A Importância de Disseminação de Conhecimentos de Segurança Cibernética

André L. A. Silva, Guilherme P. Aquino, Evandro C. Vilas Boas
Laboratório de Cyber Segurança e Internet das Coisas (CS&I Lab.), Instituto Nacional de Telecomunicações - Inatel
andre.lucas@ges.inatel.br, guilhermeaquino@inatel.br, evandro.cesar@inatel.br

***Abstract*—This work presents the activities developed by the Inatel Cyber Security Center (CxSC Telecom) to provide a cyber security culture for employees of the National Telecommunications Institute (Inatel) and the local community. Among the activities, we highlight the development of audiovisual materials for education and awareness of good practices in data manipulation, concepts related to the General Data Protection Law (GDPL), and the identification of recurring cyber-attacks. It also discusses the activities' importance and effectiveness in collaborating with the institution to adapt to GDPL.**

***Index Terms*—Cyber security, general data protection law, telecommunication networks, telecommunication.**

***Resumo*—Esse trabalho apresenta as atividades desenvolvidas pelo Centro de Segurança Cibernética do Inatel (CxSC Telecom) no âmbito de disseminar conhecimentos de segurança cibernética em colaboradores do Instituto Nacional de Telecomunicações (Inatel) e comunidade local. Dentre as atividades, destaca-se o desenvolvimento de materiais audiovisuais de educação e conscientização sobre boas práticas em manipulação de dados, conceitos relacionados a Lei Geral de Proteção de Dados e identificação de ataques cibernéticos recorrentes. Discute-se também a importância dessa atividades e sua efetividade em colaborar com a instituição no processo de adequação a LGPD.**

***Palavras chave*—LGPD, redes de telecomunicações, segurança cibernética, telecomunicações.**

I. Introdução

O avanço tecnológico e o desenvolvimento das redes e sistemas de telecomunicações possibilitaram maior conectividade entre pessoas. Processos ou atividades rotineiras antes desenvolvidas de forma física, migraram para o mundo digital transformando serviços e negócios. Dessa forma, observa-se um maior fluxo digital de informações sensíveis aos negócios das empresas e dados pessoais relacionados ao trabalho, compras online, cadastros em sites, entre outros [1]. Por conseguinte, intensifica-se a necessidade de assegurar o trânsito e armazenamento seguro dessas informações pelas redes e sistemas de telecomunicações, protegendo-os de acessos indevidos. Nesse contexto, surge o conceito de segurança da informação e segurança cibernética [2, 3].

A segurança cibernética integra um conjunto de políticas, regras e processos que envolvem tecnologias e pessoas com o objetivo de proteger informações contra acesso e uso não intencionais ou não autorizados [3, 4]. Nesse âmbito, protegem-se sistemas, redes e programas de ataques digitais que visam, em sua maioria, acessar, roubar, destruir dados sensíveis ou utilizá-los para extorquir pessoas e empresas. A segurança cibernética deve estar presente em diversas áreas da sociedade em geral para garantir princípios fundamentais aos cidadãos, amparando-se em cinco pilares fundamentais: confiabilidade, integridade, disponibilidade, autenticidade e não repúdio [3, 4]. A confiabilidade dos dados refere-se ao acesso autorizado à um determinado dado ou informação. Esse conceito não deve ser confundido com a privacidade de dados na esfera pessoal. Por exemplo, os colaboradores de uma empresa possuem conhecimento de armazenamento de seus relatórios financeiros, porém, apenas um grupo seleto possui de fato autorização para acessá-los e utilizá-los. A integridade remete-se a garantia de que um ou mais dados permaneçam exatamente como foram gerados, considerando as características iniciais de geração, produção e armazenamento. Dessa forma, garante-se que os dados ou informações não sejam adulterados. A disponibilidade introduz o conceito de garantia de acesso em relação ao tempo e acessibilidade de dados, redes e sistemas, ou seja, a qualquer hora e de qualquer lugar. A autenticidade visa garantir que uma entidade (pessoa, sistema ou dispositivo) seja realmente quem ou que diz ser. Por fim, o conceito de não repúdio relaciona-se ao fato de uma entidade não poder negar sua participação em um evento ou transação relacionada ao acesso, transmissão ou alteração de dados.

A segurança cibernética aplicada ao âmbito pessoal provê segurança no acesso ao meio digital tornando-o confiável. Em ambientes empresariais, tem-se a proteção de todas as informações nos processos da organização, aumentando sua segurança e credibilidade perante os usuários de seus serviços. No Brasil, sancionou-se a Lei Geral de Proteção de Dados (LGPD) com a finalidade de regulamentar e resguardar os direitos de privacidade dos cidadãos [1]. A LGPD entrou em vigor em agosto de 2020, abordando definições e regras sobre o tratamento de dados pelas empresas, com o objetivo de garantir segurança jurídica ao manuseio de informações digitais ou não. A legislação exige a proteção e privacidade dos dados oriundos de pessoas físicas e coletados pelas empresas durante todo o ciclo, incluindo a coleta, uso/manipulação, armazenamento e descarte [5, 6, 7]. Caso ocorra incidentes que venham a expor esses dados, a Lei estabelece diretrizes administrativas às empresas que devem notificar os respectivos titulares. Além disso, prevê-se a fiscalização e punições as transgressões por meio da Autoridade Nacional de Proteção de Dados (ANPD), que é um órgão de estância federal responsável por fazer cumprir a LGPD.

A adaptação das empresas à LGPD deve ser acompanhada por um processo de conscientização e capacitação dos seus colaboradores quanto aos procedimentos implementados. Logo, as empresas devem prover o desenvolvimento de uma cultura de segurança cibernética para que seus colaboradores tenham

Fig. 1. Exemplo de Ransomware [8]

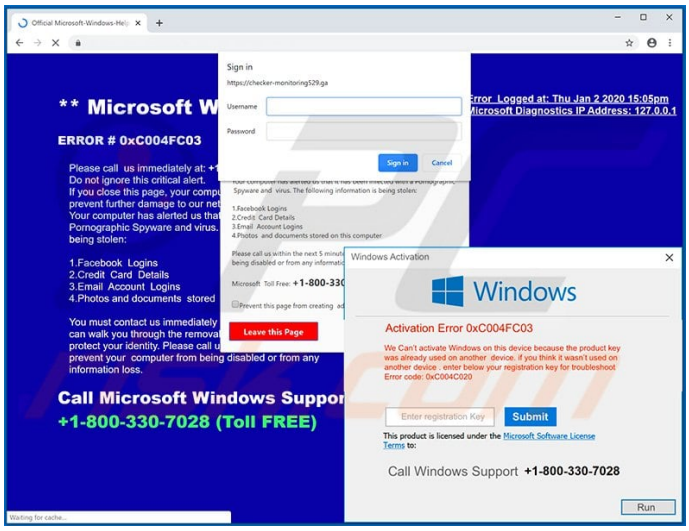

Fig. 2. Exemplo de Trojan [13]

consciência de suas responsabilidades e deveres ao manusear dados sigilosos. Nesse trabalho, abordam-se a importância de disseminação de conhecimentos de segurança cibernética e atividades desenvolvidas pelos autores no intuito de colaborar com a construção dessa cultura para os colaboradores do Instituto Nacional de Telecomunicações (Inatel) e comunidade local por meio de atividades do Centro de Segurança Cibernética do Inatel (CxSC Telecom).

Estrutura-se o trabalho em cinco seções. Na Seção II, discute-se aspectos básicos de segurança cibernética e os ataques comuns que colaboradores de uma empresa podem sofrer durante o desempenho de suas funções. Apresentam-se aspectos relacionados a LGPD na Seção III. Na Seção IV, introduz-se as ações desenvolvidas durante o ano de 2021 como forma de prover um ambiente de disseminação de conhecimento sobre segurança cibernética no Inatel. Por fim, destacam-se os principais comentários e trabalhos futuros na Seção V.

II. Ataques Cibernéticos Recorrentes

Em segurança cibernética, consideram-se os dados e informações como insumos para trabalho, sendo a garantia de sua segurança objetivo principal no que condiz com os pilares fundamentais discutidos anteriormente. Logo, a segurança cibernética corresponde a um conjunto de medidas aplicadas sobre pessoas, tecnologias e processos, para prevenir ataques cibernéticos, que visam explorar vulnerabilidades em uma rede ou sistema de telecomunicações. Dentre os ataques cibernéticos recorrentes, destacam-se o *ransomware*, *trojan* e *phishing* [9, 10, 11, 12].

O *ransomware* é uma variante de ataque cibernético comum e utilizada por atacantes em práticas criminais [10]. O ataque consiste em invadir os sistemas de uma pessoa ou organização, sequestrar os dados por meio de criptografia e solicitar resgate para a vítima. Tipicamente e para evitar qualquer tipo de rastreio financeiro, exige-se o resgate pago em criptomoedas dentro de um prazo estipulado pelo atacante. Expõem-se o indivíduo ao *ransomware* por meio de *links* maliciosos, cujo clicar inicia o *download* do *malware* que invade o sistema e criptografa os dados. Devido às campanhas de conscientização, a exposição a esse tipo de ataque requer personalização durante a abordagem, que utiliza dados ou informações pessoais geralmente compartilhadas de maneira livre pelo titular através de sites e aplicativos móveis. Na Figura 1, demonstra-se um exemplo de ataque de *ransomware*. [9, 10].

O *trojan* refere-se a um ataque para roubo de informações de contas, sejam elas bancárias, de jogos ou de aplicativos móveis [11]. Geralmente esse tipo de *malware* se disfarça como um programa gratuito e atrativo para a vítima ou ainda se apresenta como um anexo de e-mail. Quando o programa é baixado ou o anexo aberto, o *malware* se instala na máquina ou sistema da vítima comprometendo a execução de atividades futuras, que passam a ser gravadas e enviadas para o atacante. Nesse caso, informações sensíveis ou privadas (senhas e transações bancárias) podem ser capturadas e utilizadas para extração de benefícios por parte do atacante. A infecção de um sistema pelo *trojan* envolve o consentimento da vítima, uma vez que a instalação de programas é seguida de um aceite por parte do usuário. Logo, uma forma efetiva de evitar sofrer esse tipo de ataque é realizar a verificação de confiabilidade da fonte do programa que será instalado. Na Figura 2, demonstra-se uma máquina que sofreu o ataque de um *trojan* e teve a chave Windows de ativação capturada e utilizada pelo atacante em outra máquina.

O *phishing* é um ataque popular e que tem como objetivo capturar informações de pessoas que não possuem conhecimentos em segurança cibernética ou baixa instrução em lidar com as soluções tecnológicas atuais [12]. Dessa forma, o atacante explora esses pontos para obter senhas de serviços bancários e informações confidenciais. Geralmente, esse tipo de ataque acontece por meio de e-mails. Uma variante desse ataque explora mensagens de texto via redes móveis para executar ato semelhante, sendo definida como *smishing* [4]. Para prevenção contra esses tipos de ataques, deve-se procurar conhecimento em segurança cibernética para entender como essas práticas ocorrem e poder identificá-las, considerando atualização constante devido à evolução nas abordagens pelos atacantes. Na Figura 3, tem-se uma mensagem típica de *phishing* [14].

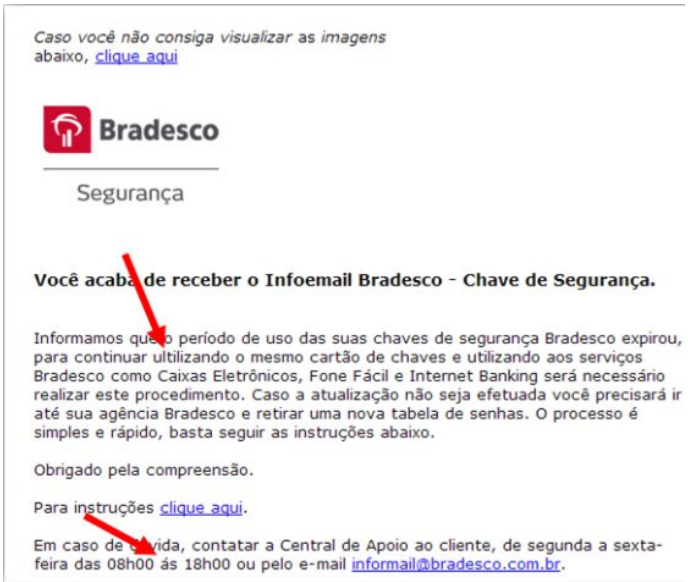

Fig. 3. Exemplo de Phishing [15]

III. Fundamentos da Lei Geral de Proteção de Dados

Nota-se que os ataques cibernéticos exploram diversas formas de execução como a falta de conhecimento de pessoas e vulnerabilidades em sistemas e redes de telecomunicações em seus processos cotidianos. Portanto, a LGPD tem o intuito de minimizar o contingente de ataques cibernéticos e prover a adequação das empresas a proteção de dados em meios físicos e digitais [5, 6]. A LGPD introduz processos detalhados para tratamento correto da informação durante todo seu ciclo dentro de uma organização, definido as responsabilidades da empresa para com os dados que detêm. Assim como, define sanções em caso de descumprimento por meio de multas. Verificam-se diretrizes no âmbito de conscientização da sociedade sobre a importância dos dados pessoais e os direitos fundamentais como a liberdade e a privacidade [7]. A legislação deve ser obedecida tanto a nível de pessoa física como pessoa jurídica.

A LGPD provê ao titular dos dados todos os direitos legais enquanto suas informações estiverem sob posse de uma outra pessoa física ou jurídica. De acordo com o artigo 1º da Lei Geral de Proteção de Dados, sua função é: ”proteger os dados fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade de pessoa natural”. Essa definição introduz dois pontos críticos que norteiam a LGPD: a proteção de direitos e a transparência de informações [5, 6, 7]. A proteção de direitos refere-se aos procedimentos de segurança que devem ser obedecidos no ciclo da informação enquanto sob o poder de uma outra pessoa física ou jurídica, evitando ações ilegais ou antiéticas. A transparência da informação permite que o titular da informação tenha livre acesso ao que está sendo feito com seus dados pessoais por terceiros. Dessa forma, garante-se o direito a privacidade, a liberdade de expressão, de comunicação e de opinião, a intimidade, a honra e a imagem, o acesso à informação, os direitos humanos, liberdade no desenvolvimento da personalidade, as dignidades e o exercício da cidadania e os direitos do consumidor.

No âmbito da legislação, classificam-se os dados em três tipos: dados pessoais, sensíveis e anonimizados [6, 7]. Os dados pessoais referem-se àqueles de uma pessoa física identificada ou identificável. Os dados sensíveis rementem-se as informações de cunho individual como origem étnica, opinião política, orientação religiosa, orientação sexual, dado genético ou biométrico. Já os dados anonimizados compreendem aqueles em que o titular não pode ser identificado. A LGPD visa proteção dentro da legislação a qualquer pessoa física identificada ou inidentificável.

Em relação as sansões, qualquer organização que não se adéque a LGPD ou porventura venha a infligir a legislação será autuada pela ANPD com cobranças de multas sobre faturamento que podem alcançar a cifra limite de 50 milhões de reais. Além da ANPD, a LGPD especifica outra figura importante e relacionada à empresa, o *Data Protection Officer* (DPO) [5]. Esse representante organizacional é responsável por receber comunicações da ANPD, comunicações ou reclamações dos titulares dos dados e definir as providências a serem executadas sobre essas comunicações. Assim como, o DPO deve acompanhar as iniciativas de adequação à LGPD por parte da empresa, como por exemplo o desenvolvimento de uma cultura de segurança cibernética para capacitação dos colaboradores.

IV. A importância de disseminação de conhecimentos em segurança cibernética

A disseminação de conhecimentos em segurança cibernética entre seus colaboradores é um dos meios pelos quais empresas devem explorar para reduzir riscos relacionados a proteção da informação. Uma vez que seus processos envolvem direta ou indiretamente pessoas, uma cultura organizacional com foco em segurança cibernética provê o correto conhecimento para que as boas práticas do ciclo da informação sejam atendidas segunda a legislação tanto para dados digitais ou físicos. Nesse contexto, a conscientização deve abranger todos os colaboradores independentemente das suas funções. Para exemplificar e segundo dados divulgados pela Verizon, 85% das violações de dados compreendem algum tipo de interação humana [16]. Portanto, verifica-se maior probabilidade de ocorrer um ataque cibernético em uma empresa por falha de seus funcionários na execução de processo de tratamento de dados pessoais que aqueles oriundos de ataques digital através de um invasor mal intencionado com propósitos de acessar informações sensíveis.

Diante da importância em disseminar conhecimentos em segurança cibernética nos colaboradores do Inatel, o CxSC Telecom desenvolveu um projeto para produção de vídeos educativos abordando pontos importantes de conscientização sobre segurança cibernética em ambiente corporativo. Esses vídeos serão utilizados para fomentar o conhecimento dos colaboradores do Inatel em processo rotineiros de tratamento da informação digital ou física. Para elaboração dos vídeos, realizaram-se pesquisas e desenvolveram-se relatórios relacionados a área de segurança cibernética envolvendo o cenário internacional, os principais ataques cibernéticos recorrentes e métodos de segurança de dados. Ademais, produziram-se quatro vídeos a respeito da LGPD e cultura de segurança cibernética em ambiente organizacional, com viés educativo e dinâmico.

No âmbito social, o CxSC Telecom desenvolve um projeto de conscientização em alunos de ensino médio e/ou técnico em escolas públicas e particulares de forma a introduzir conceitos de segurança cibernética. Nesse viés, as atividades desenvolvidas nesse projeto compreenderam a confecção de apostilas ilustrativas e educativas para aprendizado dos alunos. Utilizou-se esse material dentro do projeto Telecom Challenge - Desafio Hacker.

V. Conclusão

Nesse trabalho, discutiu-se a importância de disseminação de conhecimentos em segurança cibernética em ambiente organizacional e também para a sociedade em geral. Apresentou-se os principais tipos de ataques cibernéticos que uma pessoa pode ser exposta, assim como discutiu-se a Lei Geral de Proteção de Dados. Dessa forma, elaboraram-se materiais audiovisuais em formato de vídeo e apostilas educativas para conscientização de colaboradores institucionais do Inatel e alunos de ensino médio e/ou técnico de escolas públicas e particulares, respectivamente. Trabalhos futuros incluem a expansão das ações de conscientização em segurança cibernética para redes sociais, assim como prover materiais educativos para outros projetos do CxSC Telecom que se iniciarão nos próximos anos como, por exemplo, os Capítulos de Cyber Segurança em escolas regionais. No âmbito corporativo, indicificam-se ações voltadas para o mapeamento de riscos das áreas e a estruturação de cursos de capacitação direcionados.

Agradecimentos

Os autores agradecem ao Centro de Segurança Cibernética do Inatel (CxSC Telecom) pelo apoio financeiro na execução das atividades propostas, ao Instituto Nacional de Telecomunicações (Inatel) e ao Laboratório de Segurança Cibernética e Internet das Coisas (CS&I Lab.) por todo o suporte técnico oferecido.

Referências

[1] C. Mulholland. *A LGPD e o novo marco normativo no Brasil*. 6ª ed. Arquielago Editorial, 2020.

[2] J. Kurose e K. Ross. *Redes de computadores e a Internet: Uma abordagem top-down*. São Paulo: Person Education do Brasil, 2013.

[3] W. Stallings. *Criptografia e Segurança de Redes*. São Paulo: Person Education do Brasil, 2008.

[4] S. McClure, J. Scambray e G. Kurtz. *Hackers expostos: segredos e soluções para a segurança de redes*. Porto Alegre: Bookman, 2014.

[5] Cláudio Filipe Lima Rapôso, Haniel Melo de Lima, Waldecy Ferreira de Oliveira Junior, Paola Aragão Ferreira Silva e Elaine Elaine de Souza Barros. "Lgpd-lei geral de proteção de dados pessoais em tecnologia da informação: Revisão sistemática". Em: *RACE-Revista de Administração do Cesmac* 4 (2019), pp. 58–67.

[6] Lara Rocha Garcia, Edson Aguilera-Fernandes, Rafael Augusto Moreno Gonçalves e Marcos Ribeiro Pereira-Barretto. *Lei Geral de Proteção de Dados (LGPD): guia de implantação*. Editora Blucher, 2020.

[7] Maria Eugenia Finkelstein e Claudio Finkelstein. "Privacidade e lei geral de proteção de dados pessoais". Em: *Revista de Direito Brasileira* 23.9 (2020), pp. 284–301.

[8] *WannaCry: tudo que você precisa saber sobre o ransomware*. . [Online]. Disponível em:https://www.techtudo.com.br/listas/2017/05/o-que-voce-precisa-saber-sobre-o-ransomware-wannacrypt.ghtml. Acesso: 15.02.2022.

[9] Hamad Al-Mohannadi, Qublai Mirza, Anitta Namanya, Irfan Awan, Andrea Cullen e Jules Disso. "Cyber-attack modeling analysis techniques: An overview". Em: *2016 IEEE 4th international conference on future internet of things and cloud workshops (FiCloudW)*. IEEE. 2016, pp. 69–76.

[10] Nikolai Hampton e Zubair A Baig. "Ransomware: Emergence of the cyber-extortion menace". Em: (2015).

[11] Attlee M Gamundani e Lucas M Nekare. "A review of new trends in cyber attacks: A zoom into distributed database systems". Em: *2018 IST-Africa Week Conference (IST-Africa)*. IEEE. 2018, Page–1.

[12] Muhammet Baykara e Zahit Ziya Gürel. "Detection of phishing attacks". Em: *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*. IEEE. 2018, pp. 1–5.

[13] Tomas Meskauskas. *Como desinstalar Cryxos de um computador?* . [Online]. Disponível em:https://www.pcrisk.pt/guias-de-remocao/9712-cryxos-trojan. Acesso: 15.02.2022.

[14] *10 Ways To Avoid Phishing Scams*. . [Online]. Disponível em:https://www.phishing.org/10-ways-to-avoid-phishing-scams. Acesso: 15.02.2022.

[15] Emerson Alecrim. *O que é phishing? E como evitar golpes do tipo?* . [Online]. Disponível em:https://www.infowester.com/phishing.php. Acesso: 15.02.2022.

[16] *Interação humana foi responsável por 85% das violações de dados*. . [Online]. Disponível em: https://proximonivel.embratel.com.br/interacao-humana-foi-responsavel-por-85-das-violacoes-de-dados/. Acesso: 13.04.2022.