INSEGURANÇA DE TI EM ÓRGÃOS MUNICIPAIS DE ATENDIMENTO AO PÚBLICO.

Autoria: Kauan Richard Alves Souza, Leonardo Marzochi

Curso Superior de Tecnologia em Segurança da informação – Faculdade de Tecnologia de Americana (FATEC Americana)
Americana – SP - Brasil

kauan.r.a.s@gmail.com, leomarzochi@gmail.com

Resumo. *Este artigo trata-se dos problemas nas estruturas de TI em órgãos municipais principalmente os que envolvem dados de seus cidadãos e a necessidade de uma disponibilidade alta, logo definisse que necessita de uma noção de segurança de informação tanto por seus gestores quanto por seus funcionários, que as vezes nem conhecimento básicos dos riscos que uma má administração das informações podem trazer, que por sua vez pode ser usada por pessoas com más intenções, como exemplo: Uma pessoa má intencionada invade uma sistema municipal e coleta dados como CPF, RG e endereço de uma pessoa qualquer, logo o mesmo usa dessas informações para aberturas de contas bancárias, falsificação de documentos ou causar indisponibilidade nos serviços.*

Abstract. *This article deals with the problems in IT structures in public agencies especially those involving data of its citizens and the need for high availability, thus defining that it needs a notion of information security both by its managers and by its employees, that sometimes the basic knowledge of the risks that a bad administration of the information can bring, that in turn can be used by people with bad intentions, for example: A malicious person invades a municipal system and collects data like CPF, RG and address of any person, so he uses this information to open bank accounts, falsify documents or cause unavailability in the services.*

Fatec Americana — Centro Paula Souza — Governo do Estado São Paulo

Faculdade de Tecnologia de Americana

Kauan Richard Alves Souza
Leonardo Marzochi

INSEGURANÇA DE TI EM ÓRGÃOS MUNICIPAIS DE ATENDIMENTO AO PÚBLICO.

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana.
Área de concentração: Segurança da Informação

Americana, 07 de dezembro de 2018.

Banca Examinadora:

Edson Roberto Gaseta (Presidente)
Especialista
Faculdade de Tecnologia de Americana

Henry Alves de Godoy (Membro)
Mestre
Faculdade de Tecnologia de Americana

Márcio Roberto Baldo Taglietta (Membro)
Especialista
Faculdade de Tecnologia de Americana

1. Introdução

A segurança da informação vem se tornando um dos maiores marcos na época atual, devido ao fato da quantidade de informação manipuladas atualmente, se comparada com as passadas, cresceram disparadamente, não apenas em quesitos de informações empresariais, mais também em informações pessoais, como por exemplo, nas redes sociais, onde encontram-se informações de uma pessoa, como número de telefone, endereço, gostos, dentre outros.

A importância da segurança das informações, sejam elas privadas ou públicas, se tornaram uma obrigação, tanto por parte dos órgãos responsáveis pelo armazenamento da mesma, quanto pelo usuário que a disponibiliza, afim de ter a garantia de que as informações se mantenham seguras de pessoas com más intenções e para que sempre mantenham estes serviços funcionando.

Segurança em TI (Tecnologia da Informação) não se trata apenas de integridade, mas também de confidencialidade e disponibilidade. Casos como o ocorrido no hospital do Câncer de Barretos (GUIMARÃES, 2017) mostram claramente a importância de manter as informações disponíveis e funcionando, pois, além de impactar os usuários do hospital, impactam também sua credibilidade, além das multas, processos, entre outros. Com ataques *hackers* deste tipo, ter uma infraestrutura de TI adequada se torna uma necessidade na qual não se pode ignorar.

2. Referencial Teórico

2.1. Tipos de ataques que ocorrem em órgãos públicos e/ou privados.

Ciberataques são feitos a empresas todos os dias, de acordo com o relatório anual de cibersegurança da Cisco de 2017, o total de eventos desse tipo aumentou cerca de quatro vezes entre janeiro de 2016 até outubro de 2017, ainda sobre esse relatório, os ataques mais comuns são, *Ransomware*, *Phishing* e DDoS (Ataque de negação de serviço).

O vírus chamado *Ransomware*, é um ataque com intuito de sequestrar dados, uma vez dentro da rede ele criptografará todos os arquivos, tornando-os inacessíveis. Esse ataque é causado por *crackers* com a intenção de lucrar com o roubo de dados. A contaminação poderá ocorrer através de um anexo de e-mail, através do navegador ou até mesmo por um *pendrive* infectado. Ele pode ainda acessar mais computadores através da rede. Este malware criptografa os dados contidos na máquina infectada e cobra um resgate para devolvê-los, geralmente um pagamento por moedas virtuais, o mais comum sendo o *Bitcoin*, caso a empresa não tenha uma política de backup, a mesma pode não ter escolha a não ser pagar o resgate por seus dados. Porém não existe garantia que ao fazer o pagamento do resgate, seus dados serão liberados.

O ciberataque *Phishing*, é um ataque que tem o objetivo coletar informações e dados pessoais importantes através de mensagens falsas, com a finalidade de conseguir nomes de usuários, senhas, dados de contas bancárias e cartões de crédito, entre outros. Este ataque pode ocorrer de diversas maneiras, sendo mais comum envios de e-mails, propagandas em sites, promoções, conversas falsas, que induzem a vítima entrar em um link malicioso, onde é redirecionado para uma página falsa, assim o atacante pode coletar as informações da vítima.

O ataque cibernético DDos (um acrônimo em inglês para *Distributed Denial of Service*) é um ataque de negação de serviço, ou seja, torna um site ou sistema web indisponível. O ataque funciona da seguinte forma: O cliente principal do *cracker* submete várias máquinas ao seu controle e as fazem acessar um recurso em um determinado servidor todos na mesma faixa de tempo, assim, todos os clientes submetidos ao *cracker* acessam juntamente e de maneira ininterrupta o mesmo recurso de um servidor. Os servidores web possuem um número limitado de usuários que podem acessar seus recursos ao mesmo tempo, sendo assim, o ataque impossibilita que o servidor seja capaz de atender a qualquer outro pedido. O servidor pode reiniciar ou mesmo ficar travado dependendo do recurso.

Diariamente tanto órgãos públicos como órgãos privados recebem vários tipos de tentativas de invasões, contudo, esses são os ataques mais comuns por serem ataques de grande escala.

2.2. Ataque hacker em escala mundial 2017

Dois casos específicos ajudaram com a elaboração deste artigo. Em 2017 o mundo foi surpreendido com um ataque em massa afetando computadores em diversos países, entre eles, o Brasil.(PITAS e RUANO, 2017) tivemos em alto destaque aos órgãos públicos Brasileiros atingidos pelo *WannaCry* (*Ransomware* responsável pelo sequestro) onde, por exemplo, o Tribunal de Justiça de São Paulo teve mais de dois mil computadores afetados, cerca de 2% do total de seus computadores (CAPELAS, 2017). Neste mesmo ano houve um ataque cibernético que chamou atenção de todos, o ataque foi direcionado ao Hospital do Câncer de Barretos, onde várias filas de esperas cresceram, e pacientes de quimioterapia tiveram seu tratamento interrompido (GUIMARÃES, 2017). Ambos os ataques tiveram reflexo em todo sistema público mostrando assim a fragilidade deles perante a tecnologia.

Segundo o analista da empresa de antivírus *Kaspersky* nem todos os órgãos do governo vem a segurança da informação como algo vital, juntando isso a máquinas defasadas, que não recebem mais atualizações e que, por questões de burocracia, não podem ser descartadas, continuam sendo usadas.

4. Metodologia

Para alcançar o objetivo estabelecido, foi utilizada uma pesquisa qualitativa e quantitativa, onde na fase inicial da pesquisa, foi realizada uma pesquisa exploratória.

A pesquisa exploratória foi aplicada em um município de médio porte da Região Metropolitana de Campinas, com cerca de 230.000 habitantes. Dividida em duas fases, onde a primeira foi coletar informações com o coordenador de Tecnologia da Informação (TI) no Hospital Municipal, assim como, realizar alguns questionamentos sobre a funcionalidade da infraestrutura de TI do local. A segunda parte foi uma coleta de informações com funcionários públicos de diversos setores do município que executam atividades diárias de atendimento ao público, onde também armazenam informações pessoais dos usuários. Este levantamento de informações teve como finalidade obter a opinião dos funcionários, referente aos equipamentos de infraestrutura como, computadores, notebooks e Internet, e como o agente público lidava com a segurança das informações obtidas, assim como, saber se o funcionário recebeu ou recebe algum treinamento em questões relacionadas à segurança da informação.

A segunda parte foi realizar pesquisas de casos que ocorreram envolvendo órgãos públicos como o hospital de Câncer de Barretos, e quais as consequências tiveram após o ocorrido.

Com base nas informações coletadas, foram realizadas análises para dar continuidade na nossa pesquisa levantando gráficos e tabelas para demonstrar o nível da segurança em TI.

Por fim foi realizado um plano elaborado de uma possível solução tendo em mente questões financeiras dos municípios e questões divergentes como a falta de qualificação dos usuários.

5. Análise e interpretação dos resultados

5.1. Levantamento de informações com funcionários públicos

Foi realizada uma pesquisa de campo com a finalidade de levantar informações sobre o nível de segurança, capacitação e condições da infraestrutura de TI. O levantamento levou em consideração a opinião de treze servidores públicos.

De acordo com o levantamento feito, a Secretaria da Educação do município recebeu verba recentemente, viabilizando assim a troca dos equipamentos das escolas, equipamentos estes que se encontravam defasados, prejudicando assim, a segurança do ambiente. A secretaria possui um computador simples com configurações medianas que funciona como um servidor *proxy*, qualquer pessoa do local consegue acesso a essa máquina, ignorando dessa forma qualquer política de acesso, a secretaria também possui

um *fileserver*, o funcionário não pode dar mais informações sobre o mesmo, apenas que os arquivos pessoais como cadastros de alunos e professores, encontravam-se neste servidor. Além disso, ele reportou não haver *backup* das configurações dos computadores das salas de informática nas escolas do município, como por exemplo as regras de acesso, portanto, quando apresentado problema, toda a rede deverá ser configurada novamente, causando indisponibilidade do serviço durante alguns dias. O funcionário presente também informou não haver senha para acesso aos computadores da secretaria, ficando essa senha a critério do próprio usuário. Um ataque que cause indisponibilidade ou sequestro de informações na Secretaria de Educação não teria um impacto financeiro expressivo no município, mas em contrapartida, haverá um grande impacto moral.

O levantamento de informações também mostrou que a Secretaria de Ação Social possui seus servidores junto ao setor de TI do município, a política de *backup* da secretaria funcionada da seguinte forma: O backup das máquinas dos usuários que atendem ao público é realizado através de uma pasta compartilhada na rede, onde, em todo fim de expediente os usuários copiam os arquivos de sua máquina para essa pasta, e o setor de TI do município fica responsável por realizar o *backup*, o problema encontrado foi que, todas as secretarias fazem o *backup* na mesma pasta da rede, desta forma, outras secretarias tem acesso as informações que eles coletam e vice-versa, com exceção dos cadastros como Bolsa Família, Cadastro Único e Minha Casa Minha Vida, que são tratados pela Caixa Econômica Federal, sendo assim de responsabilidade da mesma, e que a Caixa disponibiliza curso para o tratamento destas informações.

O levantamento de informações do Hospital Municipal do município mostrou que o local possui um servidor de arquivos, um servidor de *backup*, um servidor de *proxy* e um servidor de firewall desenvolvido em Linux por eles mesmos, logo, estes servidores se tornam independentes da gestão do setor de TI do município. Esses servidores se localizam em uma sala refrigerada que funciona como um *data center*, porém, sem seguir o padrão implantado pela norma ANSI/TIA-942 (2014). Começando pelo controle de acesso no local, que por sua vez, é realizado apenas por chave e cadeado, impossibilitando assim uma auditoria em caso de acesso físico não permitido.

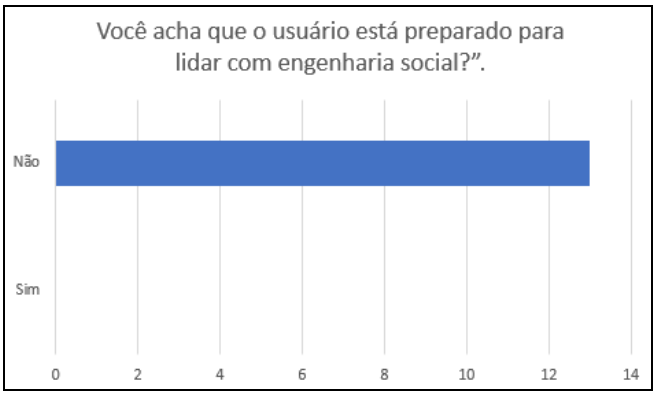
O backup dos arquivos é realizado em fitas de backup, onde ficam armazenadas na sala ao lado, o que por sua vez não é recomendado, pois se houver um incidente no local há possibilidade de afetar a sala onde as mídias encontram-se, fazendo com que todos os arquivos sejam perdidos. O local encontra-se em situação precária, com o forro do teto caindo, fiação elétrica e cabeamento da rede exposta, o que pode gerar início de incêndio, não afetando apenas a infraestrutura, mas também todos equipamentos hospitalares, assim como os usuários do hospital. De acordo com as informações coletadas, o hospital abre em média 400 fichas de pacientes por dia, sendo que uma possível parada neste serviço irá ocasionar um grande atraso no atendimento, e impossibilitar a continuidade dos usuários que já foram atendidos, além disso, o hospital não possui um plano de ação em caso de desastres. Foi constatado que a troca frequente de secretários no local prejudica a gestão de TI, por ser um cargo preenchido por

indicação, muitas vezes esse novo secretário não possui conhecimentos técnicos em informática nem do real valor da segurança da informação.

Ao analisar as informações coletadas, é possível notar que um eventual ataque pode causar grande impacto financeiro e moral ao município, diminuindo a credibilidade da gestão, fazendo com que os usuários do serviço público se mostrem descontente, e cause um grande gasto financeiro para a cidade.

Também foi levantado a seguinte questão: "Você acha que o usuário está preparado para lidar com engenharia social?". Houve uma resposta única: "Não":

Figura 1: Questão apresentado aos funcionários do município.

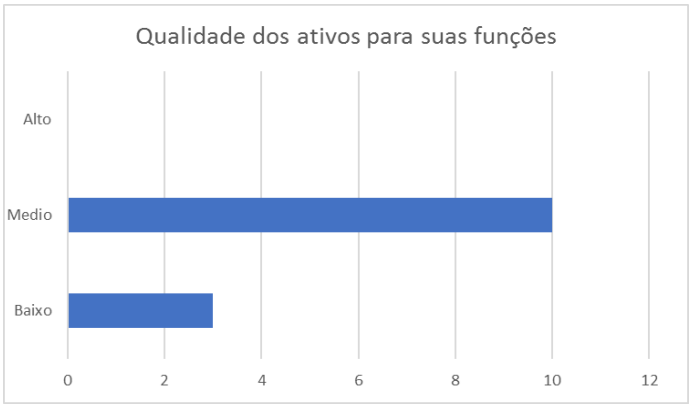


Fonte: Próprio autor

Os servidores públicos que fizeram parte do levantamento disseram que o usuário que não recebe treinamento básico seria facilmente suscetível a esse tipo de ação. Dentre os setores analisados o único que tinha um melhor treinamento para esse tipo de ataque, foi o setor de Ação Social, pois a Caixa Econômica Federal prepara os usuários de seus sistemas.

Por fim foi levantado informações sobre a qualidade dos equipamentos:

Figura 2: Qualidade dos ativos para suas funções



Fonte: Próprio autor

Dos 13 funcionários que colaboraram com levante de informações, três deles opinaram como nível baixo de qualidade dos ativos disponíveis. Já a maioria (10) opinou por um nível médio, ou seja, os ativos realizam as atividades, porém, não são os melhores para elas.

5.2. Aumentos nos casos de ataques a órgãos públicos

Por tratar-se de um estudo censitário, foram avaliadas diversas notícias de ataques cibernéticos mais realizados que envolveram órgãos públicos e privados de diversas áreas, e consecutivamente suas consequências.

As notícias abordam ataques que envolvem diversas entidades e a porcentagem que a mesma vem crescendo referente ao ano anterior, conforme tabela 1. Do ano de 2016 para 2017, a quantidade de tentativas de ataques DDOS que já ocorreram chega a aumentar em 400%.

Tabela 1: Porcentagem de crescimento de ataques cibernéticos em relação aos anos anteriores

Tipos de ataques	2015 - 2016	2016 - 2017
Ataques por ransomware	30%	55%
Ataques por malware	31%	49%
DDoS (sites)	138%	400%
Phishing (email)	39%	44%

Fonte: Próprio autor

Nota-se que neste levantamento os ataques virtuais cresceram em grande escala se comparado aos anos anteriores, a expetativa segundo a DFNDR Lab é de que esse número cresça cerca de 70% nos próximos 3 semestres (CANDEIRAS, 2017)

Logo, vemos que o Brasil vem se tornando um grande alvo de ataques, isso devido ao seu péssimo investimento em tecnologia, o que impossibilita novos meios de proteção contra invasões desses níveis. Segundo um estudo realizado pela *Karpersky* (2018), o Brasil é o 6º no ranking dos países que mais sofrem ataques cibernéticos no mundo. Em 2015 o país ocupava a 10º posição na lista, perdendo apenas para países como: Rússia, Ucrânia, China, Índia e México (FLORENZANO, 2018)

Outro estudo realizado, porém, desta vez pela empresa Norton, afirma que o porcentual de habitantes com acesso à internet prejudicados por crimes virtuais no Brasil é maior do que a média mundial, o que coloca o país entre os mais afetados por este tipo de ação. Pesquisas realizadas em 2016 mostram claramente a gravidade desses ataques.

Ao analisar o setor público, vemos que continuamente, os mesmos sofrem com ataques a infraestruturas, o que vem se tornando mais grave a cada dia. Casos são inúmeros: em 2012, por exemplo hackers do grupo Anonymous tirou do ar o site do Banco do Brasil. Poucos dias depois foi a vez dos sites do governo da Bahia, da Secretaria da Fazenda e da Assembleia Legislativa do Estado. Esse tipo de ataque é conhecido como DDoS, por sua vez ele controla diversas máquinas conhecidas como máquinas *zombie* e acessam um recurso todas de uma vez fazendo assim que o mesmo fique fora de ar.

Em 2014, e-mails e sistemas de dados do Ministério das Relações Exteriores do Brasil sofreram um ataque cibernético onde os atacantes invadiram a intranet que reúne todas as comunicações diplomáticas, até mesmo as sigilosas, e divulgaram estas informações (G1, 2017)

Porém isso não ocorre apenas no Brasil. Em 2015 mais de 4 Milhões de funcionários americanos tiveram seus dados expostos por hackers chineses, pouco tempo despois de dados do Departamento do Interior e da Agências de Gerencialmente Pessoal também serem comprometidos. Contudo diferente do Brasil o governo norte americano contratou uma empresa especializada em proteção contra roubo de identidade.

5.3.1 Ataques que levaram a este artigo

Em 2017, houveram 2 ataques em específicos que deixaram sua marca neste ano. O primeiro deles, foi o ataque que prejudicou por volta de 100 países no mundo e ocorreu no dia 12 de maio de 2017.

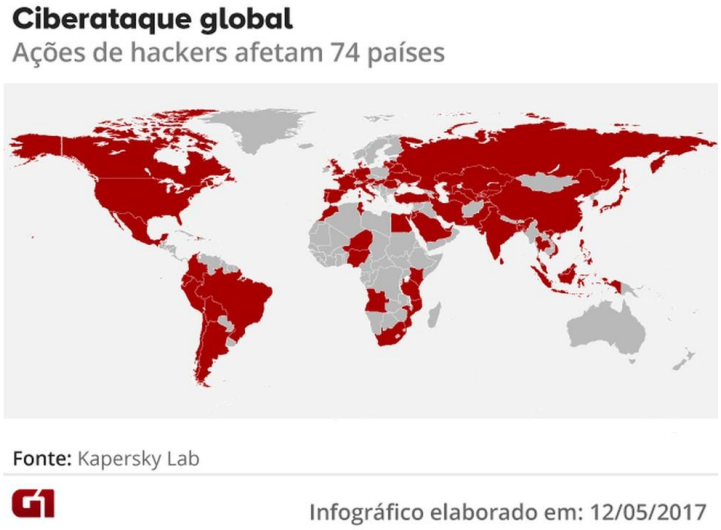
Um ataque sem precedentes, de forma coordenada atingiu empresas e órgãos públicos do ao redor do mundo, foi utilizado ferramentas vazadas anteriormente da NSA (Agência de Segurança Nacional Americana) através dele os criminosos

criptografaram arquivos de computadores, inutilizando sistemas, assim como seus dados.(BERCITO, 2017) após a criptografia dos dados os *crackers* pediram um regate com a quantia média de US$ 400 dólares em *bitcoins*.

No Brasil foram 14 órgãos públicos afetados por este ataque, dentre eles tribunais de justiça e ministérios, levando a desligarem seus computadores e tirarem seus sites do ar.

De acordo com a GSI (Gabinete de Segurança Institucional) as invasões ocorrem por meio de e-mails com arquivos infectados com o vírus que se espalhou através de uma brecha no Windows que a Microsoft alegou ter arrumado dia 13 de março deste mesmo ano. Porém aqueles que não atualizaram seus computadores foram infectados da mesma maneira.

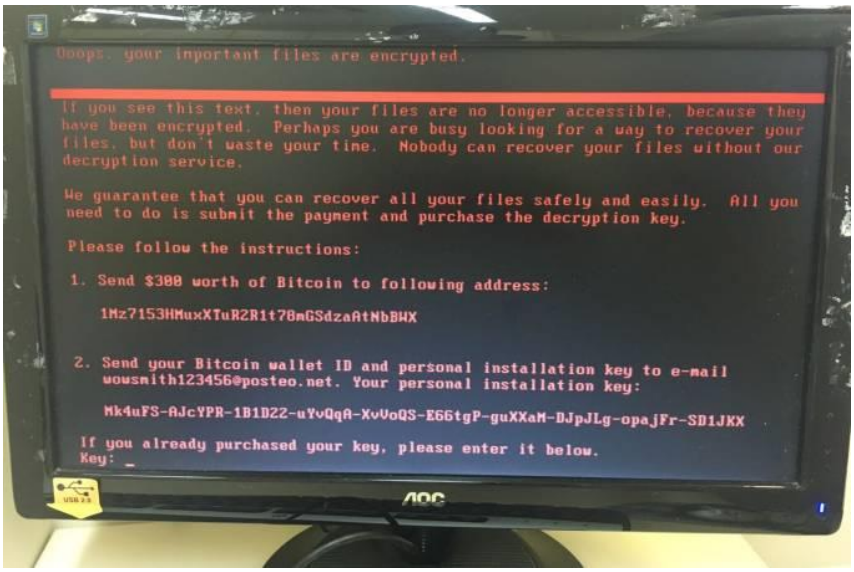
Figura 2: Ações de hackers afetam 74 países



Fonte: Portal G1 2017

O outro ataque cibernético que levou a este artigo foi o ataque que aconteceu dia 27 de junho de 2017 no Hospital de Câncer de Barretos/SP, neste ataque os invasores utilizaram o mesmo método de *ransomware* que ocorreu anteriormente, os *crackers* "sequestraram" os dados e solicitaram um resgate por computador de US$ 300 em *bitcoins* (o equivalente a R$ 995,40, ao câmbio daquela época), como o hospital obtinha cerca de mil computadores infectados o valor total serial de R$ 995,4 mil (FRANZÃO, 2017)

Figura 03: Tela de computador invadido por hackers no Hospital de Câncer de Barretos (SP)



Fonte: Veja (2017)

Como resultado, os funcionários passaram a trabalhar em formulários manuais o que deixou o serviço muito lento, levando a mais de 3000 consultas canceladas, além disso, cerca de 350 pacientes tiveram seus exames prejudicados. O ocorrido levou cerca de cinco dias para se normalizar, o que gerando grande descontento pela população principalmente devido ao fato de envolver pessoas com câncer em um nível avançado, o que poderia ter resultado em uma catástrofe ainda maior (GUIMARÃES, 2017)

O pagamento não foi realizado, devido a um conselho de Fabio Assolni (Analista da empresa de antivírus Kaspersky). De acordo com ele: "O pagamento para reativar o acesso a computadores equivale a negociar com bandidos e deve ser evitado, pois leva a influência de outros hackers para praticarem o mesmo". Ele mostrou que se pode ter outras alternativas que não sejam negociações pois a mesmas pode influenciar cada vez mais hackers a invadires outros órgãos públicos.

5. Conclusão e proposta de continuidade do trabalho

Este levantamento de informações mostra claramente alguns pontos que precisam ser melhorados na segurança da informação em órgãos municipais, sendo que em alguns casos, um possível ataque realizados por hackers, pode gerar um grande problema como visto anteriormente. Deve ser levado em conta que todos os dados são importantes, os mesmos podem prejudicar um projeto público ou como ocorreu em Barretos/SP (2017), inutilizar um sistema de atendimento ao público. Investir em segurança da informação tem um custo, e que por muitas vezes se torna difícil ao profissional de TI conseguir aprovação para um projeto de melhorias, contudo, há algumas maneiras para evitar vulnerabilidades a serem exploradas, de maneira mais atrativa para o setor financeiro.

A proposta de capacitação continua do funcionário público em habilidades práticas para o uso de ativos e prevenção de ataques, pode ser aplicada de maneira que não gere um grande custo financeiro. Essa capacitação profissional vai desde a profissional base até a administração, sendo que ambos irão aprender técnicas e maneiras corretas para com a segurança, com o uso de ativos e com seus dados. A proposta de continuidade deste trabalho, trata – se de uma plataforma de ensino EAD (Ensino a distância), como já existe atualmente em órgãos privados. O setor de TI do município, consegue disponibilizar cursos de aprendizagem, onde os funcionários podem aprender a lidar com os ativos que eles usam, e com isso torna-los mais aptos perante a segurança de informação. Em órgãos privados esses cursos são utilizados para ensinar aos usuários a não deixarem senhas expostas na mesa, não divulgar informações por telefone, manter seus dados organizados, reconhecer um alerta ou uma mensagem de spam, dentre outras boas maneiras com o uso de ativos. Esses cursos também são de caráter obrigatórios e geram certificações no final de cada um deles. Com essa proposta é possível diminuir uma grande vulnerabilidade, ensinar boas práticas e preparar os funcionários públicos para possíveis tentativas de invasões.

Referências

ARCON - Os desafios enfrentados pelos órgãos públicos para proteger seus dados, **Arcon Serviços Gerenciados de Segurança 25 de fevereiro de 2018**. Disponível em: < https://www.arcon.com.br/blog/os-desafios-enfrentados-pelos-orgaos-publicos-para-proteger-seus-dados> 05 de mai de 2018.

BERCITO, D - Onda de ciberataques atinge órgãos e empresas em ao menos 74 países, **Folha de S.Paulo, 12 de maio de 2017.** Disponível em: <www1.folha.uol.com.br/mundo/2017/05/1883408-mega-ciberataque-derruba-sistemas-de-comunicacao-ao-redor-do-mundo.shtml> Acesso em 13 out de 2018.

CANDEIRAS, H - Relatório DFNDR Lab aponta para um crescimento de 44% em ciberataques no Brasil, **BIT Magazine 19 de outubro de 2017**. Disponível em: < https://www.bitmag.com.br/2017/10/relatorio-dfndr-lab-aponta-para-um-crescimento-de-44-em-ciberataques-no-brasil/> Acesso em 17 de mai de 2018.

CAPELAS, B. No Brasil, órgãos públicos foram os mais afetados pelo WannaCry, **O Estado de São Paulo, 28 de maio de 2017**. Disponível em: <https://link.estadao.com.br/noticias/cultura-digital,no-brasil-orgaos-publicos-foram-os-mais-afetados-pelo-wannacry,70001816480> Acesso em 16 de out de 2018.

FLORENZANO, C - Brasil é o 6° no ranking de ataques cibernéticos, **CBSI 21 de janeiro de 2018**. Disponível em: <https://www.cbsi.net.br/2018/01/brasil-e-o-6-no-ranking-de-ataques.html> Acesso em 05 de mai de 2018.

FRANZÃO, F - Hackers atacam hospital de câncer no Brasil, **VEJA 27 de junho de 2017.** Disponível em: < https://veja.abril.com.br/brasil/hackers-atacam-hospital-de-cancer-no-brasil/> Acesso em 21 de jul de 2018.

G1 - Veja empresas e órgãos públicos do Brasil que tiraram sites do ar após ciberataque, **Portal de notícias G1 12 de maio de 2017**. Disponível em: < https://g1.globo.com/tecnologia/noticia/veja-empresas-e-orgaos-publicos-que-tiraram-sites-do-ar-apos-ciberataque-mundial.ghtml> Acesso em 21 de jul de 2018.

GUIMARÃES, K. Os crimes dos hackers que interrompem até quimioterapia em sequestros virtuais de hospitais. **BBC Brasil**, 10 ago. 2017. Disponível em: <https://www.bbc.com/portuguese/brasil-40870377>. Acesso em: 17 set. 2018.

MITNICK, K – A arte de invadir, **John Wiley & Sons em 4 de março de 2005**. Disponível em: <Disponível: http://papahacker.blogspot.com/2013/08/a-arte-de-invadir-kevin-mitnick-e-book.html> Acesso 12 de abr de 2018.

PITAS, C. E RUANO, C. - Ataque cibernético global atinge computadores em quase 100 países, **Diaŕio Comércio Indústras e Serviços,** 12 maio de 2017. Disponível em: <https://www.dci.com.br/servicos/ataque-cibernetico-global-atinge-computadores-em-quase-100-paises-1.492806> Acesso em 14 set 2018.

REDAÇÃO - Número de ataques ddos dispara no Brasil, **Telesintese 17 de julho de 2017**. Disponível em: < http://www.telesintese.com.br/ataques-ddos-disparam-brasil/> Acesso em 17 de mai de 2018.

REDAÇÃO - Registros de ataques de negação de serviço cresceram quase 400% no Brasil em 2017, segundo o CERT.br, **Tudo sobre hospedagem de sites 28 de março de 2018**. Disponível em: < https://tudosobrehospedagemdesites.com.br/ataques-negacao-de-servico-cresceram-no-brasil-em-2017/> Acesso em 02 de jun de 2018.

RODRIGUES, R - Brasil é país que mais sofre com ataques de ransomware na AL, **Kaspersky Lab 11 de setembro de 2017**. Disponível em: < https://www.kaspersky.com.br/blog/brasil-e-pais-que-mais-sofre-com-ataques-de-ransomware-na-al/9626/> Acesso em 05 de mai de 2018.