começa por explicar e apresentar algumas das principais ameaças da atualidade de acordo com o Curso Cybersecurity Essentials que podem comprometer o Batalhão de Comunicações do Exército Brasileiro.

Sun Tzu foi um filósofo e guerreiro chinês no século 6 a.C. Sun Tzu escreveu o livro intitulado *A arte da guerra,* que é um trabalho clássico sobre as estratégias disponíveis para derrotar o inimigo. Seu livro tem orientado estrategistas há décadas. Um dos princípios orientadores de Sun Tzu foi conhecer seu adversário. Embora ele se referisse especificamente à guerra, muitos dos seus conselhos podem ser levados a outros aspectos da vida, incluindo os desafios de segurança da informação.

4.1 Os criminosos virtuais

Nos primeiros anos do mundo da segurança cibernética, os típicos criminosos virtuais eram adolescentes ou amadores que operavam a partir de um PC em casa, com os ataques, na maior parte, limitados a brincadeiras e

vandalismo. Hoje, o mundo dos criminosos virtuais tornou-se mais perigoso. Os invasores são indivíduos ou grupos que tentam explorar vulnerabilidades para ganho pessoal ou financeiro. Os criminosos virtuais estão interessados em tudo, de cartões de crédito a projetos de produtos e qualquer coisa com valor.

4.1.1 Os amadores

Amadores, ou os hackers inexperientes, têm pouca ou nenhuma qualificação profissional, muitas vezes usando ferramentas existentes ou instruções encontradas na Internet para lançar ataques. Alguns são apenas curiosos, enquanto outros tentam demonstrar suas qualificações profissionais e causar danos. Eles podem estar usando ferramentas básicas, mas os resultados ainda podem ser devastadores.

4.1.2 Hackers

Esse grupo de criminosos invade computadores ou redes para obter acesso por vários motivos. A intenção da invasão determina a classificação destes invasores como hackers “do bem” (white hacker), suspeitos (gray hacker) ou “do mal” (black hacker). Os invasores “do bem” invadem redes ou sistemas de computador para descobrir fraquezas a fim de melhorar a segurança desses sistemas. Os proprietários do sistema dão permissão para executar a invasão e recebem os resultados do teste. Por outro lado, os invasores “do mal” aproveitam qualquer vulnerabilidade para ganho pessoal, financeiro ou ganho político. Os invasores suspeitos situam-se entre os invasores “do bem” e os invasores “do mal”. Os invasores suspeitos podem encontrar uma vulnerabilidade e relatá-la para os proprietários do sistema, se essa ação coincidir com sua agenda. Alguns hackers gray hat (suspeitos) publicam os fatos sobre a vulnerabilidade na Internet, para que outros invasores possam explorá-la.

4.1.3 Hackers organizados

Esses criminosos incluem empresas de hacktivistas, criminosos virtuais, terroristas e os hackers patrocinados pelo Estado. Os criminosos virtuais geralmente são grupos de criminosos profissionais, focados em controle, poder e riqueza. Os criminosos são altamente sofisticados e organizados e ainda podem proporcionar o crime digital como um serviço. Os hacktivistas fazem declarações políticas para sensibilizar para questões que são importantes para eles. Os hacktivistas publicam publicamente informações embaraçosas sobre suas vítimas. Os invasores patrocinados pelo estado reúnem informações ou cometem sabotagem em nome de seu governo. Esses invasores são geralmente altamente treinados e bem financiados. Seus ataques se concentram em objetivos específicos que são benéficos para o seu governo. Alguns atacantes patrocinados pelo estado são, até mesmo, membros das forças armadas de seus países

4.2 Tipos de meaças

Existem diferentes tipos de ameças que podem comprometer as missões desempenhadas pelo Batalhão de Comunicações de acordo com o Curso Cybersecurity Essentials da CISCO.

4.2.1 Ameaças à segurança interna

Os ataques podem se originar de dentro de uma organização ou de fora da organização. Um usuário interno, como um funcionário ou parceiro de contrato, pode, de forma acidental ou intencional:

- Tratar erroneamente os dados confidenciais

- Ameaçar as operações de servidores internos ou de dispositivos de infraestrutura de rede

- Facilitar ataques externos conectando mídias USB infectadas no sistema de computador corporativo

- Convidar acidentalmente um malware para a rede por e-mail ou sites mal-intencionados

Ameaças internas têm o potencial de causar maior dano que as ameaças externas, pois os usuários internos têm acesso direto ao edifício e a seus dispositivos de infraestrutura. Os invasores internos normalmente têm conhecimento da rede corporativa, de seus recursos e de seus dados confidenciais. Eles também podem ter conhecimento de contramedidas de segurança, políticas e níveis mais altos de privilégios administrativos.

4.2.2 Ameaças à segurança externa

Ameaças externas de amadores ou invasores habilidosos podem explorar vulnerabilidades em dispositivos conectados em rede ou podem usar engenharia social, como enganações, para ter acesso. Ataques externos exploram fraquezas ou vulnerabilidades para obter acesso a recursos externos.

5. SEGURANÇA DA INFORMAÇÃO

Este capítulo analisa os ataques mais comuns à segurança da informação que poderão comprometer a Continuidade, a Disponibilidade e a Integridade dos sistemas do Batalhão de Comunicações.

As ameaças, as vulnerabilidades e os ataques são o foco central dos profissionais da segurança da informação:

- Uma ameaça é a possibilidade de ocorrer um evento prejudicial, como um ataque.

- Uma vulnerabilidade é uma fraqueza que torna um alvo suscetível ao ataque.

- Um ataque é a exploração deliberada de uma fraqueza descoberta em sistemas informatizados, como alvos específicos ou meramente como alvos de oportunidade

Antes de apresentar os ataques que os invasores citados no capítulo 4 podem realizar, faz-se necessário o conhecimento dos Princípios da Segurança da Informação. Segundo o curso Cybersecurity Essentials da CISCO, os princípios apresentam-se com as seguintes definições:

5.1 O princípio da Confidencialidade

A confidencialidade impede a divulgação de informações para pessoas, recursos ou processos não autorizados. Um outro termo para confidencialidade é privacidade. As empresas restringem o acesso para garantir que apenas os operadores autorizados possam usar dados ou outros recursos de rede. Por exemplo, um programador não deve ter acesso às informações pessoais de todos os funcionários.

As empresas precisam treinar os funcionários sobre as melhores práticas para proteção de informações confidenciais, para se protegerem e também à organização, contra-ataques. Os métodos usados para garantir a confidencialidade incluem criptografia, autenticação e controle de acesso aos dados.

5.2 O Princípio da Integridade de dados

A integridade é a precisão, a consistência e a confiabilidade dos dados durante todo o seu ciclo de vida. Um outro termo para integridade é qualidade. Os dados passam por várias operações, como captura, armazenamento, recuperação, atualização e transferência. Os dados devem permanecer inalterados durante todas essas operações por entidades não autorizadas.

Os métodos usados para garantir a integridade de dados incluem *hashing*, verificações de validação de dados, verificações de consistência dos dados e controles de acesso. Sistemas de integridade de dados podem incluir um ou mais dos métodos listados acima.

5.3 O Princípio da Disponibilidade

A disponibilidade dos dados é o princípio usado para descrever a necessidade de manter a disponibilidade dos sistemas e serviços de informação o tempo todo. Ataques cibernéticos e falhas do sistema podem impedir o acesso a sistemas e serviços de informação. Por exemplo, a interrupção da disponibilidade do site de um concorrente por causa de um ataque pode proporcionar uma vantagem para seu rival. Ataques DoS (Denial-of-service, Negação de serviço) ameaçam a disponibilidade do sistema e impedem que usuários legítimos acessem e usem os sistemas de informações, quando necessário.

Os métodos usados para garantir a disponibilidade incluem a redundância do sistema, backups do sistema, maior resiliência do sistema, manutenção de equipamentos, sistemas operacionais e software atualizados e planos para recuperação rápida de desastres não previstos.

6 ATAQUES E DEFESAS

Os profissionais de segurança cibernética devem compreender como funciona cada ataque, o que explora e como afeta a vítima. O capítulo começa explicando, de acordo com o curso Cybersecurity Essentials, a ameaça de códigos maliciosos e malwares junto com os tipos de disfarces envolvidos na engenharia social, logo depois serão abordadas algumas técnicas de defesa e prevenção que poderão ser adotadas nos Batalhões de Comunicações como medidas preventivas ou corretivas.

6.1 Os ataques

Um ataque cibernético é qualquer tipo de manobra ofensiva usada por criminosos virtuais contra alvos como sistemas informatizados, redes de computadores ou outros dispositivos de computador. Os cibercriminosos iniciam manobras ofensivas contra redes com e sem fio.

6.1.1 Malwares

Software mal-intencionado ou malware é um termo usado para descrever o software desenvolvido para interromper as operações do computador ou obter acesso a sistemas informatizados, sem o conhecimento ou permissão do usuário. Malware tornou-se um termo genérico usado para

descrever todos os tipos de softwares hostis ou invasores. O termo malware inclui vírus de computador, worms, cavalos de Troia, ransomware, spyware, adware, scareware e outros programas mal-intencionados. O malware pode ser óbvio e simples de identificar ou pode ser muito furtivo e quase impossível de detectar.

6.1.2 Vírus, worms e cavalos de troia

Os criminosos virtuais miram os dispositivos finais do usuário por meio da instalação do malware.

6.1.2.1 Vírus

Um vírus é um código malicioso executável que está anexado a outro arquivo executável, como um programa legítimo. A maioria dos vírus necessitam de inicialização do usuário final e podem ser ativados a uma hora ou data específica. Os vírus de computador geralmente são transmitidos através de uma das três formas: de mídia removível; de downloads na Internet; e de anexos de e-mail. Os vírus podem ser inofensivos e apenas exibir uma imagem ou podem ser destrutivos, como os que modificam ou excluem dados. Para evitar a detecção, o vírus sofre mutação. O simples ato de abrir um arquivo pode ativar um vírus. Um setor de *boot*, ou vírus de sistema de arquivo, infecta pendrives USB e podem ser transmitidos para o disco de rígido do sistema. A execução de um programa específico pode ativar um vírus de programa. Uma vez ativo, o vírus de programa normalmente afetará outros programas no computador ou outros computadores na rede. O vírus Melissa foi um exemplo de transmissão de vírus por e-mail. O vírus Melissa afetou dezenas de milhares de usuários e causou uma estimativa de US$ 1,2 bilhão em danos.

6.1.2.2 *Worms*

Worms é um código malicioso que se replica ao explorar de forma independente vulnerabilidades em redes. Os *worms* normalmente deixam a rede mais lenta. Enquanto um vírus requer um programa do *host* para execução, os *worms* podem ser executados se modo autônomo. Exceto pela infecção inicial, os *worms* não necessitam mais da participação do usuário. Após afetar o *host*, um *worm* é pode ser transmitido muito rapidamente pela rede. *Worms* compartilham padrões similares. Todos eles têm habilitam uma vulnerabilidade, uma maneira de se propagar, e todos eles contêm uma carga.

Os *worms* são responsáveis por alguns dos ataques mais devastadores na Internet. Por exemplo, em 2001, o *worm* Code Red infectou 658 servidores. Em 19 horas, o worm infectou mais de 300.000 servidores.

6.1.2.3 Cavalo de troia

Um cavalo de Troia é um malware que realiza operações mal-intencionadas, sob o pretexto de uma operação desejada, como jogar um game online. Esse código malicioso explora os privilégios do usuário que o executa. Um cavalo de Troia difere de um vírus porque o cavalo de Troia se liga a arquivos não executáveis, como arquivos de imagem, arquivos de áudio ou jogos.

6.1.3 Bombas lógicas

Uma bomba lógica é um programa mal-intencionado que utiliza um gatilho para ativar o código malicioso. Por exemplo, os acionadores podem ser datas, horas, outros programas em execução ou a exclusão de uma conta de usuário. A bomba lógica permanece inativa até que o evento acionador aconteça. Assim que ativada, a bomba lógica implementa um código malicioso que danifica um computador. Uma bomba lógica pode sabotar os registros de banco de dados, apagar arquivos e atacar sistemas operacionais ou aplicativos. Recentemente, especialistas em segurança digital descobriram bombas lógicas que atacam e destroem os componentes de hardware em uma

estação de trabalho ou servidor, incluindo as ventoinhas, CPU, memória, discos rígidos e fontes de alimentação. A bomba lógica sobrecarrega esses dispositivos até o superaquecimento ou falha.

6.1.4 Ransomware

O ransomware aprisiona um sistema de computador ou os dados nele encontrados até que a vítima faça um pagamento. O ransomware normalmente funciona criptografando os dados no computador com uma chave desconhecida ao usuário. O usuário deve pagar um resgate aos criminosos para remover a restrição.

Outras versões do ransomware podem lançar mão das vulnerabilidades de sistemas específicos para bloquear o sistema. O ransomware se propaga como um cavalo de Troia e resulta de um arquivo baixado ou de um ponto fraco no software.

A meta do criminoso é sempre o pagamento através de um sistema de pagamento indetectável. Depois que a vítima efetua o pagamento, o criminoso fornece um programa que descriptografa os arquivos ou envia um código de desbloqueio.

6.1.5 Backdoors e Rootkits

6.1.5.1 Backdoor

Um backdoor refere-se ao programa ou código lançado por um criminoso que comprometeu um sistema. O backdoor ignora a autenticação usada para acessar o sistema. Alguns programas comuns de backdoor são o Netbus e Back Orifice, que permitem o acesso remoto a usuários do sistema não autorizados. A finalidade do backdoor é conceder aos criminosos virtuais o acesso futuro ao sistema, mesmo se a empresa corrigir a vulnerabilidade original usada para atacar o sistema. Em geral, os criminosos fazem com que

usuários autorizados executem inconscientemente um programa Cavalo de Troia na máquina, para instalar um backdoor.

6.1.5.2 Rootkit

Um rootkit modifica o sistema operacional para criar um backdoor. Os invasores usam o backdoor para acessar o computador remotamente. A maioria dos rootkits utiliza as vulnerabilidades do software para escalonar privilégios e modificar arquivos de sistema. O escalonamento de privilégios utiliza os erros de programação ou falhas de projeto para conceder o acesso criminoso aos recursos e dados da rede. Também é comum os rootkits modificarem a computação forense do sistema e as ferramentas de monitoramento, o que os torna muito difíceis de ser detectados. Muitas vezes, um usuário deve apagar e reinstalar o sistema operacional de um computador infectado por um rootkit.

6.1.6 Spam

O e-mail é um serviço universal usado por bilhões de pessoas em todo o mundo. Como um dos serviços mais populares, o e-mail se tornou uma grande vulnerabilidade para usuários e organizações. Spam, também conhecido como lixo eletrônico, é e-mail não solicitado, nem autorizado. Na maioria dos casos, o spam é um método de anúncio. Entretanto, o spam pode enviar links perigosos, malware ou conteúdo enganoso. O objetivo final é obter informações confidenciais, como o número na previdência social ou informações da conta no banco. A maioria dos spam vem de vários computadores em redes infectadas por um vírus ou *worm*. Esses computadores infectados enviam o máximo de lixo eletrônico possível.

6.1.7 Spywares, Adwares e Scarewares

6.1.7.1 Spywares

Spyware é o software que permite que um criminoso obtenha informações sobre as atividades do computador do usuário. O spyware frequentemente inclui rastreadores de atividade, coleta de toque de tela e captura de dados. Para tentar combater as medidas de segurança, o spyware quase sempre modifica as configurações de segurança. Muitas vezes, o spyware se junta ao software legítimo ou a cavalos de Troia. Muitos sites de shareware estão cheios de spyware.

6.1.7.2 Adwares

Normalmente, o adware exibe pop-ups irritantes para gerar receita para seus autores. O malware pode analisar os interesses do usuário rastreando os sites visitados. Em seguida, ele pode enviar anúncios pop-ups relacionados a esses sites. Algumas versões do software instalam Adware automaticamente. Alguns tipos de adware só oferecem anúncios, mas também é comum que o adware venha com spyware.

6.1.7.3 Scarewares

O scareware persuade o usuário a executar uma ação específica por medo. O scareware simula janelas pop-up que se assemelham às janelas de diálogo do sistema operacional. Essas janelas transmitem mensagens falsificadas que afirmam que o sistema está em risco ou precisa da execução de um programa específico para retornar à operação normal. Na verdade, não há problemas e, se o usuário concordar e permitir a execução do programa mencionado, o malware infectará o sistema.

6.1.8 Phishing

Phishing é uma forma de fraude. Os criminosos virtuais usam e-mail, mensagem instantânea ou outras mídias sociais para coletar informações, como credenciais de logon ou informações da conta, ao colocar uma fachada de entidade ou pessoa confiável. O phishing ocorre quando uma parte mal-

intencionada envia um e-mail fraudulento disfarçado de uma fonte legítima e confiável. A intenção da mensagem é enganar o destinatário para instalar o malware no dispositivo dele ou compartilhar informações pessoais ou financeiras. Um exemplo de phishing é um e-mail falsificado para parecer que veio de uma loja de varejo, solicitando que o usuário clique em um link para receber um prêmio. O link pode ir para um site falso que pede informações pessoais ou pode instalar um vírus.

Spear phishing é um ataque de *phishing* altamente direcionado. Embora o *phishing* e o *spear phishing* usem e-mails para alcançar as vítimas, o *spear phishing* envia e-mails personalizados a uma pessoa específica. O criminoso pesquisas os interesses da vítima antes de enviar o e-mail. Por exemplo, um criminoso descobre que a vítima está interessada em carros, procurando um modelo específico de carro para comprar. O criminoso entra no mesmo fórum de discussão de carros utilizado pela vítima, forja uma oferta de venda de carro e envia um e-mail para o alvo. O e-mail contém um link para as fotos do carro. Ao clicar no link, a vítima instala inconscientemente o malware no computador.

6.1.9 Plugins

Os plugins Flash e Shockwave da Adobe permitem a criação de animações gráficas e desenhos interessantes que melhoram muito o visual de uma página da Web. Os plugins exibem o conteúdo desenvolvido usando o software apropriado.

Até pouco tempo, os plugins tinham um registro de segurança considerável. À medida que o conteúdo baseado em Flash cresceu e se tornou mais popular, os criminosos examinaram os plugins e softwares Flash, determinaram vulnerabilidades e exploraram o Flash Player. A exploração com sucesso pode causar uma falha no sistema ou permitir que um criminoso assuma o controle do sistema afetado. Espera-se um aumento nas perdas de

dados à medida que os criminosos continuem analisando as vulnerabilidades dos plugins e protocolos mais populares.

6.1.10 Engenharia social

Engenharia social é um meio totalmente não técnico de um criminoso coletar informações sobre a vítima. Engenharia social é um ataque que tenta manipular indivíduos para realizar ações ou divulgar informações confidenciais.

Os engenheiros sociais frequentemente dependem da boa vontade das pessoas para ajuda, mas também miram nos pontos fracos. Por exemplo, um invasor pode chamar um funcionário autorizado com um problema urgente, que requer acesso imediato à rede. O invasor pode recorrer à vaidade do funcionário, valer-se de autoridade usando técnicas que citam nomes ou apelar para a ganância do funcionário.

Há alguns tipos de ataques de Engenharia social:

6.1.10.1 Pretexting

Ocorre quando um invasor chama uma pessoa e mente para ela na tentativa de obter acesso a dados confidenciais. Um exemplo envolve um invasor que finge precisar de dados pessoais ou financeiros para confirmar a identidade do destinatário.

6.1.10.2 Something for Something (Quid pro quo)

Ocorre quando um invasor solicita informações pessoais de uma pessoa em troca de algo, como um presente.

Táticas de Engenharia social

Engenheiros sociais utilizam várias táticas. As táticas de engenharia social incluem:

- Autoridade – As pessoas são mais propensas a cooperar quando instruídas por "uma autoridade"
- Intimidação – Os criminosos intimidam a vítima a realizar uma ação
- Consenso/prova social – As pessoas realizarão essa ação se acharem que as outras pessoas aprovarão
- Escassez – As pessoas realizarão essa ação se acharem que existe uma quantidade limitada
- Urgência – As pessoas realizarão essa ação se acharem que existe um tempo limitado
- Familiaridade/gosto – Os criminosos criam empatia com a vítima para estabelecer um relacionamento
- Confiança – Os criminosos criam uma relação de confiança com uma vítima, que pode precisar de mais tempo para ser estabelecida

Os profissionais de segurança digital são responsáveis por ensinar os outros funcionários da empresa sobre as táticas dos engenheiros sociais.

6.1.10.3 Shoulder Surfing e Busca de informações na lixeira

6.1.10.3.1 Shoulder Surfing

Um criminoso observa ou bisbilhota a vítima para obter PINs, códigos de acesso ou números de cartão de crédito. Um invasor pode estar perto da sua vítima ou pode usar binóculos ou câmeras de circuito fechado para descobrir informações. É por isso que uma pessoa só pode ler uma tela de atendimento bancário em determinados ângulos. Esses tipos de proteções dificultam muito o Shoulder Surfing.

6.1.10.3.2 Busca de informações na lixeira

"A lixeira de um homem é o tesouro de outro". Essa frase pode ser especialmente verdadeira no mundo da busca de informações na lixeira, que é o processo de revirar o lixo da vítima para ver quais informações uma empresa descartou. Considere a possibilidade de proteger a lixeira. Quaisquer informações confidenciais devem ser devidamente eliminadas através de trituração ou do uso de sacos de incineração, um recipiente que contém documentos confidenciais ou secretos para posterior destruição pelo fogo.

6.1.10.4 Representação e farsas

A representação é o ato de fingir ser outra pessoa. Por exemplo, um scan de telefone recente mirava nos contribuintes. Um criminoso, disfarçado de funcionário da Receita Federal, dizia para as vítimas que elas deviam dinheiro à Receita. As vítimas devem pagar imediatamente através de uma transferência bancária. O impostor ameaçou que a falta de pagamento resultará em prisão. Os criminosos também usam a representação para atacar os outros. Eles podem prejudicar a credibilidade das pessoas, usando publicações em site ou redes sociais.

Uma farsa é um ato com a finalidade de enganar ou ludibriar. Uma farsa virtual pode causar tanto problema quanto uma violação real. Uma farsa provoca uma reação do usuário. A reação pode criar um medo desnecessário e um comportamento irracional. Os usuários passam as farsas por e-mail e redes sociais.

6.1.10.5 Piggybacking e tailgating

Piggybacking ocorre quando um criminoso se identifica juntamente com uma pessoa autorizada, para entrar em um local protegido ou uma área restrita. Os criminosos usam vários métodos de piggyback:

- Parecem ser escoltados pela pessoa autorizada
- Juntam-se a uma grande multidão, fingindo ser um membro

- Escolhem uma vítima que é descuidada em relação às regras do estabelecimento

Tailgating é outro termo que descreve a mesma prática.

6.1.11 Negação de serviço

Os ataques de negação de serviço (DoS) são um tipo de ataque à rede. Um ataque de negação de serviço (DoS) resulta em algum tipo de interrupção de serviço aos usuários, dispositivos ou aplicações. Existem dois tipos principais de ataque de negação de serviço (DoS):

- Quantidade exorbitante de tráfego – O invasor envia uma enorme quantidade de dados a uma taxa que a rede, o host ou o aplicativo não pode suportar. Isso causa uma desaceleração na transmissão ou resposta ou uma falha em um dispositivo ou serviço.
- Pacotes formatados maliciosamente – O invasor envia um pacote formatado maliciosamente para um host ou aplicativo e o receptor não consegue contê-lo. Por exemplo, um aplicativo não pode identificar os pacotes que contêm erros ou os pacotes formatados incorretamente encaminhados pelo invasor. Isso causa lentidão ou falha na execução do dispositivo receptor.

Os ataques de negação de serviço (DoS) são um grande risco porque podem facilmente interromper os Sistemas de Comando e Controle de um Batalhão de Comunicações e causar perda significativa de tempo, dinheiro e situação tática. Esses ataques são relativamente simples de conduzir, mesmo por um invasor não capacitado.

O objetivo de um ataque de negação de serviço é negar acesso aos usuários autorizados, tornando a rede indisponível (lembre-se dos três princípios básicos de segurança: confidencialidade, integridade e disponibilidade).

Um ataque de negação de serviço distribuída (DDoS) é semelhante a um ataque de negação de serviço (DoS), porém é originado por várias fontes

coordenadas. Por exemplo, um ataque de negação de serviço distribuída (DDoS) pode ocorrer da seguinte maneira:

Um invasor cria uma rede de *hosts* infectados, denominada *botnet*, composta por zumbis. Os zumbis são os *hosts* infectados. O invasor usa um sistema de controle para controlar os zumbis. Os computadores zumbis examinam e infectam constantemente mais *hosts*, criando mais zumbis.

Quando está pronto, o hacker instrui os sistemas controlados para fazer com que o *botnet* de zumbis execute um ataque de negação de serviço distribuído (DDoS).

Um ataque de negação de serviço distribuída (DDoS) usa muitos zumbis para sobrecarregar uma vítima.

6.1.12 Ataques de Dia Zero

Um ataque de dia zero, às vezes conhecido como uma ameaça de dia zero, é um ataque de computador que tenta explorar as vulnerabilidades do software que são desconhecidas ou não divulgadas pelo fornecedor do software. O termo zero hora descreve o momento em que alguém descreve essas explorações. Durante o tempo que os fornecedores de software demoram para desenvolver e liberar um *patch*, a rede está vulnerável a essas explorações. A defesa contra esses ataques rápidos requer que os profissionais de rede adotem uma visão mais sofisticada da arquitetura da rede. Não é mais possível conter as intrusões em alguns pontos da rede.

6.1.13 Ataques de WEP e WPA

Wired Equivalent Privacy (WEP) é um protocolo de segurança que tentou fornecer uma rede de área local sem fio (WLAN) com o mesmo nível de segurança de uma LAN com fio. Como as medidas de segurança físicas ajudam a proteger uma LAN com fio, o WEP procura fornecer proteção similar para dados transmitidos pela WLAN com criptografia.

O WEP usa uma chave de criptografia. Não há provisão para gerenciamento de tecla com WEP, então o número de pessoas que compartilham a chave continuará a crescer. Desde que todo mundo está

usando a mesma chave, o criminoso tem acesso a uma grande quantidade de tráfego para ataques analíticos.

O WEP também tem vários problemas com o seu vetor de inicialização (IV), que é um dos componentes do sistema criptográfico:

- É um campo de 24 bits, que é muito pequeno.
- É um texto desprotegido, o que significa que é legível.
- É estático para que fluxos de chave idênticos se repitam em uma rede dinâmica.

O Wi-Fi Protected Access (WPA) e, em seguida, o WPA2 surgiram como protocolos melhorados para substituir o WEP. O WPA2 não tem os mesmos problemas de criptografia pois um invasor não pode recuperar a chave pela observação do tráfego. O WPA2 está suscetível ao ataque porque os criminosos virtuais podem analisar os pacotes transmitidos entre o *access point* e um usuário legítimo. Os criminosos virtuais usam um analisador de pacote e, em seguida, executa os ataques offline na frase secreta.

6.2 As Defesas

Agora já está ciente de alguns dos riscos relacionados ao uso de computadores e da Internet serão abordados alguns métodos de prevenir e mitigar os principais ataques citados anteriormente

6.2.1 Defesas contra malware

Alguns passos simples podem ajudar a se proteger contra todas as formas de malware:

• Programa de antivírus - A maioria dos conjuntos de antivírus captura as formas mais comuns de malware. Contudo, os criminosos virtuais desenvolvem e implantam novas ameaças diariamente. Portanto, o segredo de uma solução antivírus eficaz é manter as assinaturas atualizadas. Uma assinatura é como uma impressão digital. Identifica as características de um código malicioso.

• Software atualizado - Muitas formas de malware atingem seus objetivos explorando as vulnerabilidades do software, no sistema operacional e

nos aplicativos. Embora as vulnerabilidades do sistema operacional sejam a principal fonte de problemas, as vulnerabilidades dos aplicativos atuais representam o maior risco. Infelizmente, embora os fornecedores de sistemas operacionais estejam cada vez mais propensos a realizar correções, a maioria dos fornecedores de aplicativos não está.

6.2.2 Defesas contra Spam

Mesmo com essas funcionalidades de segurança implementadas, alguns spans ainda podem passar. Observe alguns dos indicadores mais comuns de Spam:

• Um e-mail sem assunto.

• Um e-mail solicitando uma atualização de uma conta.

• O texto do e-mail tem erros de ortografia ou uma pontuação estranha.

• Links no e-mail são longos e/ou incompreensíveis.

• Um e-mail parece uma correspondência de uma empresa idônea.

• Um e-mail que solicita que o usuário abra um anexo.

Se receber um e-mail que contém um ou mais desses indicadores, o usuário não deverá abrir o e-mail ou os anexos. É muito comum que a política de e-mail de uma empresa exija que um usuário que recebeu esse tipo de e-mail denuncie para a equipe de segurança digital. Quase todos os provedores de e-mail filtram spam. Infelizmente, o spam ainda consome a largura de banda e o servidor do destinatário ainda precisa processar a mensagem.

6.2.3 Defesas contra Engenharia Social

Uma armadilha evita o piggybacking, usando dois conjuntos de portas. Depois que os indivíduos entram pela porta externa, essa porta deve fechar antes que entrem na porta interna.

Defesa contra disfarce são a conscientização das táticas de engenharia social e orientar os funcionários corretamente sobre medidas de prevenção como as seguintes:

• Nunca fornecer informações confidenciais ou secretas por e-mail, sessões de bate-papo, pessoalmente ou por telefone às pessoas desconhecidas.

• Resistir à tentação de clicar em e-mails e links de site atraentes.

• Ficar de olho em downloads não iniciados ou automáticos.

• Estabelecer políticas e instruir os funcionários sobre essas políticas.

• Quando se trata de segurança, dar um sentido de apropriação aos funcionários.

• Não se submeter à pressão de pessoas desconhecidas.

6.2.4 Defesas contra DDOS

Uma empresa pode tomar uma série de medidas para se defender contra diversos ataques. Configurar firewalls para descartar todos os pacotes de fora da rede, com endereços que indiquem que foram originados dentro da rede. Essa situação não ocorre normalmente e isso indica que um criminoso virtual tentou executar um ataque de spoofing.

Para evitar ataques DoS e DDoS, assegure que os patches e upgrades sejam atuais, distribua a carga de trabalho entre os sistemas de servidor e bloqueie os pacotes externos de Internet Control Message Protocol (ICMP) na borda da rede. Os dispositivos de rede usam pacotes ICMP para enviar mensagens de erro. Por exemplo, o comando ping usa pacotes ICMP para verificar se um dispositivo pode se comunicar com outro na rede.

Os sistemas podem impedir que a vítima sofra um ataque de repetição, criptografando o tráfego, fornecendo autenticação criptográfica e incluindo um carimbo de hora em cada parte da mensagem.

6.2.5 Defesas contra-ataques a dispositivos móveis e sem fio

Há várias etapas a serem seguidas para defesa contra os ataques ao dispositivo sem fio e móvel. A maioria dos produtos WLAN usa configurações padrão. Utilize os recursos de segurança básicos sem fio, como autenticação e criptografia, ao alterar as configurações padrão.

Colocação de pontos de acesso (*access point*) restrito com a rede ao posicionar esses dispositivos fora do firewall ou dentro de uma zona desmilitarizada (DMZ) que contenha outros dispositivos não confiáveis como e-mail e servidores da Web.

As ferramentas WLAN, como NetStumbler, podem descobrir os *access points* e estações de trabalho não autorizados. Desenvolva uma política de convidado para abordar a necessidade de os convidados legítimos precisarem se conectar à Internet durante a visita. Para funcionários autorizados, utilize uma rede privada virtual de acesso remoto (VPN) para acesso WLAN.

Este tipo de defesa é muito importante dentro dos Batalhões de Comunicações, local com grande volume de pessoas e de informação sigilosa, a política interna das organizações não deve permitir a instalação de pontos de acesso ligados a rede interna da Organização Militar.

6.3 Considerações

Como visto neste capítulo, os riscos sempre vão existir, em qualquer meio. É possível, também, analisando todas as técnicas de defesa citadas observar um fator comum entre elas: a conscientização dos integrantes do sistema como um todo é chave para o sucesso das defesas implementadas.

Educação para os desenvolvedores, administradores de redes e principalmente para os usuários

A melhora não virá somente do uso de tecnologias de segurança ou da criação de leis, mas também da compreensão dos problemas e da mudança em como as pessoas utilizam desenvolvem a tecnologia.

7. NO MUNDO REAL

Este capítulo abordará de forma objetiva alguns dos principais ataques cibernéticos da atualidade envolvendo erros humanos.

7.1 O Stuxnet

De acordo com o Bicca (2014) do site O Arquivo, o Stuxnet é um *worm* de computador projetado especificamente para atacar o sistema operacional SCADA, desenvolvido pela Siemens para controlar as centrífugas de enriquecimento de urânio iranianas. Foi descoberto em junho de 2010 pela empresa bielorrussa desenvolvedora de antivírus Kaspersky. É o primeiro worm descoberto que espiona e reprograma sistemas industriais. Ele foi especificamente escrito para atacar o sistema de controle industrial SCADA, usados para controlar e monitorar processos industriais. O Stuxnet é capaz de reprogramar controladores pré-configurados e esconder as mudanças. O vírus pode estar camuflado em mais de 100 mil computadores, porém, para sistemas operacionais domésticos como o Windows e Mac OS X, o worm é inofensivo, só funciona efetivamente nas centrífugas de enriquecimento de urânio iranianas, já que cada usina possui sua própria configuração do sistema SCADA.

7.1.1 A origem

A origem do vírus Stuxnet ainda não foi definida, sabe-se que provavelmente tenha sido desenvolvido a mando de um país (Estados Unidos ou Israel), teoria defendida por Mikka Hypponen, não sendo possível o seu desenvolvimento por usuários domésticos e necessitando-se de informações detalhadas e de difícil acesso sobre o funcionamento da usina.

7.1.2 Ataque

O Stuxnet foi o primeiro worm de computador a incluir um rootkit de Controladores pré-configurados. Também é o primeiro worm conhecido por ter como alvo uma infraestrutura industrial crítica. Ainda, o alvo provável do worm foi a infraestrutura do Irã que utiliza o sistema de controle da Siemens. De acordo com jornais, a infestação do worm pode ter danificado as instalações

nucleares iranianas de Natanz e acabou atrasando o início da produção da usina de Bushehr. A Siemens, inicialmente, declarou que o *worm* não causou nenhum dano. Além do Irã, também foram afetados pelo *worm* Indonésia, Estados Unidos, Austrália, Inglaterra, Malásia e Paquistão. Como a usina não tem computadores conectados à Internet, a infecção deve ter ocorrido quando um dispositivo com o vírus foi conectado aos computadores da usina.

No complexo de Dimona, no deserto de Negev, em Israel, funcionavam centrífugas nucleares virtualmente idênticas às localizadas em Natanz, o que permitiu testar o Stuxnet em condições muito próximas das reais, antes de desfechar o ataque real. O *worm* tinha duas funções. A primeira delas era fazer com que as centrífugas iranianas começassem a girar 40% mais rapidamente por quinze minutos, o que causava rachaduras nas centrífugas de alumínio. A segunda forma inicialmente gravava dados telemétricos de uma típica operação normal das centrífugas nucleares, sem que o alarme soasse, para depois reproduzir esse registro para os operadores dos equipamentos enquanto as máquinas, na verdade, as centrífugas estavam literalmente se destruindo sob a ação do Stuxnet sem que os funcionários soubessem.

A propagação ocorreu com disseminação de pendrives com o Stuxnet no estacionamento da usina, em Natanz visto que os controladores e servidores não eram conectados à internet. Um funcionário ao deparar-se com o dispositivo, conectou-o em um computador ligado na rede da usina, isto foi o suficiente para o vírus fosse replicado em todos os dispositivos internos inclusive os controladores SCADA, responsável por gerenciar todas as etapas do enriquecimento de urânio do Irã.

7.1.3 Conclusões

Kevin Hogan, diretor sênior do setor de resposta a ataques da Symantec observou que 60% dos computadores infectados no mundo estavam no Irã, mais de 60.000, isso pode ser explicado pelo fato da usina não ser conectada à

Internet, o ataque foi direcionado para que um funcionário da usina fosse infectado. A Kaspersky Lab concluiu que o *worm* fora desenvolvido pelo governo de um país. O governo iraniano declarou em novembro de 2010 que algumas centrífugas haviam sido danificadas e que o vírus danificara atacara apenas computadores pessoais da usina. Esse ataque, acompanhado de outros ataques do mesmo gênero, pode ser considerado o início de uma ciberguerra, que poderia tornar-se uma preocupação para governos de todo o mundo.

7.2 O Flames

Ainda de acordo com Bicca (2014), esta praga infesta máquinas no Oriente Médio e é considerada “uma das mais complexas ameaças já descobertas”. Um assustador vírus de computador batizado de Flame está à solta no Irã e outras partes do Oriente Médio, infectando PCs e roubando informações. E agora a International Telecommunications Union, um órgão ligado às Nações Unidas, alerta que outros países podem estar correndo risco de sofrer um ataque.

7.2.1 A origem

O Flame está à solta desde 2010, de acordo com a Kaspersky, mas sua data de criação é incerta. Ele foi descoberto há cerca de um mês após o Ministério do Petróleo do Irã descobrir que os servidores de várias empresas haviam sido atacados. Esta descoberta levou à evidência de mais ataques a outros ministérios e indústrias iranianas.

O criador do Flame é desconhecido, mas é provável que uma nação esteja por trás dele. O vírus não foi projetado para roubar dinheiro de contas bancárias, e é muito mais complexo do que qualquer coisa comumente usada por “hacktivistas”, então esta é a única possibilidade que faz sentido.

7.2.2 O ataque

Os especialistas em segurança dizem que o Flame é a ciber-arma mais complexa já feita. Ele é capaz de se replicar mesmo em redes seguras e, então, controlar cada função dos computadores e espioná-los, enviando informações aos seus criadores. Para realizar esse serviço, o código consegue ativar microfones e câmeras, registrar cada tecla pressionada, tirar *screenshots*, extrair a localização geográfica de fotografias e até enviar e receber instruções e dados através de comandos por Bluetooth.

As informações roubadas são transmitidas para uma rede de servidores espalhados através do mundo. No total, cerca de 1.000 máquinas foram infectadas. São computadores situados na Cisjordânia, no Irã, no Líbano, na Síria, no Sudão, na Arábia Saudita, no Egito, nos Estados Unidos. Na Hungria, na Áustria, na Rússia e em Hong-Kong. A infecção se mostra bastante direcionada e toca mais computadores profissionais, em bancos por exemplo, que computadores pessoais, ressalta Laurent Heslault

A diferença para o Stuxnet, este foi concebido para danificar processos industriais, e o Flame parece estar direcionado a propósitos de espionagem. Não parece dirigir-se a um setor determinado, mas é um conjunto de ferramentas projetadas para a ciber-espionagem.

7.2.3 Conclusões

A International Telecommunications Union está avisando a outros países para “ficar em alerta” quando ao vírus, que potencialmente poderia ser usado para atacar infraestruturas críticas, entretanto empresas de segurança não alertam sobre nenhum risco direto ao usuário comum da Internet. Graham Cluley, da Sophos, lembra que o Flame só foi encontrado em algumas centenas de máquinas. “Certamente, é bastante insignificante quando comparado aos 600.000 Macs infectados com o malware Flashback no início deste ano”, disse Cluley em um post na internet.

7.3 O Wannacry

De acordo com Aliguieri (2012) o Wannacry está utilizando uma brecha de segurança no windows está infectando milhares de computadores ao redor do globo. O ataque parece ser uma campanha de infecção massiva a dezenas de organizações, incluindo hospitais, companhias de telecom, órgãos governamentais e transportadoras.

O ransomware é um forma de malware que infecta um sistema e criptografa seus arquivos. Esses dados são mantidos “sequestrados”, até que as solicitações do cracker sejam atendidas.

O software utilizado para o ataque de hoje é o WannaCry 2.0, também conhecido como WanaCrypt0r 2.0**,** tem se propagado através de email. Após a infectado o resgate solicitado é de 300 dólares em bitcoins e as estimativas são de que a infecção já atingiu mais de 70000 máquinas em mais de 70 países, incluindo o Brasil. As máquinas afetadas têm 6 horas para pagar o resgate dos dados.

7.3.1 A origem

O ransomware foi detectado pela primeira vez no início de fevereiro de 2017. A ameaça propaga-se através de um anexo de correio eletrônico ou através de outros computadores comprometidos na mesma rede graças a um executável, com características de *worm*, que procura replicar-se por servidores Windows que estejam acessíveis através da porta 445. Após ganhar acesso a um sistema, procede à sua replicação e execução, tentando depois a ligação a um domínio na Internet. Caso esta ligação seja bem-sucedida, o processo é terminado sem que a sua componente de ransomware seja executada. Em caso contrário, um ficheiro comprimido e protegido por palavra-chave é extraído para o sistema e executado. A ameaça procede depois à extração de um cliente, para a comunicação com os servidores de comando e controlo; e à alteração de privilégios do utilizador de modo a facilitar a criptografia dos dados.

7.3.2 O ataque

O ataque denominado Wannacry, consistiu na disseminação de um software malicioso, que bloqueia os computadores com sistema operativo Windows e exige um pagamento para os libertar.

A ameaça utiliza técnicas de exploração alegadamente desenvolvidas pela Agência de Segurança Nacional dos Estados Unidos. A divulgação de *exploits* pelo grupo The Shadow Brokers a 14 de abril de 2017 levou ao lançamento de uma correção crítica pela Microsoft em março de 2017. A técnica de exploração utilizada pelo malware deve-se a uma vulnerabilidade (EternalBlue/MS17-010) referente ao protocolo Server Message Block (SMBv1 e SMBv2) que permite a execução de código remoto ou, em alternativa, a um backdoor

Após a encriptação dos dados, serviços relacionados com a recuperação de dados e restauro do sistema são desativados pelo ransomware, apesar dos esforços realizados pela Microsoft, nem todos os usuários atualizaram seu sistema operacional com a correção e vulnerabilidade não pode ser sanada.

Como acontece com ameaças semelhantes, é exigido o resgate dos dados através do pagamento de $300 em bitcoin num prazo de três dias, e com a ameaça de destruição dos dados caso esta quantia não seja paga. A mensagem foi traduzida para mais de vinte idiomas. Os três endereços bitcoin incorporados no software malicioso foram monitorizados através de um bot. No dia 14 de maio de 2017, os resgates pagos totalizavam cerca de 33.000 dólares.

7.3.3 Conclusões

Apesar da grandeza em escala do ataque, o valor pedido pelo resgate foi muito aquém do esperado. O pedido inicial era de 300 dólares, pagos em bitcoin, e escalando para 600 dólares após 3 dias de infecção. Após uma semana, os dados seriam apagados. Pode-se perceber que os envolvidos detinham conhecimento em técnicas para despertar senso de urgência nos afetados.

Mesmo com toda a distribuição, o lucro registrado até então foi muito baixo. Todas as movimentações das 3 carteiras monitoradas de bitcoin que são públicas, por meio do sistema de *blockchain* não somam mais de 150 mil dólares.

8 ANÁLISE DOS DADOS

8.1 Análise do Stuxnet

Analisando o ataque cibernético causado pelo Stuxnet foi possível observar que o mesmo era extremamente direcionado, e que o atacante tinha como missão específica comprometer as centrífugas de enriquecimento de urânio no Irã.

Os pendrives colocados no estacionamento de forma proposital despertavam a curiosidade de quem passava no local, até que um dos funcionários guardou e conectou-o em um dos computadores com acesso à rede interna. O atacante não precisou se preocupar em burlar gigantescos sistemas de segurança, ele indiretamente conseguiu o acesso físico ao servidor por uso da engenharia social.

Este ataque confirmou a fragilidade dos recursos humanos quando não estão capacitados e cientes dos riscos que estão sujeitos na Segurança da Informação.

8.2 Análise do Flame

O Flame é um malware sofisticado, projetado para espionagem ele é capaz de roubar milhões de informações dos mais variados tipos: consegue enviar tudo o que a vítima digita, é capaz, também, de enviar fotos da tela do computador e ativar o microfone para escutar as conversas ambientes.

O ataque que o Flame desencadeou só foi possível graças à ingenuidade dos usuários que clicam em banners e links de propaganda com o malware, as vítimas são seduzidas pelos dizeres e acabam dando permissão para o que ele se instale na máquina vítima e replique-se na rede interna comprometendo outros usuários inocentes.

Os operadores que conhecem as tentativas de *phishing* e cientes dos riscos diante do desconhecido reportam as atividades suspeitas para que sejam tomadas as providências cabíveis e o ataque não seja desencadeado.

8.3 Análise do Wannacry

O Wannacry foi visto pela primeira vez em 2017, tendo como vítima as máquinas com o sistema operacional Microsoft Windows. O malware, após infectar a máquina comprime os ficheiros do computador com uma palavra-chave, impedindo que o usuário volte a ter acesso, em troca, a vítima se vê obrigada a realizar um pagamento de 300 dólares como resgate para os ficheiros novamente.

O ataque só é possível por dois grandes erros do usuário, o primeiro, está novamente ligado com os conhecimentos de *phishing*, ao clicar no anúncio ou link o usuário da permissão para que o malware se instale, o segundo grande erro está ligado com a atualização do sistema operacional, a Microsoft já havia disponibilizado semanas anteriores um *patch* contendo as correções das vulnerabilidades que o Wannacry exploram, mas os usuários negligenciaram esta importante medida e não instalaram em suas máquinas e servidores esta correção.

9 CONCLUSÃO

A pesquisa teve como objetivo geral diagnosticar as ocorrências envolvendo o ser humano no comprometimento da segurança da informação, tal pesquisa pode ser trazida para a realidade do Exército Brasileiro como forma de elucidar as principais atividades que também podem comprometer a continuidade, integridade e disponibilidade dos sistemas de táticos de um Batalhão de Comunicações no cumprimento de suas missões.

Destacou-se a necessidade de uma pesquisa interdisciplinar, que abordasse a Segurança da Informação e a doutrina militar dos Batalhões de Comunicações. Todos esses assuntos foram necessários para uma compreensão completa do assunto para que, assim, houvesse a formulação de uma resposta adequada ao problema.

Hoje a informação é considerada como um dos principais ativos das instituições e empresas devendo ser protegida a qualquer custo, diante disso, surgem, a cada dia, novas tecnologias que prometem elevar a segurança desses ativos, entretanto, foi observado que nada adiantará se os recursos humanos, que operam estes sistemas não conhecem os verdadeiros perigos e armadilhas do cenário cibernético que estão inseridos.

Em virtude disso, surgiu à necessidade de abordar no presente trabalho os principais perigos que acometem as organizações e também as ferramentas utilizadas na busca pelo combate dos problemas existentes, para que depois de identificadas possam ser adotadas medidas preventivas.

A Segurança da Informação está relacionada de maneira antagônica com a comodidade que as tecnologias proporcionam, pois uma boa segurança resulta em grandes verificações e preocupações que precisam ser adotadas gerando um grande desafio para os usuários.

Este estudo buscou o entendimento de como funcionam as particularidades das ferramentas e técnicas mais utilizadas sob a ótica voltada para os ataques cibernéticos abordados na monografia.

Com a pesquisa concluída ficou evidente a fragilidade encontrada nos sistemas de informações atuais e a dificuldade dos operadores adotarem medidas simples de segurança que evitariam o comprometimento de dados e informações sensíveis.

Ainda pode-se destacar o fator humano, talvez o maior vilão dentre todos os encontrados, pois as informações quase que em sua totalidade são manipuladas por eles gerando os maiores perigos para os dados da organização militar. Deixando, de forma evidente, a importância de sua capacitação para que atuem de forma eficaz com todos os outros sistemas se segurança uma barreira sólida contra as ameaças da atualidade.

REFERÊNCIAS

ARRUDA, Felipe. **Engenharia Social: o malware mais antigo do mundo**. 2011. Disponível em: <https://www.tecmundo.com.br/seguranca/8445-engenharia-social-o-malware-mais-antigo-do-mundo.htm>

CERVO, Amado Luiz; BERVIAN, Pedro Alcino. **Metodologia científica: para uso dos estudantes universitários**. 2. ed. São Paulo: McGraw-Hill do Brasil, 1978

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos da metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

FILHO, Antonio Mendes da Silva. **Segurança da Informação: Sobre a Necessidade de Proteção de Sistemas de Informações**. 2008. Disponível em:<http://www.espacoacademico.com.br/042/42amsf.htm>

FONTES, Edison. **Segurança da Informação: o usuário faz a diferença**. 1a edição. São Paulo: Saraiva, 2006.

MITNICK, Kevin D., 1963 - **A arte de invadir: as verdadeiras histórias por trás das ações de hackers, intrusos e criminosos eletrônicos** / Kevin D. Mitnick e William L Simon - São Paulo: Pearson Prentice Hall, 2005.

MITNICK, K. D.; SIMON, W. L. Mitnick : **A arte de enganar**. São Paulo: PearsonEducation do Brasil, 2003.

PROMON, Business & Tecnology review. **Segurança da Informação – Um diferencial determinante na competitividade das corporações**. Rio de Janeiro, 2005. Disponível em:<http://www.promon.com.br/portugues/noticias/download/Seguranca_4Web.pdf>

SÊMOLA, Marcos. **Gestão da Segurança da Informação: Uma visão Executiva**. Rio de Janeiro: Campus, 2003.

BROWN, A.S.; BRACKEN, E., ZOCCOLI, S. e Douglas, K. Generating **andremembering passwords.** ***Applied Cognitive Psychology***, 2004.

CÂMARA, Marcelo, R. **Engenharia Social, a Psicologia da aplicação e sua prevenção**. Natal, Rio Grande do Norte. 2009.

Proof. Ciclo OODA: **Conheça esta nova abordagem de gestão de riscos**. Disponível em: <http://www.proof.com.br/blog/inovacao-em-seguranca/ciclo-ooda-conheca-esta-nova-abordagem-de-gestao-de-riscos/>

RAMOS, Anderson. **Política de cibersegurança das empresas 'esquece' usuário, diz estudo**. 2017. Disponível em: <http://m.folha.uol.com.br/tec/2017/09/1917727-politica-de-ciberseguranca-das-empresas-esquece-usuario-diz-estudo.shtml>

LAITMAN, Michael. **A Falha Fundamental por trás do Ciber-Ataque**. 2017. Disponível em: <http://www.michaellaitman.com/pt/artigos/falha-fundamental-por-tras-ciber-ataque/>

KLEIN, Soeli Claudete. **Engenharia social na Área da Tecnologia da Informação**. 2004. 63p., Monografia (trabalho de Ciências Exatas e Tecnológicas, Centro Universitário Feevale). Novo Hamburgo, RS. 2004.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. **Política de Segurança da Informação: guia prático e implementação**. Rio de Janeiro: Ciência Moderna, 2006.

BRASIL. Estado-Maior do Exército. Manual de Campanha. C 11-20 – **BATALHÃO DE COMUNICAÇÕES**. 2003.

BRASIL. Estado-Maior do Exército. Manual de Campanha. EB20-MC-10.205 – **COMANDO E CONTROLE**. 2015

BICCA, R, **Os vírus Stuxnet e Flame**. Disponível em <http://www.oarquivo,com.br/variedades/ciencia-e-tecnologia/2251-os-virus-stuxnet-e-flame-parte-1.html>. Acesso em: 07 Abr. 2018.

AGUILIERI, Frank. **Ataque massivo do ransonware WannaCry afeta dezenas de países**. Disponível em <http://www.getcard.com.br/novo/ataque-massivo-do-wanna-cry-2-0-afeta-dezena-de-paises/>. Acesso em: 19 Maio. 2018.

BRASIL. Ministério da Defesa. MD31-M-03 – **DOUTRINA PARA O SISTEMA MILITAR DE COMANDO E CONTROLE**. 2015

BICCA, R, **Os vírus Stuxnet e Flame**. Disponível em <http://www.oarquivo,com.br/variedades/ciencia-e-tecnologia/2251-os-virus-stuxnet-e-flame-parte-1.html>. Acesso em: 07 Abr. 2018.

CISCO, Netacad. **Cibersecurity Essentials.** Disponível em <https://www.netacad.com/pt-br/courses/security/cybersecurity-essentials> Acesso em: 12 Fev. 2018