UNIVERSIDADE FEEVALE

WILLIAM RIBEIRO DA SILVA

ISAI4E - INTERVENÇÃO PARA A MELHORIA DE CONSCIENTIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO

(Título Provisório)

Anteprojeto de Trabalho de Conclusão

Novo Hamburgo
2020

WILLIAM RIBEIRO DA SILVA

ISAI4E - INTERVENÇÃO PARA A MELHORIA DE CONSCIENTIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO

(Título Provisório)

Anteprojeto de Trabalho de Conclusão de Curso, apresentado como requisito parcial à obtenção do grau de Bacharel em Ciência da Computação pela Universidade Feevale

Orientador: Dr. Daniel Dalalana Bertoglio

Novo Hamburgo
2020

RESUMO

Nos dias atuais, é comum o uso da tecnologia para a otimização e agilidade de processos em um ambiente corporativo. Assim, manter a segurança e integridade de tais processos e suas informações têm se tornado um desafio maior a cada dia devido ao constante aperfeiçoamento das técnicas utilizadas por atacantes. Atualmente, uma das maiores ameaças de segurança aos computadores de uma organização está na forma em que os colaboradores os usam. Comportamentos como falta de informação, negligência, indiferença e apatia podem estar presentes e contribuir para tais ameaças. Sendo assim, se faz necessário que os gestores direcionem mais recursos a medidas que visam aumentar o nível de conscientização em assuntos que tangem a segurança da informação e privacidade em empresas e organizações. Há estudos que mostram que o uso de intervenções com o intuito de obter melhorias na conscientização de segurança da informação em equipes de colaboradores já se provou eficiente. Dessa forma, o presente trabalho tem como objetivo propor uma intervenção abordando a conscientização de segurança da informação, mensurando melhorias de forma quantitativa. Tal intervenção se dará por forma de treinamento/workshop, proporcionando uma imersão aos participantes, possibilitando que o período de execução chegue a semanas, e também que um acompanhamento da evolução e medição de melhorias seja documentada. Os workshops e demais atividades acontecerão após a aplicação de um questionário em uma amostra de voluntários. Os resultados serão medidos através de comparação entre as respostas dos questionários aplicados antes e depois dos workshops. A pesquisa, de natureza aplicada, será executada com procedimento quase-experimental.

Palavras-chave: Segurança da informação, conscientização, treinamento, intervenção, questionário.

SUMÁRIO

MOTIVAÇÃO

Antigamente, ao tratar aspectos de proteção e segurança de ativos e informações no âmbito empresarial, entendia-se que os problemas pertinentes a esses aspectos costumavam ser abordados sob um ponto de vista mais técnico e operacional. Contudo, devido às novas necessidades da segurança da informação, estudos apontam uma atenção especial das lideranças para com os comportamentos de seus colaboradores, de forma a avaliar e observar como estes podem influenciar tais problemas (SOOMRO; SHAH; AHMED, 2016).

De forma complementar, devido à maior segurança contra ataques remotos dedicada aos servidores das organizações, a fim de ganhar acesso à uma rede, atacantes têm direcionados seus vetores de ataques para os colaboradores das empresas, uma vez que as estações de trabalho comumente apresentam mais vulnerabilidades do que servidores. Documentos em PDF são regularmente utilizados em investidas contra usuários, visto que ainda existe um consenso de que a plataforma é segura e uma alternativa adequada para outras aplicações, como Microsoft Word (BRANDIS; STELLER, 2012). Assim, compreende-se que problemas relacionados a segurança da informação não podem ser resolvidos apenas com soluções técnicas, uma vez que muitos dos mesmos são provenientes de falha humana (PARSONS et al., 2013).

O estudo de Parsons et al. (2013) descreve três pesquisas que evidenciam os principais fatores que impactam a segurança da informação, embora não considerem o que os usuários pensam ou fazem no que diz respeito a essas falhas. A principal delas trata a abordagem de Deloitte (2013), que já foi criticada por apresentar falhas na metodologia, na elaboração dos questionários e nas estatísticas dos resultados encontrados. Há dados que demonstram que, por vezes, resultados inadequados provenientes de amostras tendenciosas foram obtidos. Também foi identificado que algumas perguntas do questionário não foram elaboradas de forma clara – isso fez com que os resultados destas perguntas apresentassem dados que podem ser interpretados de maneiras diferentes.

Em um estudo revisando metodologias utilizadas em pesquisas de segurança da informação, Guillot (2007) menciona que a pesquisa de Deloitte (2006) falhava em informar se os participantes tinham, ou não, acesso a resultados de auditorias internas ao responder as questões. A omissão desta informação levava a crer que a amostra escolhida para responder às questões podia ser tendenciosa e estar comprometida. A pesquisa não endereçava estes detalhes, o que comprometia sua credibilidade. Não obstante, algumas questões, que

originalmente visavam mostrar a usabilidade de uma determinada tecnologia ou ferramenta de segurança, falharam em provar que a implementação destas ferramentas foi executada corretamente.

Nesse sentido, a pesquisa realizada pela AusCERT (2006) apontava que 98% dos participantes afirmavam ter algum software de antivírus instalado em seus computadores. Contudo, a quantidade de ataques de vírus detectados passava dos 65%. Guillot (2007) criticava que estes resultados levariam a crer que, ao mesmo tempo, os restantes 35% dos participantes poderiam ter vivenciado ataques bem-sucedidos, ou que nenhum ataque fora detectado. Assim, a pesquisa da AusCERT (2006 apud Guillot, 2007) seria considerada incerta se o intuito era medir o número de ataques bem-sucedidos, ataques detectados ou o número de tentativas de ataque.

Adicionalmente, pesquisas patrocinadas por alguma marca ou empresa são comuns. Isso pode acabar causando resultados tendenciosos, considerando que cada organização tem seu próprio ponto de vista e agenda (ANDERSON et al., 2012).

Comumente, empresas que dependem de sistemas de informação e outras tecnologias possuem um departamento de TI que auxilia com tarefas diárias de manutenção de sistemas e estações de trabalho. Dentre outros, os processos comuns destas equipes envolvem a atualização de software de antivírus e sistemas operacionais, manutenção de firewall, backup de informações do computador dentre outros. Adicionalmente, em ambientes controlados pela empresa, em que alguns aspectos do manuseio do computador como padrões de senhas, limite de tempo ocioso e instalação de software podem ser controlados, um julgamento do funcionário pertinente a segurança não é necessário. Estes tipos de controles pela empresa, embora tragam mais segurança para o ambiente, acabam não aumentando a conscientização do funcionário pelo fato de tudo em sua volta estar sendo controlado (PARSONS et al., 2013).

Comportamentos dos funcionários podem ser influenciados por diversos fatores. Dentre eles, consegue-se destacar a personalidade, a própria empresa e sua cultura organizacional. (VROOM; VON SOLMS, 2004). Pode-se, então, destacar a importância de programas de conscientização referentes a segurança da informação, focando em aprimorar as medidas de segurança tomadas pelos colaboradores. Albrechtsen e Hovden (2010) e Parsons et al., (2013) expõem que o foco em uma política de treinamentos e conscientização dos colaboradores é capaz de resultar em uma incidência menor de vulnerabilidades de segurança provenientes de erro humano.

Albrechtsen e Hovden (2010) propuseram um estudo realizado através de uma intervenção em uma agência de administração pública Norueguesa. O objetivo da intervenção era mudar as atitudes dos colaboradores referentes à segurança da informação através de workshops formados por grupos de 15 a 20 indivíduos cada, atingindo um total de 100 colaboradores. Os workshops foram executados com um formato de fórum aberto, onde todos os indivíduos poderiam expressar suas opiniões e visões sobre o tópico da conscientização de segurança da informação. Adiante, perguntas contendo situações de possível risco foram apresentadas ao grupo. O objetivo era que os membros do workshop apresentassem suas opiniões e debatessem maneiras de superar esses riscos. Para medir se o nível de conscientização em segurança da informação sofreu melhorias, um teste com perguntas associadas a segurança da informação foi aplicado no grupo que passou pelo processo de intervenção.

O estudo de Albrechtsen e Hovden (2010) obteve resultados positivos ao apresentar progresso no nível de conscientização de segurança da informação. Majoritariamente, os resultados obtidos apresentaram melhorias. Por exemplo, o grupo apresentou uma melhora de 4.03 para 4.27 na questão relacionada a reportar incidentes de segurança. Melhorias também foram reportadas quanto ao ato de bloquear o computador ao se ausentar da estação de trabalho. Os índices mudaram de 2.39 para 3.35. Mais adiante, efetuando o teste novamente seis meses após o estudo, os resultados de melhoria se mantiveram. Foi possível também se notar um avanço na conscientização do grupo de controle, o qual não passou pelo processo de intervenção.

Os workshops executados por Albrechtsen e Hovden (2010) ocorreram apenas uma vez com cada grupo de colaboradores, fazendo com que a intervenção durasse um período curto de tempo. O presente trabalho pretende executar uma intervenção mais longa, utilizando de práticas tais como entrevistas, workshops, questionários e chats, proporcionando uma imersão ao participante, possibilitando que o período de execução chegue a semanas. O intuito de se tomar um período mais longo de execução de intervenção é poder acompanhar a evolução do participante, dessa forma tentando evitar que falsos positivos surjam.

Já o estudo de Parsons et al., (2013) apresenta uma pesquisa voltada a quantificar as vulnerabilidades no aspecto de segurança da informação causadas por erros humanos. Dessa forma, os autores desenvolveram o *Human Aspects of Information Security Questionnaire* (HAIS-Q). Em sua primeira parte, o estudo visou provar o conceito do questionário. Futuramente, em uma pesquisa realizada com 500 trabalhadores australianos, os resultados

apontaram que colaboradores portadores de conhecimento em processos e políticas de segurança da informação apresentavam melhores atitudes conexas a incidentes de segurança. Ao mesmo tempo, os resultados do estudo mostraram que o conhecimento em políticas e procedimentos tiveram mais impacto na atitude dos colaboradores em relação a estes aspectos comparado ao comportamento auto-reportado.

A fim de validar ainda mais a eficácia do questionário HAIS-Q, um novo estudo foi efetuado no ano de 2017. 112 estudantes responderam ao questionário, e, mais adiante, participaram de um experimento voltado a ataques do tipo *phishing*. Os resultados mostraram que estudantes que obtiveram maiores notas no questionário HAIS-Q também obtiveram uma melhor performance no experimento, provando, assim, que o HAIS-Q pode fornecer informações que ajudem a predizer a atitude de um indivíduo frente a um incidente de segurança (PARSONS et al., 2017).

A partir disso, este trabalho objetiva compreender as lacunas presentes na conscientização dos tópicos que afetam a segurança da informação, por parte das pessoas/colaboradores, em ambientes corporativos. Do mesmo modo, visa propor uma intervenção em formato de treinamento/workshop para abordar a conscientização de segurança da informação de modo a mensurar os ganhos, melhorias e demais critérios que podem ser atingidos por essa intervenção. Tais melhorias serão mensuradas comparando os resultados do questionário aplicado no início do estudo com os resultados do questionário realizado na amostra de voluntários que participaram do workshop. Portanto, este estudo é norteado pela seguinte questão de pesquisa: “Como capacitar pessoas/colaboradores de modo a desenvolver conhecimentos específicos da área de Segurança da Informação que possam contribuir com a cultura de segurança e privacidade no âmbito empresarial?”.

OBJETIVOS

Propor uma intervenção em formato de treinamento/workshop para abordar a conscientização de segurança da informação de modo a mensurar os ganhos, melhorias e demais critérios que podem ser atingidos por essa intervenção.

Objetivos específicos:

- Analisar estudos que abordam a conscientização de segurança da informação;
- Identificar as principais lacunas na conscientização de segurança da informação;
- Investigar formas de conscientização;
- Desenvolver uma intervenção para a conscientização de segurança da informação;
- Selecionar os grupos participantes da pesquisa;
- Executar intervenção a proposta nos grupos participantes;
- Utilizar questionários como instrumento para validações da intervenção proposta.

METODOLOGIA

Este trabalho tem como objetivo propor uma intervenção em formato de treinamento/workshop para abordar a conscientização de Segurança da Informação e visa responder a seguinte questão de pesquisa: “Como capacitar pessoas/colaboradores de modo a desenvolver conhecimentos específicos da área de Segurança da Informação que possam contribuir com a cultura de segurança e privacidade no âmbito empresarial?”. Em sua natureza, a pesquisa é definida como aplicada, visto que, segundo Prodanov e Feitas (2013), a pesquisa aplicada objetiva gerar conhecimentos para a aplicação prática dirigida a solução de problemas específicos.

Será realizada uma revisão de literatura para identificar as principais lacunas na conscientização dos aspectos que afetam a Segurança da Informação em ambientes corporativos. Além disso, em seguida, será elaborado um questionário e um treinamento a ser aplicado em um grupo formado por voluntários que ocupem cargos em ambientes corporativos e executem suas tarefas diárias em computadores. Para a coleta de dados da revisão da literatura, serão realizadas pesquisas nas bases de dados Science Direct, IEEE, Springer e ACM. Os descritores que serão utilizados nas bases serão “*information security*”, “*awareness*” e “*enterprise*”, sendo possível adicionar novos descritores para refinar os resultados. Além disso, os artigos científicos serão pesquisados utilizando filtros como ano de publicação, autor, idioma, relevância, etc.

A próxima etapa da pesquisa, será a leitura dos resumos e conclusões dos artigos científicos obtidos nas bases de dados. Após o entendimento de que os mesmos têm relevância para a pesquisa, será feita a leitura completa dos artigos. Subsequentemente, de forma qualitativa, serão documentados os resultados e conclusões obtidas nos artigos estudados como, por exemplo, lacunas, dificuldades, limitações e etc. Tais resultados serão utilizados de modo que um plano de intervenção possa ser construído e, posteriormente, implementado.

O plano de intervenção consistirá, primeiramente, na aplicação de um questionário em um grupo de voluntários, dos quais será selecionada uma amostra para a aplicação de um treinamento em Segurança da Informação. Adiante, a amostra selecionada para o treinamento passará pelo questionário uma segunda vez. De forma quantitativa, os resultados dessa pesquisa serão tabelados e analisados, de maneira que seja possível medir se o nível de conscientização em Segurança da Informação sofreu alteração. Tal intervenção caracteriza o

procedimento como Quase-Experimental, dado que o presente trabalho constitui uma classe de estudos de natureza empírica sem um controle completo do ambiente e sem randomização de amostra participante e grupo de controle (CAMPBELL; STANLEY, 1979).

Tipo de Pesquisa			Características		
Quanto à Natureza	Quanto à Forma de Abordagem do Problema	Quanto aos Fins da Pesquisa	Quanto aos Procedimentos	Gerais	Tipos de instrumento
BÁSICA	QUANTITATIVA	EXPLORATÓRIA	Bibliográfica	- Base em material já elaborado	Fontes Bibliográficas
			Documental	- Materiais que não receberam tratamento analítico ou podem ser reelaborados - Efeitos de variável – formas de controle	Fontes Secundárias de dados
APLICADA	QUALITATIVA	DESCRITIVA	Experimental	- Verificar a relação entre variáveis	Plano da pesquisa – Manipulação de condições e observação dos efeitos produzidos
			Quase-Experimental		
			Ex-Post-Facto	- Conhecer Comportamento Interrogação Direta	Observação, questionário e entrevistas
			Levantamento	- Idem levantamento – um grupo ou uma comunidade - Estudo aprofundado de um ou poucos objetos	Questionário, entrevista e formulário
		EXPLICATIVA	Estudo de Campo		Variados - Questionário, entrevistas, formulários e observação
			Estudo de caso		Várias técnicas

CRONOGRAMA

Trabalho de Conclusão I

Etapa	Meses			
	Mar	Abr	Mai	Jun
Coleta de artigos em base de dados	X	X		
Leitura de resumos/conclusões e exclusão de artigos baseados nos critérios	X	X		
Documentação dos resultados e conclusões da pesquisa bibliográfica		X	X	X
Escrita do TC I		X	X	X
Revisão do TC I		X	X	X
Entrega do TC I				X

Trabalho de Conclusão II

Etapa	Meses			
	Ago	Set	Out	Nov
Análise do questionário	X			
Elaboração do treinamento	X	X		
Aplicação do questionário		X		
Aplicação do treinamento em amostra		X		
Aplicação do questionário em amostra treinada		X		
Organização e análise de dados obtidos		X	X	X
Escrita do TC II	X	X	X	X
Revisão do TC II	X	X	X	X
Entrega do TC II				X

BIBLIOGRAFIA

ALBRECHTSEN, Eirik; HOVDEN, Jan. **Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study.** Computers & Security, [s.l.], v. 29, n. 4, p. 432-445, jun. 2010.

ANDERSON, Ross; BARTON, Chris; BÖHME, Rainer; CLAYTON, Richard; VAN EETEN, Michel J. G.; LEVI, Michael; MOORE, Tyler; SAVAGE, Stefan. **Measuring the Cost of Cybercrime. The Economics Of Information Security And Privacy**, [s.l.], p.265-300, out. 2013. Springer Berlin Heidelberg.

CAMPBELL, D.T.; STANLEY, J. C. **Delineamentos Experimentais e Quase-experimentais de Pesquisa.** São Paulo: Editora Pedagógica e Universitária, 1979.

DELOITTE (Reino Unido). **Global Security Survey**. Londres, 2006. Disponível em: <https://web.archive.org/web/20060701083330/http://www.deloitte.com/dtt/cda/doc/content/dtt_fsi_2006%20Global%20Security%20Survey_2006-06-13.pdf>. Acesso em: 26 mar. 2020.

DELOITTE (Reino Unido). **Raising the Bar. 2011 TMT Global Security Study – Key Findings.** Holanda, 2013. Disponível em: <https://www2.deloitte.com/ug/en/pages/technology-media-and-telecommunications/articles/2013-tmt-global-securitystudy.html>. Acesso em: 26 mar. 2020.

GUILLOT, Alexis; KENNEDY, Sue. **Information Security Surveys: A Review of the Methodologies, the Critics and a Pragmatic Approach to their Purposes and Usage**. In: AUSTRALIAN INFORMATION SECURITY MANAGEMENT CONFERENCE, 5., 2007, Perth. **Proceedings of The 5th Australian Information Security Management Conference.** Perth: Edith Cowan University, 2007. p. 61 - 72.

PARSONS, Kathryn; MCCORMAC, Agata; BUTAVICIUS, Marcus; PATTINSON, Malcolm; JERRAM, Cate. **Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security**, [s.l.], v. 42, p.165-176, maio 2014.

PARSONS, Kathryn; CALIC, Dragana; PATTINSON, Malcolm; BUTAVICIUS, Marcus; MCCORMAC, Agata; ZWAANS, Tara. **The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers & Security**, [s.l.], v. 66, p. 40-51, maio 2017

SOOMRO, Zahoor Ahmed; SHAH, Mahmood Hussain; AHMED, Javed. **Information security management needs more holistic approach:** A literature review. **International Journal Of Information Management**, [s.l.], v. 36, n. 2, p.215-225, abr. 2016.

VROOM, Cheryl; VON SOLMS, Rossouw. **Towards information security behavioural compliance. Computers & Security**, [s.l.], v. 23, n. 3, p.191-198, maio 2004.