ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS DA AERONÁUTICA

CURSO DE APERFEIÇOAMENTO DE OFICIAIS 3/2022

EDUARDO FRANCISCO **SIEBER** FILHO, Cap Eng

Proteção de Dados do COMAER Contra Ataques de *Ransomware*

Rio de Janeiro

2022

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS DA AERONÁUTICA
CURSO DE APERFEIÇOAMENTO DE OFICIAIS 3/2022

EDUARDO FRANCISCO **SIEBER** FILHO, Cap Eng

Proteção de Dados do COMAER Contra Ataques de *Ransomware*

Trabalho de conclusão de curso apresentado no Curso de Aperfeiçoamento de Oficiais da Aeronáutica como requisito parcial para aprovação no Curso de Pós-graduação *Lato Sensu* em Liderança com Ênfase em Gestão no COMAER.
Linha de Pesquisa: Guerra Cibernética
Orientador: Israel Cordeiro dos Santos Rocha, Maj Eng

Rio de Janeiro
2022

EDUARDO FRANCISCO **SIEBER** FILHO, Cap Eng

Proteção de Dados do COMAER Contra Ataques de *Ransomware*

Trabalho de conclusão de curso apresentado no Curso de Aperfeiçoamento de Oficiais da Aeronáutica.

Aprovado por:

_____

Jaqueline de Azevedo Bruno, Ten Cel Int
EAOAR

_____

Israel Cordeiro dos Santos Rocha, Maj Eng
EAOAR

Rio de Janeiro

2022

RESUMO

As informações organizacionais armazenadas em sistemas computacionais são consideradas ativos críticos, imprescindíveis para a concretização de negócios e tomada de decisões, necessitando então que sua segurança seja gerida de maneira absoluta. Em face ao elevado índice de ataques por *software* de sequestro (*ransomware*) em 2021 e ao elevado nível de ameaça oferecido por este crime às informações da instituição, torna-se imperativo adotar medidas que mitiguem os riscos inerentes a este tipo de ataque, principalmente em organizações que operam sistemas de infraestrutura crítica, a exemplo do COMAER, no Controle do Espaço Aéreo. Em complemento, destaca-se o papel dos usuários de TI destreinados em segurança cibernética na disseminação deste tipo de ataque. Técnicas de engenharia social empregadas com objetivo de possibilitar os ataques de *ransomware* facilmente ludibriam esses usuários, fazendo-os adotar ações que comprometam os recursos de TI da Organização. Agravando a situação, a FAB possui características organizacionais para ser potencial e constante alvo desses ataques. Diante desse cenário, este ensaio é de parecer que sejam adotados treinamentos periódicos em segurança cibernética para os usuários de TI do COMAER, como forma de mitigar ataques de *ransomware* à Instituição. Mediante a implementação dessa proposta, haverá ganhos substanciais no nível de segurança cibernética das informações estratégicas armazenadas em sistemas de TI da Força Aérea Brasileira, contribuindo diretamente para o aumento da capacidade do COMAER em proteger sistemas de TI contra ataques cibernéticos, conforme diretriz do Plano Estratégico Militar da Aeronáutica em vigor.

Palavras-chave: Ransomware. Segurança Cibernética. Guerra Cibernética. Engenharia Social.

1 **INTRODUÇÃO**

Em um contexto mundial, as informações organizacionais armazenadas em sistemas computacionais são consideradas ativos críticos, imprescindíveis para a concretização de negócios e apoio a decisões de natureza comercial, governamentais, sociais, de guerra, dentre outras, necessitando então que sua segurança seja gerida de maneira absoluta. Analogamente, as informações pertencentes ao Comando da Aeronáutica (COMAER) devem ser tratadas como um patrimônio a ser protegido, pois compõem um recurso vital para o pleno funcionamento de toda a Força Aérea Brasileira (BRASIL, 2022).

Em nível global, foi observado em 2021 um elevado índice de ataques executados com uso de *Software* de Sequestro (*ransomware*) contra organizações dos mais diversos setores, inclusive Defesa e Aeroespacial, denotando assim elevada motivação dos criminosos em perpetrar esse tipo de ataque.

Os ataques de *ransomware* representam uma grande ameaça à segurança de redes corporativas, pois incapacitam o acesso às informações da Organização, causando sérios danos à imagem e operações da Organização.

Em sua maioria, esses ataques são disseminados por meio de técnicas de engenharia social[1], que levaram os usuários a executar as ações necessárias para que o ataque obtenha êxito. Técnicas de *phishing*[2], baseadas em e-mails contendo links ou arquivos comprometidos com a finalidade de enganar os usuários foi o principal vetor utilizado pelos atacantes para a disseminação de *ransomware* (UNIÃO EUROPEIA, 2021).

Neste cenário, organizações dotadas de elevada notoriedade e reconhecimento público, que armazenam informações sensíveis de natureza estratégica nacional, ou que operam serviços de infraestrutura crítica (como o de controle do espaço aéreo, no caso do COMAER), são frequentemente alvos da cobiça dos criminosos, pois representam altas recompensas monetárias ou de fama nos casos de sucesso do ataque.

Desse modo, motivado pelos fatores da FAB ter características para ser constante alvo de ataques cibernéticos com uso de *ransomware*, e o fato de que o

[1] ato de enganar um indivíduo, ganhando sua confiança, com objetivo de que ele revele informação sensível ou aja de acordo com a vontade do atacante (PORTUGAL, 2022).

[2] mecanismo de elaborar mensagens ou *e-mails* que tentam enganar os receptores para que estes abram anexos maliciosos, cliquem em *links* inseguros, revelem as suas credenciais através de páginas de phishing aparentemente legítimas, façam transferências de dinheiro etc. (PORTUGAL, 2022).

sucesso dessas investidas só é possível mediante interações descuidadas dos usuários, este ensaio defende a adoção de treinamentos periódicos em segurança cibernética para os usuários de TI do COMAER, como forma de mitigar ataques de *ransomware* contra a Instituição. Por fim, essa adoção, contribuirá diretamente para o aumento da capacidade de proteção de Sistemas de TI do COMAER contra ataques cibernéticos, indo ao encontro do que propõe a diretriz para Tecnologia da Informação do Plano Estratégico Militar da Aeronáutica (BRASIL, 2018).

2 **DESENVOLVIMENTO**

2.1 **A FAB Como Potencial Alvo do Elevado Poder Destrutivo de *Ransomware.***

Ransomware, ou “Software de Sequestro” é um esquema de extorsão pelo qual os atacantes sequestram e criptografam os arquivos do computador da vítima e, em seguida, exigem um resgate por esses arquivos em sua condição original (LUO; LIAO, 2007).

Relatam, Luo e Liao (2007) que estes *softwares* maliciosos são baseados em algoritmos matemáticos de Criptografia de Chave Pública, portanto é praticamente impossível obter a chave de resgate por meio de adivinhação, engenharia reversa, técnicas de dicionário ou força bruta. Ainda, segundo estes autores, em *ransomwares* que empregam criptografia de 660 bits, seriam necessários 30 anos para obter-se a chave por método de força bruta, utilizando-se um processador de 2.2GHz.

Para recuperar as informações “sequestradas”, pode-se considerar o pagamento do resgate ao atacante (sem garantias de retorno) ou a restauração dos dados originais a partir de um *backup*. Para que a segunda opção funcione, existe a dependência de uma série de fatores, como a existência do *backup*, o quanto ele está atualizado e local de armazenamento, já que por vezes, o backup pode ter sido também sequestrado e criptografado pelo *ransomware*. De fato, no mínimo, uma infecção por *ransomware* causa impacto na disponibilidade das informações, pois o processo de restauração do *backup* como solução do problema demanda um tempo de execução, no qual a informação estará inacessível.

No âmbito do COMAER, a indisponibilidade ou perda de informações implicará em impactos para o funcionamento de algum setor, ou quiçá de toda a instituição. Pode-se imaginar uma situação hipotética, na qual devido a uma infecção por

ransomware, informações sobre um determinado projeto, que não tinha cópia de segurança foram sequestradas. Neste caso, há uma decisão a ser tomada: pagar o resgate sem qualquer garantia de entrega da informação original, ou considerá-la como perdida. Se o *backup* existir, o principal impacto enfrentado será a indisponibilidade da informação durante o processo de restauração, o que já pode acarretar atrasos em projetos ou paradas em prestações de serviço.

Existe ainda um risco intrínseco ao ser vítima desse tipo de ataque: O *ransomware* utilizado no ataque pode ter enviado as informações sequestradas para a nuvem da Internet, oferecendo a possibilidade de exposição indesejada da informação, levando a uma possível responsabilização jurídica dos gestores responsáveis à luz da Lei Geral de Proteção de Dados (LGPD).

Ademais, esse tipo de ataque se demonstra uma ameaça grave não só ao dispositivo do usuário isoladamente, mas também à rede corporativa na qual ele está conectado: Richardson e North (2017) afirmam que alguns tipos de *ransomware* foram aperfeiçoados a ponto de não somente criptografar e sequestrar informações armazenadas no dispositivo infectado, mas também em qualquer outro dispositivo de armazenamento externo ou compartilhamento de rede a ele conectados. Adicionalmente, de acordo com União Europeia (2021), recentemente novos tipos de *ransomware* surgiram com a capacidade de propagarem-se de maneira autônoma.

Esses fatos elevam o grau de alerta e nível de proteção necessários para com a informação, pois uma infecção por este tipo de agente causará indisponibilidade ou perda de informações salvas em unidades de rede ou em qualquer outro dispositivo móvel conectado ao computador infectado. Ainda, é necessário considerar a possibilidade de uma infecção em cadeia na rede de dados da Organização, devido à capacidade de disseminação autônoma de algumas variantes deste *software*.

Nestes casos, a infecção de um único computador da rede do COMAER por variantes de disseminação autônoma, poderia resultar em uma contaminação em cadeia dos computadores em rede, causando indisponibilização de informações e elevada carga de trabalho para reparo em todos os computadores comprometidos.

Em 2021, Agências de Segurança Cibernética dos Estados Unidos, Inglaterra e Austrália reportaram um aumento nos ataques sofisticados de alto impacto envolvendo *ransomware* contra infraestruturas críticas, inclusive do setor de Defesa (ESTADOS UNIDOS, 2021). Corroborando com esse cenário, um relatório da consultoria conjunta de Defesa Cibernética, composta pelo FBI, CISA, NSA, ACSC e

NCSC mostra que estes órgãos observaram um aumento global em incidentes de *ransomware* sofisticados de alto impacto contra Organizações de infraestrutura crítica em 2021 (ESTADOS UNIDOS, 2021).

Ataques contra estes serviços, a exemplo do Controle do Espaço Aéreo, exercido pelo COMAER, podem implicar em indisponibilidade nos sistemas, causando sérios impactos à missão da Força Aérea Brasileira, danos à imagem e confiabilidade da Instituição, e até mesmo acidentes que comprometam vidas.

Sendo assim, considerando o elevado impacto negativo à Instituição causado por um ataque cibernético com emprego de *ransomware*, e o fato de a FAB possuir as características institucionais que a elegem a ser constante alvo deste tipo de ataque, é mandatório que sejam adotados treinamentos periódicos em Segurança Cibernética para os usuários de TI da FAB, o que possibilitará a mitigação do risco de ocorrência destes ataques, conforme será apresentado doravante neste trabalho.

2.2 **Usuários de Recursos de TI Destreinados Atuam Como Disseminadores de *Ransomware*.**

Atualmente, novas técnicas de engenharia social estão sendo empregadas para explorar falhas ocasionadas pelos usuários de recursos de TI. Em conjunto com os tradicionais métodos de *e-mails* maliciosos, a exploração de sites ainda é amplamente utilizada: nessa modalidade, atacantes forjam ou adulteram páginas de empresas, órgãos do governo, hospitais, ou qualquer outro ator de interesse do usuário, oferecendo *downloads* de *software* maliciosos disfarçados, ou tentando enganar os usuários de maneira que estes forneçam dados pessoais ou credenciais de rede. Estes ataques empregam diversas iscas para atrair vítimas: prêmios em dinheiro em troca de preenchimento de pesquisas pelo usuário, que na verdade são falsas e só buscam capturar dados dos usuários, pagamentos antecipados por vacinas de COVID, que nunca seriam fornecidas, sites com a proposta de serem *streamers* gratuitos de filmes, que demandam a instalação de *software* para assisti-los.

Muitos desses ataques enganam facilmente os usuários, pois empregam histórias que, apesar de falsas, são muito bem elaboradas, com temáticas atuais que exploram a inocência ou ganância das pessoas.

Complementa esse cenário a pesquisa evidenciada por Richardson e North (2017), que mostra que 93% de todos os *e-mails* de *phishing* por eles analisados continham algum tipo de *malware*, 59% das infecções de *ransomware* ocorreram por meio de *e-mail* (seja por anexo ou *link* da mensagem), 24% por *website* ou aplicação e 18% por mídia social ou dispositivos de armazenamento externo.

Agravando a situação e o potencial risco oferecido por usuários de TI destreinados, os *softwares* de defesa, como *Ad-Blockers*, *firewall* e Antivírus não são suficientes para proteger a Organização deste tipo de ataque. De acordo com Richardson e North (2017), os ataques de *ransomware* e as técnicas de *phishing* estão em constante evolução para permanecer à frente da capacidade de detecção dessas ferramentas de segurança.

Nota-se então que a utilização da Internet, apesar de indispensável no apoio ao desenvolvimento das mais diversas atividades da FAB, oferece riscos cibernéticos quando feita de maneira descriteriosa pelos usuários de recursos de TI, que por meio de sua conduta descuidada, podem acabar comprometendo os ativos da Instituição.

Entretanto, ferramentas como o correio eletrônico e a navegação na Internet são importantes atores de suporte às operações do COMAER, de modo que não é minimamente razoável optar pela desativação desses recursos como método para conter os problemas de ataques cibernéticos oriundos deste meio.

Portanto, é necessário promover a redução da possibilidade de ocorrência desses ataques por meio da atuação na mudança da consciência e do comportamento dos usuários.

Ratificam essa assertiva Abawajy e Kim (2010), quando afirmam que o objetivo fundamental dos treinamentos e conscientização sobre segurança cibernética é gerar uma mudança de atitudes, capaz de alterar a cultura organizacional, criando a percepção de que a segurança cibernética é crítica, pois uma falha acarretará consequências potencialmente adversas para todos. Portanto, o aumento da conscientização dos usuários reduz a probabilidade de ocorrência de incidentes e violações de segurança e eleva a probabilidade de que atividades suspeitas sejam reconhecidas e relatadas às equipes de segurança cibernética pelos usuários.

Sendo assim, fica evidente que a adoção de treinamentos periódicos em Segurança Cibernética para os usuários de TI da FAB mitigará o risco de um ataque cibernético com a utilização de *ransomware* contra a FAB, pois capacitará seus

usuários a reconhecer e lidar com os principais vetores de disseminação deste tipo de ataque, evitando que suas ações comprometam os recursos de TI da Organização.

3 **CONSIDERAÇÕES FINAIS**

Os ataques cibernéticos perpetrados com a utilização de *ransomware* (ou *software* de sequestro) representam uma grande ameaça à FAB, pois acarretam impactos na disponibilidade ou, no pior dos casos, na integridade das informações e na operacionalidade de sistemas de controle de Infraestrutura Crítica.

A Força Aérea Brasileira, por ser uma Organização de notável reconhecimento público e por operar infraestruturas críticas, desperta a atenção e cobiça dos criminosos, fato que a torna potencial alvo de ataques cibernéticos.

Vale também destacar o papel fundamental dos usuários de TI como vetores de disseminação deste tipo de ataque. Conforme discutido, a maioria dos ataques cibernéticos com emprego de *ransomware* só ocorreram graças ao emprego de técnicas de engenharia social, que exploraram condutas descuidadas dos usuários, levando-os a adotar ações que possibilitaram o comprometimento dos ativos de TI e, por consequência, das informações e da imagem da Instituição

Considerando o cenário apresentado, este ensaio é de parecer que sejam adotados treinamentos periódicos em segurança cibernética para os usuários de TI do COMAER, o que resultará na mitigação de ataques de *ransomware* à Instituição. A implementação dessa proposta promoverá ganhos substanciais no nível de segurança cibernética das informações estratégicas armazenadas em sistemas de TI da Força Aérea Brasileira, contribuindo diretamente para o aumento da capacidade do COMAER em proteger sistemas de TI contra ataques cibernéticos, indo ao encontro da diretriz para Tecnologia da Informação do Plano Estratégico Militar da Aeronáutica em vigor.

REFERÊNCIAS

ABAWAJY, Jemal; KIM, Tai-Hoon. Performance Analysis of Cyber Security Awareness Delivery Methods. **Communications In Computer And Information Science**, [S.L.], p. 142-148, 2010. Springer Berlin Heidelberg. http://dx.doi.org/10.1007/978-3-642-17610-4_16.

BRASIL. Comando da Aeronáutica. **Portaria n. 2.102/GC3, de 18 de dezembro de 2018**. Aprova a reedição do Plano Estratégico Militar da Aeronáutica. Rio de Janeiro, 2018a.

BRASIL. Portaria do Gabinete do Estado Maior da Aeronáutica 273/GC3 de 18 de Abril de 2022. Aprova a Diretriz que estabelece a Política de Segurança da Informação do Comando da Aeronáutica (DCA 14-8). **Boletim do Comando da Aeronáutica**: Rio de Janeiro, RJ, n. 074, Anexo, pag. 92-116, 20 abr. 2022.

ESTADOS UNIDOS. Cybersecurity & Infrastructure Security Agency. **2021 Trends Show Increased Globalized Threat of Ransomware**. 2022. Disponível em: https://www.cisa.gov/uscert/sites/default/files/publications/AA22-040A_2021_Trends_Show_Increased_Globalized_Threat_of_Ransomware_508.pdf. Acesso em: 13 set. 2022

LUO, Xin; LIAO, Qinyu. Awareness Education as the Key to Ransomware Prevention. **Information Systems Security**, [S.L.], v. 16, n. 4, p. 195-202, 4 set. 2007. Informa UK Limited. http://dx.doi.org/10.1080/10658980701576412. Acesso em: 20 set. 2022.

PORTUGAL, Centro Nacional de Cibersegurança de. **Glossário**. 2022. Disponível em: https://www.cncs.gov.pt/pt/glossario/. Acesso em: 02 nov. 2022.

RICHARDSON, Ronny; NORTH, Max. Ransomware: Evolution, Mitigation and Prevention. **International Journal of Management Reviews**, Kennesaw State University, Ga Usa, v. 13, n. 1, p. 1-13, 01 jan. 2017. Disponível em: https://digitalcommons.kennesaw.edu/facpubs/4276. Acesso em: 17 set. 2022.

UNIÃO EUROPEIA. Agência da União Europeia para a Cibersegurança. **RELATÓRIO ENISA SOBRE O CENÁRIO DAS AMEAÇAS DE 2021**. 2021. Disponível em: https://www.enisa.europa.eu/publications/etl-2021/enisa-threat-landscape-2021-2022-final_pt.pdf. Acesso em: 13 set. 2022. Acesso em: 13 set. 2022.