COMPARAÇÃO DE MATURIDADE DA APLICAÇÃO DA SEGURANÇA DA INFORMAÇÃO EM APLICAÇÕES WEB DE INSTITUIÇÕES PÚBLICO-PRIVADAS

MATURITY COMPARISON OF INFORMATION SECURITY APPLICATION IN PUBLIC-PRIVATE INSTITUTIONS WEB APPLICATIONS

Caike Gabriel Burgos[*]
Hérick Pereira Raposo[**]
Thiago Giovanella[***]

RESUMO

Com o grande fluxo de dados trafegando pela rede, tem-se a necessidade da aplicação de medidas protetivas e boas práticas de conduta a respeito do armazenamento, replicação e disponibilização de dados. Este artigo visa realizar análises em aplicações web de instituições públicas e privadas, com a finalidade da comparação de vulnerabilidades encontradas em suas respectivas aplicações, deste modo, mostrar como se encontra a proteção de dados nas instituições público-privadas do Circuito das Águas. Para isso, foi necessário rever e respeitar os parâmetros legais da Lei Geral de Proteção de Dados, a respeito da anonimização da identidade e também de dados sensíveis das instituições analisadas para fins de estudo. Para a realização das análises e levantamento de dados e informações, utilizou-se aplicações específicas que são encontradas no Sistema Operacional Kali Linux, sendo essas ferramentas gratuitas e pré-instaladas no sistema. Depois de realizadas as análises e as devidas informações obtidas, as vulnerabilidades foram relacionas as respectivas aplicações nas quais foram encontradas, deste modo, tem-se por fim que as instituições públicas se mostraram mais vulneráveis quando comparadas as instituições privadas apresentando maior incidência de vulnerabilidades em um maior número de instituições.

Palavras-Chave: Vulnerabilidades. Dados. Proteção. Anonimização. Análises.

ABSTRACT

With the large flow of data traveling across the network, there is a need for protective measures and best practices regarding data storage, replication and availability. That said, this paper aims to perform analyzes on web applications of public and private institutions, with the purpose of comparing vulnerabilities found in their respective applications, thus showing how data protection is found in public-private institutions of the Circuito das Águas. For this, it was necessary to review and respect the legal parameters of the Lei Geral de Proteção de Dados, regarding the anonymization of identity and also sensitive data of the institutions analyzed for study purposes. To perform the analysis and survey of data and information, we used specific applications that are found in the Kali Linux Operating System, and these tools are free and preinstalled on the system. After the

[*] Universidade Vale do Rio Verde. caikegburgos@hotmail.com
[**] Universidade Vale do Rio Verde. herickraposo97@gmail.com
[***] Professor Orientador. Universidade Vale do Rio Verde. prof.thiago.giovanella@unincor.edu.br

analysis and the information obtained, the vulnerabilities were related to the respective applications in which they were found. Thus, it was concluded that public institutions were more vulnerable when compared to private institutions with a higher incidence of vulnerabilities in a larger number of institutions.

Keywords: Vulnerability. Data. Protection. Anonymization. Analysis.

Introdução

Primordialmente, é necessário salientar a diferença entre dado e informação. Um dado constitui-se de um registro sem valor e um contexto analítico, a informação por sua vez, constitui-se da adesão de dados a um contexto de entendimento, ganhando consequentemente valor. Para que haja a proteção das informações é necessário à maturidade na forma do manuseio, tratamento e utilização das mesmas.

Assim, este trabalho visa destacar as disparidades entre a maturidade de aplicações da segurança da informação em aplicações web em instituições público-privadas, tendo como diretriz a importância da informação nos tempos modernos e os riscos que elas correm em um mundo globalizado.

Segundo informações disponibilizadas pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, CERT (2013), ataques como negações de serviços (DDoS), *Brute force* e interceptação de tráfego, são comumente efetuadas em sistemas computacionais devido a vulnerabilidades e pontos fracos em relação a segurança da informação.

Portanto, é de extrema importância que sejam aplicadas medidas protetivas nas aplicações visando promover a eficácia dos pilares da informação (confiabilidade, integridade e disponibilidade), bem como a aplicação de políticas de segurança, tais como a privacidade das informações disponibilizadas na web e restrição de acesso, e por fim apresentar os resultados obtidos com a implementação e desenvolvimento deste trabalho, bem como ilustrar a maior ocorrência de vulnerabilidades em aplicações web de instituições públicas, e compará-las com as encontradas em instituições privadas, deste modo mostrar como se encontra a segurança da informação em ambos os meios de atuação das instituições.

Revisão de literatura

Com a globalização e a evolução tecnológica, a informação tornou-se um dos principais bens socioeconômicos. Com a facilidade de acesso à informação e fácil comunicação, o número

de internautas cresce exponencialmente. Segundo dados divulgados pelo Instituto Brasileiro de Geografia e estatística (IBGE, 2018), o número de brasileiros com 10 anos ou mais que acessam a internet passou de 64,7% para 69,8% no ano de 2016 para 2017. São quase 10 milhões a mais de usuários. Além disso, o Registro.BR (2019), entidade responsável pela gestão de registros de domínios no Brasil, indica que o número de domínios computados até o momento, 2019, são de aproximadamente 3.984.000.

Deste modo, com o aumento de usuários na internet, houve o crescimento paralelo da utilização e influência das aplicações web, necessitando-se da aplicação de medidas de segurança nas mesmas.

Aplicações Web e seu funcionamento

Segundo Ndegwa (2016), com a expansividade da internet e seu número de usuários, empresas a utilizam como um canal de comunicação econômico, permitindo desta maneira a facilitação de transições seguras e aumento na troca e tratamento de informação com o público alvo, armazenando, processando e apresentando tais informações ao usuário. Em aplicações web temos duas vertentes, o usuário, onde o mesmo dispara uma solicitação para o servidor web, pela internet, o qual encaminha a solicitação para o servidor de aplicação web que por sua vez executa a ação correspondente a solicitação do usuário. Posteriormente, o servidor de aplicação web envia os resultados para o servidor web, o qual encaminha os resultados ao cliente e apresenta os dados dispostos formatando-os.

Deste modo, levando-se em consideração que as informações são armazenadas em servidores, havendo o tratamento de dados, quando executado em território nacional, a instituição provedora do serviço deve adequar-se aos parâmetros da lei de proteção de dados LGPD, garantindo os alicerces da segurança da informação (PINHEIRO, 2018).

Segurança da informação

Segundo Coelho, Araújo e Bezerra (2014), o conceito de Segurança da Informação, compreende a proteção de informações e recursos entre outras diretrizes, tais como erros e manipulação de dados.

Assim, Lyra (2017) reforçando a ideia de Stallings (2015) a define como a priorização e proteção dos princípios fundamentais da informação (CIDAL): Confidencialidade, Integridade, Disponibilidade, Autenticidade e Legalidade.

Vulnerabilidade e ataques em aplicações web

Vulnerabilidades são falhas em potencial que ao serem exploradas podem infringir um dos pilares da segurança da informação (confidencialidade, disponibilidade, integridade).

Dentre as vulnerabilidades as mais recorrentes segundo OWASP (2017) são: Injeção, quebra de autenticação, exposição de dados sensíveis, entidades externas de XML (XXE), *Cross-Site Scripting* (XSS), configuração de segurança incorreta, desserialização insegura, utilização de componentes vulneráveis, registro e monitoração insuficientes.

Tamanha preocupação normativa e legal, baseia-se na crescente necessidade de medidas protetivas e controle contra golpes e exploração de vulnerabilidades de sistemas. Mediante este cenário, organizações como a *Open Web Application Security Project* (OWASP) e o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), responsabilizam-se à normatização e padronização de medidas de boas práticas de segurança da informação, catalogando as principais vulnerabilidades encontradas até o presente momento, 2019.

Segundo CERT (2013) são vários os possíveis motivos de uma ação de ataque podendo ser: demonstração de poder, motivos financeiros e/ou ideológica, bem como prestígios ou motivação comercial.

Com seu objetivo definido, os atacantes utilizam técnicas de ataque a aplicações, como por exemplo: Falsificação de e-mails, interceptação de tráfego, Força Bruta, Desconfiguração de página, Negação de serviços dentre outras técnicas de ataque.

Regulamentação

Com tamanha importância, as informações devem ser armazenadas e acessadas de forma minuciosa, sendo assim, é necessária uma padronização, legislação, bem como uma autoridade nacional de fiscalização para que haja garantia dos princípios básicos da Segurança da Informação.

Pensando nisso, foi alterada no ano de 2018 a lei de proteção de dados pessoais de número 13.709 (LGPD). A lei se divide em disposições preliminares da proteção de dados, do art. 1° ao 45°.

Segundo o artigo 6º da LGPD (2018), para que as instituições fiquem em conformidade legal, é necessário que haja a alteração e implementação de sistemas consistentes de controle e aplicação de medidas preventivas de segurança da informação, prevenindo danos provenientes a vazamento de dados, melhorando procedimentos e fluxos internos e externos de dados de forma transparente, com finalidade declarada, com informações com acesso facilitado ao titular (art. 9°; art. 15°). De mesmo modo, salienta-se no artigo 7º que para que ocorra o tratamento de dados, o mesmo deve proceder mediante o consentimento do titular dos dados.

Sendo assim, para meios de normatização a respeito de normas técnicas, as instituições, além de atenderem as exigências da Lei Geral de Proteção de dados, devem estar em conformidade com a Família Normativa ISO/IEC 27000 (2014), sendo ela o padrão internacional para Tecnologia da Informação, Técnicas de Segurança e Sistemas de Gestão de Segurança da Informação (SGSI), fornece um modelo a ser seguido mediante normas técnicas, configurações e operações que envolvem o processo de implementação e dão uma visão geral de todas as áreas da tecnologia. Dentre todas as normas advindas da ISO/IEC 27000, as mais utilizadas e conhecidas são: ISO 27001 e a ISO 27002, as quais envolvem requisitos que visam a implementação dos controles de segurança da informação adequadas as organizações, além de definir códigos e práticas para o controle, políticas, processos, procedimentos e orientação para alcançar os pilares da segurança da informação.

Materiais e métodos

Este artigo trata-se de um estudo de cunho exploratório observacional Quanti-Quali que associa a análise de dados obtidos com a qualidade da segurança da informação nas aplicações web das instituições nas cidades que compõem a região do Circuito das Águas de Minas Gerais, baseando na observação de vulnerabilidades encontradas.

Desta maneira este estudo tem por delineamento o levantamento de informações através de aplicações e verificações de vulnerabilidades de aplicações das instituições público-privadas, comparando o número de instituições expostas a cada tipo de vulnerabilidade. Sendo assim, o desenvolvimento deste trabalho seguiu os parâmetros da

legais exigidos pela Lei Geral de Proteção de Dados a respeito da anonimização de dados, e garantia do sigilo das instituições participantes, dito isto, nenhum dado obtido será utilizado para outros fins fora deste trabalho.

Foram selecionadas um total de 20 instituições para esta pesquisa, sendo 10 de cunho público e outras 10 de cunho privado, sendo elas empresas prestadoras de serviços essenciais, tais como instituições de ensino, prefeituras, hospitais, provedores de internet, todas elas localizadas no Circuito das Águas em Minas Gerais tendo como justificativa o alto índice de dados trafegados e o número de informações pessoais e de terceiros registradas e alocadas nas aplicações.

Foi necessário rever e respeitar os termos legais da LGPD, especificamente os artigos 11° e o artigo 12°, ou seja, o tratamento de dados pessoais poderá acontecer sem o consentimento do titular em caso de anonimização de dados e de identidade perante estudos, deste modo não necessitando de uma TLCE.

Para este estudo, foram utilizados dois notebooks com acesso à internet e o sistema Kali Linux executando em modo Live USB, além da utilização das ferramentas para análise: Dmitry (onde são retornados dados como, informações contratuais, versão do servidor, subdomínios, informações de domínio), Nmap (apresenta informações básicas do servidor, portas abertas e serviços vulneráveis, análise catalogada de vulnerabilidades conforme a *Common Vulnerabilities and Extosures*), Nikto (retorno de vulnerabilidades) e Uniscan (compilado de ferramentas que oferecem todos os retornos possíveis: vulnerabilidades, portas, subdomínios), deste modo facilitando o levantamento das informações necessárias para a realização do estudo.

Além de analisar as aplicações web, foi necessário também relacioná-las as suas respectivas homepages, com a premissa de que um atacante sempre buscará um elo vulnerável no sistema para realizar as suas explorações.

Com o delineamento do estudo e as aplicações web selecionadas, iniciou-se o desenvolvimento através do levantamento de informações básicas a respeito das instituições, obtendo a versão do servidor, tipos de serviços, data de criação e expiração, IP e subdomínios. Para este passo, foram utilizadas as ferramentas Osinte Framework e Dmitry.

Dando sequência no estudo, com as informações básicas a respeito das aplicações web obtidas, inicia-se a verificação de vulnerabilidades, nesta etapa as ferramentas Nikto, Uniscan e Nmap, realizam a análise nas aplicações.

Por fim, com as vulnerabilidades encontras, estas relacionadas a cada tipo de

instituição, foi realizado um relatório de vulnerabilidades, onde foi construído gráficos e tabelas, onde mostra a quais tipos de vulnerabilidades incidem sobre cada instituição.

Resultados

Após realizar os levantamentos de informações nas aplicações web de instituições público-privadas, de forma minuciosa, foram encontradas algumas vulnerabilidades as quais cada instituição está exposta, além de configurações realizadas erroneamente, cabeçalhos com informações incompletas e também portas abertas.

Nas instituições públicas, especificamente, em suas aplicações web e sites correlatos destaca-se que dentre as 10 (dez) instituições selecionadas 6 (seis) delas continham em suas aplicações irregularidades como a não utilização de TLS, cookies vulneráveis bem como servidores desatualizados. De mesmo modo 2 (duas) delas apresentam *backdoors*, configuração PHP irregular e SQL *Injection*. E por fim temos DOS e XST com grau de ocorrência equivalentes além da incidência de execução remota em uma única instituição dentre as selecionadas.

Em relação as *Home Pages* (sites), as vulnerabilidades *Blind* SQL, Configuração irregulares de PHP, servidores desatualizados e XSS são decorrentes no mesmo número de instituições, bem como as vulnerabilidades de *Cooki*e e DOS que possuem valor de incidência equivalentes. E por fim temos a não utilização de TLS decorrentes em 3 (três) das 10 (dez) instituições.

Tabela 1 – Incidência de vulnerabilidades em site e aplicação web de instituições públicas

	Site	Aplicação
Backdoors	0	2
Blind SQL	1	0
Codigo aberto	0	0
Configuração PHP	1	2
COOKIE	2	6
DOS	2	3
Execução remota de comandos	0	1
Servidor desatualizado	1	6
SQL Injection	0	2
TLS	3	6
XSS	1	0
XST	0	3

Fonte: Próprio Autor, 2019

Em relação as instituições privadas, o número de aplicações vulneráveis a configuração PHP incorretas ou desatualizadas, *Cookie*s e servidores desatualizados se mostram equiparadas assim como as instituições com aplicações suscetíveis a ataques DOS, SQL *Injection*, não utilização de TLS e XST.

Tratando-se de *Home Pages* (sites), coincidentemente o grau de incidência de vulnerabilidades como: *Blind* SQL, Código aberto, configurações PHP, DOS, servidores desatualizados, SQL *Injection* e TLS são equivalentes, diferenciando –se do número de instituições com *Cookies* vulneráveis.

Tabela 2 – Incidência de vulnerabilidades em site e aplicação web de instituições privadas

	Site	Aplicação
Backdoors	0	0
Blind SQL	1	0
Codigo aberto	1	0
Configuração PHP	1	2
COOKIE	3	2
DOS	1	1
Execução remota de comandos	0	0
Servidor desatualizado	1	2
SQL Injection	1	1
TLS	1	1
XSS	0	0
XST	0	1

Fonte: Próprio Autor, 2019

Tendo em vista um panorama geral dos resultados das análises de vulnerabilidades web, observa-se que as aplicações de instituições públicas estão mais suscetíveis a maior incidência de vulnerabilidades quando comparadas com as privadas. Como é representado no gráfico a seguir:

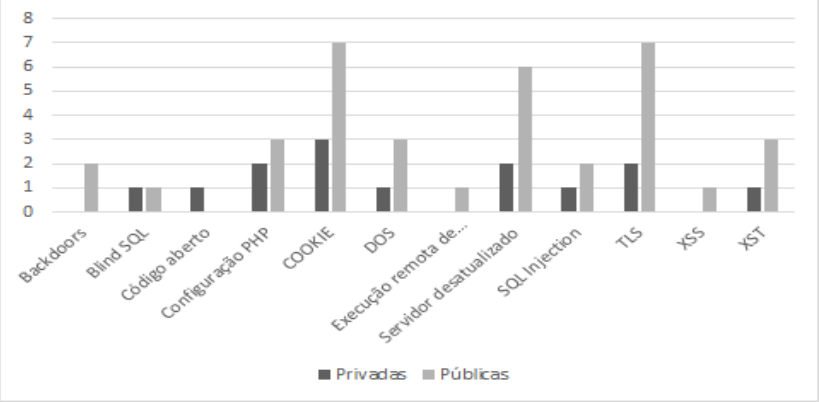

Figura 1 – Comparação da incidência de vulnerabilidades entre instituições públicas e privadas

Fonte: Próprio Autor, 2019.

Considerações finais

Vale destacar que se esperava no início da pesquisa maior incidência de vulnerabilidades em ambos seguimentos devida a alta incidência apresentada em estudos similares, deste modo pode-se concluir que o cenário atual se tratando do número de incidência de vulnerabilidades de instituições públicas-privadas das cidades que compõem o Circuito das Águas no Sul de Minas Gerais é razoavelmente baixo mediante estudos que embasaram o desenvolvimento deste artigo, entretanto, conforme o esperado as instituições públicas se mostram mais vulneráveis quando comparadas com instituições privadas.

Durante as análises observou-se que as instituições públicas que obtiveram menor incidência de vulnerabilidades recebiam serviços terceirizados de instituições privadas em prol da segurança.

É importante destacar o baixo índice de ocorrência das vulnerabilidades XSS e SQL *Injection* sendo estas muito comuns, tendo como origem o conhecimento das instituições em relação as mesmas, precavendo-se. Entretanto destaca-se a grande incidência de servidores desatualizados e a não utilização de TLS, que embora muito conhecidos não foram corretamente aplicados.

É importante destacar que as vulnerabilidades encontradas em servidores desatualizados, configuração incorreta de PHP, DOS influenciam diretamente um dos pilares da segurança da informação, sendo este, a Disponibilidade.

De mesmo modo, as vulnerabilidades Código aberto, XST, XSS, *Blind*-SQL e SQL *Injection* interferem diretamente no princípio de Integridade.

Por sua vez, as vulnerabilidades *COOKIE* vulnerável, *Backdoors*, Execução Remota de Procedimentos, SQL Injection e a não utilização de TLS, ferem o princípio da Confidencialidade.

Curiosamente, algumas medidas de boas práticas como a adesão de HTTP *Header*, *Header* XSS, e cabeçalho anti-click (os quais previnem a intrusão e vulnerabilidades no sistema) não foram empregadas em nenhuma das aplicações.

Por fim, conclui-se que nenhum sistema é totalmente à prova de ataques e vulnerabilidades, cabe as instituições buscarem a maneira mais eficaz para se protegerem e evitar que seus dados sejam expostos na internet, respeitando os parâmetros delimitados pela Lei Geral de Proteção de Dados, resguardando a integridade das informações de seus usuários.

Referências

CERT. **Cartilha de Segurança para Internet**. 4. ed. São Paulo: Creative Commons, 2013. (Comitê Gestor da Internet no Brasil)

COELHO, Flávia Estélia Silva; ARAÚJO, Luiz Geraldo Segadas de; BEZERRA, Edson Kowask. **Gestão da Segurança da Informação:** NBR 27001 e NBR 27002. Rio de Janeiro: Escola Superior de Redes, 2014.

IBGE (Rio de Janeiro). **Número de usuários de internet cresce 10 milhões em um ano no Brasil**. 2018. Disponível em: http://agenciabrasil.ebc.com.br/economia/no ticia/2018-12/numero-de-usuarios-de- internet-cresce-10-milhoes-em-um-ano-no-brasil. Acesso em: 20 fev. 2018.

ISO/IEC (Comp.). **Information technology**. Security techniques - Information security management systems — Overview and vocabulary. 2014. Disponível em: https://standards.iso.org/ittf/PubliclyAvailab leStandards/c063411_ISO_IEC_27000_2014.zip. Acesso em: 10 abr. 2019.

LGPD. Casa Civil Subchefia Para Assuntos Jurídicos (Comp.). Lei nº 13.709, de 14 de agosto de 2018: dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2 015-2018/2018/Lei/L13709.htm. Acesso em: 2 abr. 2019.

LYRA, Maurício Rocha. **Segurança e Auditoria de Sistemas de Informação** 2. ed. Brasília: Editora Moderna, 2017.

NDEGWA, Amos. **What is a Web Application?** 2016. Disponível em: https://www.maxcdn.com/one/visual- glossary/web-application/. Acesso em: 19 mar. 2019.

OWASP - Open Web Application Security Project. **OWASP Top 10.** 4. ed. São Paulo: Creative Commons, 2017. Disponível em: https://www.owasp.org/images/0/06/OWAS P_Top_10-2017-pt_pt.pdf. Acesso em: 3 abr. 2019.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais**: comentários à Lei 13.709/2018 (LGPD). São Paulo: Saraiva, 2018. (Diretoria Executiva: Flavia Alves Bravin).

REGISTRO.BR (Comp.). **Domínios.br registrados até o momento.** 2019. Disponível em: https://registro.br/estatisticas.html. Acesso em: 13 mar. 2019.

STALLINGS, William. **Criptografia e Segurança de Redes:** princípios e práticas. 6. ed. São Paulo: Pearson, 2015.