AS PRÁTICAS DE GOVERNANÇA E O GERENCIAMENTO DOS SERVIÇOS DE TI ORIENTADO AO *COBIT* COMO UM VETOR, PARA A DETECÇÃO DO *MALWARE*, DENOMINADO *RANSOMWARE*

Paulo Marcos Cabral Junior
https://orcid.org/0009-0007-3081-6042

RESUMO

No Brasil existe um baixo investimento nos sistemas de defesa e não investimos na questão da detecção, para isso é necessário ter um Centro de Operações de Segurança (*SOC – Security Operation Center*), de modo a monitorar o tráfego da rede. Neste trabalho, usou-se uma abordagem qualitativa, sendo consultados artigos acadêmicos, dissertações e teses, sobre o *Cobit* como um vetor, para a detecção deste *Malware.* Foram discutidas diversas ferramentas e procedimentos para se evitar a sua contaminação pelo *Ransomware*. Conclui-se que, quando se utilizam as ferramentas, que usam inteligência artificial e proteções especializadas, tem-se uma probabilidade maior de não ser infectado.

Palavras-chave: *Ransomware. Malware. Cobit.*

1 INTRODUÇÃO

O modelo de governança convém que os dirigentes governem a TI, através de três tarefas principais: Avaliar o uso atual e futuro da TI; Dirigir ou orientar a preparação e a orientação de planos e políticas para assegurar que, o uso da TI, atenda aos objetivos do negócio; Monitorar o cumprimento das políticas e o desempenho, em relação aos planos.

A Associação de Auditoria e Controle de Sistemas de Informação (tradução de *Information Systems Audit and Control Association* – ISACA) tem documentado ameaças constantes, nas estruturas de riscos em tecnologia da informação (TI) e na governança, no contexto da TI e cibersegurança. Pode-se dizer que o risco é qualquer negócio ou missão de risco, relacionado ao uso ou dependência da tecnologia da informação e comunicação (TIC); da tecnologia operacional (TO) ou da internet das coisas (*IoT*).

Os riscos cibernéticos têm características de difícil compreensão, pelas partes interessadas da empresa. Sendo assim, os membros do conselho executivos das empresas, que necessitam da tecnologia para atingir os seus objetivos estratégicos e operacionais, devem ser responsáveis pela gestão dos riscos na TI. O conceito envolvendo essas ameaças incluiu: os perigos e vulnerabilidades; apetite de risco; tolerância; impacto; priorização e resposta, que são essenciais para as áreas de: governança; gestão e avaliação; riscos operacionais.

No Brasil existe um baixo investimento nos sistemas de defesa e não investimos na questão da detecção, para isso é necessário ter um Centro de Operações de Segurança (*SOC – Security Operation Center*), de modo a monitorar o tráfego da rede. Outras ferramentas utilizadas são o Gerenciamento de Informações e Eventos de Segurança (*SIEM - Security Information Events Response*), juntamente com a Orquestração, Automação, e Resposta de Segurança (*SOAR - Security Orchestration, Automation and Response*), que completam um sistema eficiente e robusto.

Entre as práticas mais assertivas está o modelo 3-2-1-1-0, que consiste em ter: três cópias diferentes dos dados, dois tipos distintos de mídia, sendo um deles fora do local e outro, com técnica *air gap* ou imutável, e apresentar zero erros após testes ou recuperação. Com isso, sua empresa torna-se preparada em caso de qualquer incidente, especialmente, os de *ransomware*. As atualizações de *software* de proteções, enriquecimento de ofensa com valor agregado, leva a uma redução do tempo de atendimento do analista e configuração de limite dinâmico com base no apetite ao risco ou escalonamentos reduzidos de falsos positivos, economizando tempo no tratamento de incidentes de baixo valor; especialmente as recentes técnicas de aprendizado de máquina e inteligência artificial, a fim de filtrar alertas de baixo valor de semelhanças, a esse *malware*.

Presume-se que existam defesas integradas e eficazes contra o *ransomware*, como por exemplo: a utilização de boas práticas, juntamente com uma governança eficiente, os backups regulares e um sistema integrado defesas utilizando os *SOCs; SIEMs; SOACs; X-Force Investigate; X-Force Detect;* e utilizando algoritmos de inteligência artificial que aprendem com as experiências anteriores; entre outras ferramentas, tudo isso rodando no *COBIT*.

Fica a pergunta a ser respondida: No *COBIT 5,* seria possível executar tarefas de difícil complexidade em segurança dos dados, com um custo factível, e tornar um sistema bastante seguro, contra ataques de *ransomware*?

2 DESENVOLVIMENTO

A governança de segurança cibernética está preocupada em lidar com eventos e incidentes inesperados. Segundo conteúdo adaptado do *ISACA®. Transforming Cybersecurit,* o *COBIT 5* tem a governança da cibersegurança, os objetivos dividido em cinco tipos, a saber:

Orientado por inteligência artificial de ameaças: Integrar e internalizar novos riscos e ameaças, implementando elementos adaptativos e alinhavando o risco, com as necessidades e a inteligência das ameaças.

Funções de segurança integradas: Agregar as funções de segurança com aplicabilidades nos negócios e Implementar o comportamento de informações e dos canais de comunicação.

Proativo e baseado na antecipação: Prever os ataques e comportamento do invasor; Evitar o minimalismo nos gastos e nas estratégias de segurança e; Implantar uma segurança sistêmica para ciclo de vida.

Flexível, adaptável e a resiliência: Implantar adaptações e autorreflexão das aprendizagens que tragam uma melhoria operacional e organizacional, incluindo uma continuidade de negócios de serviço de TI.

Orientado para o serviço do negócio: Definir e implementar a segurança, como um serviço para os negócios.

A **governança de segurança cibernética** está relacionada à sua excelente capacidade adaptativa e à natureza flexível das disposições de governança. É necessário reconhecer o fato de que: ataques, incidentes e violações sempre visam o “elo mais fraco”, na segurança da cadeia de valor da empresa.

O **COBIT 5**, é um Modelo Corporativo para Governança e Gestão de TI da Organização estabelece habilitadores para gerenciar a segurança cibernética que esteja

conectado com as práticas de governança, risco e conformidade (*GRC*), em toda a empresa.

2.1 Gerenciamento de Riscos

No gerenciamento do risco o perfil de risco é descrito como sendo uma identificação do risco global, no qual, a empresa está exposta, consistindo em:

a) **Registro do Risco**: fornece informações detalhadas sobre cada risco identificado com o responsável pelo risco, gerando detalhes do cenário e das suas premissas com as partes interessadas afetadas, com indicadores das causas. Fornece informações sobre as respostas aos riscos e o *status* das respostas aos riscos, através de prazo para as ações.

a.1) **Cenário do registro de risco**: é uma descrição detalhada de uma ameaça relacionado a uma atividade, o quando ocorre, pode levar a um impacto aos negócios.

a.2) **Resultado das análises do perfil dos riscos**: é uma técnica para tornar o risco mais compreensível, e permitir uma adequada análise na avaliação dos riscos.

b) **Plano de ação do perfil do risco**: Fornece uma estrutura que documenta a ordem de prioridade em que as ações de risco individuais devem ser implementadas e, como elas devem ser realizadas.

c) **Evento da perda do perfil de risco**: Podendo ocorrer um erro no processamento do sistema, que resulta em algum tipo de perda.

d) **Perfil do fator de risco**: Condição que pode influenciar a frequência e o impacto e, em última análise, o impacto nos negócios de eventos ou cenários relacionados.

e) **Resultado de avaliação independente do perfil de risco**: O relatório de auditoria contém descobertas de avaliações que devem ser levadas em consideração, durante as atividades de identificação e análise de riscos.

2.2 Malware Ransomware

Segundo o relatório da *Datto*, *Global State of the Channel Ransomware* (2021), essas são as cinco maneiras mais comuns pelas quais, os *ransomware* infectam suas vítimas:

- E-mails de phishing;
- Práticas inadequadas dos usuários;
- Falta de treinamento em segurança cibernética;
- Senhas fracas e gerenciamento de acesso;
- Acesso RDP aberto.

2.3 Centro de Operações de Segurança (*SOC*)

As equipes de *SOC* são responsáveis por monitorar, detectar, conter e remediar ameaças de TI em aplicativos, dispositivos e sistemas críticos, em seus ambientes de nuvem pública e privada, bem como, em locais físicos.

2.4 Orquestração Automação e Resposta de Segurança (*SOAR*)

O *SOAR* como sendo: a coleção de tecnologias diferentes, que permitem às empresas coletar dados e alertas de segurança de diferentes fontes.

2.5 Gerenciamento de Informações e Eventos de Segurança (*SIEM)*

O *SIEM* oferece suporte à detecção de ameaças, conformidade e gerenciamento de incidentes, por meio da coleta e análise de eventos de segurança.

2.6 IBM Security X-Force

Esta ferramenta avalia o cenário de ameaças cibernéticas e auxilia as organizações a entenderem: as ameaças em evolução, seus riscos associados e como priorizar os esforços de segurança cibernética. Os invasores de *Ransomware* aumentaram a pressão para extorquir pagamento combinando criptografia de dados com ameaças de vazamento de dados em sites públicos.

2.7 Inteligência Artificial

Por ser mais rápida e eficiente do que ajustes manuais, a IA pode aumentar a efetividade de defesa, com os bloqueios realizados em tempo real, como uma postura pró-ativa.

3 CONCLUSÃO

O *COBIT* e a segurança cibernética acabam sustentando os impactos sobre as pessoas jurídicas, como, o sequestro vultoso de quantias das empresas. Ameaças internas têm o potencial de causar maior dano. Os invasores internos 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. *SOCs; SIEMs; SOARs; IBM Security X-Force; Inteligência Artificial* podem perder parte da efetividade, deixando de ser um forte aliado no combate a essas cepas de *Ransorware*. Que a inteligência artificial seja um divisor de águas, tanto para o bem, como para o mal. Notícia de procedimentos adversos, que se aperfeiçoam, mas aparece, em contra partida, defesas que aprendem sozinho, e podem bloquear esse ataque do *Malware Ransomware,* e que as máquinas sejam afetadas. Crê-se que os ataques ficaram mais difíceis de serem identificados, mas, quando se utilizam as ferramentas, que usam inteligência artificial para defender os servidores ou pontos de acesso, essas tarefas cada vez mais robustas tornam a cibersegurança mais eficiente.

REFERÊNCIAS

ALBERTIN, R. M. M.; ALBERTIN, A. L.. **Estratégias de Governança da Tecnologia da Informação: Estrutura e Prática**. RJ: ELSEVIER Editora Ltda, 2010.

BRASIIANO, A. **Risco no ar: Ataques cibernéticos, estratégia integrada**. #RisconoAR76, acessado em 15/01/2022

FERNANDES, A. A.; ABREU, V. D de. **Implantando a Governança de TI: da Estratégia à Gestão dos Processos e Serviços**. 3ª edição. RJ: BRASPORT, 2012.

GASETA, E. R.. **Fundamentos de Governança de TI**. Rio de Janeiro: RNP/ESR, 2011.

HIGH SECURITY CENTER - HSC. ***Ransomware Attack - Geração do Webinar***. – Disponível em: https://www.youtube.com/watch?v=lbL5WzYac1E – Acesso em: 24 Jan. 2022.

IBM SECURITY. ***X-Force Threat Intellgence Index***. [https://www.ibm.com/downloads/cas/M1X3B7QG], acesso em 25/01/2022.

ISACA®. ***Cibersecurity Nexus: Cybersecurity Fundamentals Study Guide*** *- 3nd edition*. USA: IL, 2015

ISACA®. ***CISM® Review Manual 15th Edition.*** USA: IL, 2015

ISACA®. COBIT® 2019 - ***FRAMEWORK: GOVERNANCE AND MANAGEMENT OBJECTIVES.*** USA: IL, 2018. ISBN 978-1-60420-764-4

ISACA®. ***Risk IT Framework 2nd Edition***. USA: IL, 2020. ISBN 978-1-60420-820-7

ISACA®. ***Transforming Cybersecurity: Using COBIT 5***. USA: IL, 2013.

ISACA®. ***COBIT 5 for Risk***. USA: IL, 2013. ISBN: 978-1-60420-458-2

ISACA®. ***COBIT 5 NA ISACA® FRAMEWORK*: Modelo Corporativo para Governança e Gestão de TI da Organização.** USA: IL, 2012. ISBN 978-1-60420-284-7

TECMASTER. ***Microsoft Defender* usa IA para prever ataques de *ransonware***. [https://tecmasters.com.br/microsoft-defender-ia-ransomware/], acesso em 25/01/2022.

VAST, R. *et al.* "***Artificial Intelligence based Security Orchestration, Automation and Response System***". 2021 6th International Conference for Convergence in Technology (I2CT), 2021.