CLEISEANO EMANUEL DA SILVA PANIAGUA
(ORGANIZADOR)

Collection:

APPLIED ENVIRONMENTAL AND SANITARY ENGINEERING 2

Atena Editora
Ano 2022

CLEISEANO EMANUEL DA SILVA PANIAGUA
(ORGANIZADOR)

Collection:

APPLIED ENVIRONMENTAL AND SANITARY ENGINEERING 2

Atena Editora
Ano 2022

Editora chefe
Profª Drª Antonella Carvalho de Oliveira
Editora executiva
Natalia Oliveira
Assistente editorial
Flávia Roberta Barão
Bibliotecária
Janaina Ramos
Projeto gráfico
Bruno Oliveira
Camila Alves de Cremo
Daphynny Pamplona
Luiza Alves Batista
Natália Sandrini de Azevedo
Imagens da capa
iStock
Edição de arte
Luiza Alves Batista

Atena Editora
Ano 2022

Atena
Editora
Ano 2022

Collection: applied environmental and sanitary engineering 2

Diagramação: Camila Alves de Cremo
Correção: Mariane Aparecida Freitas
Indexação: Amanda Kelly da Costa Veiga
Revisão: Os autores
Organizador: Cleiseano Emanuel da Silva Paniagua

Dados Internacionais de Catalogação na Publicação (CIP)

C697 Collection: applied environmental and sanitary engineering 2 / Organizador Cleiseano Emanuel da Silva Paniagua. – Ponta Grossa - PR: Atena, 2022.

Formato: PDF
Requisitos de sistema: Adobe Acrobat Reader
Modo de acesso: World Wide Web
Inclui bibliografia
ISBN 978-65-5983-988-9
DOI: https://doi.org/10.22533/at.ed.889220305

1. Environmental and sanitary engineering. I. Paniagua, Cleiseano Emanuel da Silva (Organizador). II. Título.
CDD 628

Elaborado por Bibliotecária Janaina Ramos – CRB-8/9166

Atena Editora
Ponta Grossa – Paraná – Brasil
Telefone: +55 (42) 3323-5493
www.atenaeditora.com.br
contato@atenaeditora.com.br

Atena Editora
Ano 2022

DECLARAÇÃO DOS AUTORES

Os autores desta obra: 1. Atestam não possuir qualquer interesse comercial que constitua um conflito de interesses em relação ao artigo científico publicado; 2. Declaram que participaram ativamente da construção dos respectivos manuscritos, preferencialmente na: a) Concepção do estudo, e/ou aquisição de dados, e/ou análise e interpretação de dados; b) Elaboração do artigo ou revisão com vistas a tornar o material intelectualmente relevante; c) Aprovação final do manuscrito para submissão.; 3. Certificam que os artigos científicos publicados estão completamente isentos de dados e/ou resultados fraudulentos; 4. Confirmam a citação e a referência correta de todos os dados e de interpretações de dados de outras pesquisas; 5. Reconhecem terem informado todas as fontes de financiamento recebidas para a consecução da pesquisa; 6. Autorizam a edição da obra, que incluem os registros de ficha catalográfica, ISBN, DOI e demais indexadores, projeto visual e criação de capa, diagramação de miolo, assim como lançamento e divulgação da mesma conforme critérios da Atena Editora.

DECLARAÇÃO DA EDITORA

A Atena Editora declara, para os devidos fins de direito, que: 1. A presente publicação constitui apenas transferência temporária dos direitos autorais, direito sobre a publicação, inclusive não constitui responsabilidade solidária na criação dos manuscritos publicados, nos termos previstos na Lei sobre direitos autorais (Lei 9610/98), no art. 184 do Código Penal e no art. 927 do Código Civil; 2. Autoriza e incentiva os autores a assinarem contratos com repositórios institucionais, com fins exclusivos de divulgação da obra, desde que com o devido reconhecimento de autoria e edição e sem qualquer finalidade comercial; 3. Todos os e-book são *open access, desta forma* não os comercializa em seu site, sites parceiros, plataformas de *e-commerce,* ou qualquer outro meio virtual ou físico, portanto, está isenta de repasses de direitos autorais aos autores; 4. Todos os membros do conselho editorial são doutores e vinculados a instituições de ensino superior públicas, conforme recomendação da CAPES para obtenção do Qualis livro; 5. Não cede, comercializa ou autoriza a utilização dos nomes e e-mails dos autores, bem como nenhum outro dado dos mesmos, para qualquer finalidade que não o escopo da divulgação desta obra.

Atena
Editora
Ano 2022

PRESENTATION

The e-book: “Collection: Applied Environmental and Sanitary Engineering 2” consists of fifteen chapters that present works that aimed to contribute both to improving the quality and health of the environment and man, as well as to the development of technologies to reduce costs and improve the quality of basic sanitation, remedying and reducing the environmental impacts resulting from human activities.

Waste management in Brazil is “invisible” in the eyes of government plans at the municipal level, which is why precarious sanitation conditions prevail in most municipalities. In view of this, the scientific community has been reiterating through numerous studies, the need to implement systems for the collection and final disposal of waste in an environmentally more correct way.

The basic sanitation system in Brazil has been restructuring itself due to security and information technology that helps to monitor and automate water and sewage treatment systems, the final disposal of waste, the loss of water resources due to failures or ruptures of pipe among others. Added to this, the numerous software that are developed to improve operating systems that can present information in real time and operation in continuous flow, helping operators.

Finally, the study and development of new treatment technologies from agro-industry residues or from new technologies that aim to implement and improve the efficiency of existing conventional processes,

In this perspective, Atena Editora has been working with the aim of stimulating and encouraging researchers from Brazil and other countries to publish their work with a guarantee of quality and excellence in the form of books and book chapters that are available on the Editora’s website and elsewhere. digital platforms with free access.

Cleiseano Emanuel da Silva Paniagua

SUMÁRIO

CAPÍTULO 9

A IMPORTÂNCIA DE INVESTIMENTOS EM SEGURANÇA DA INFORMAÇÃO PARA AS OPERADORAS DE SERVIÇO DE SANEAMENTO: UM OLHAR SOB OS INCIDENTES DIVULGADOS

Data de aceite: 01/04/2022
Data de submissão: 23/02/2022

André Gambier Campos
Bacharel em Ciências Sociais pela Universidade de São Paulo (USP) e em Direito pela Pontifícia Universidade Católica de São Paulo (PUCSP), Mestre e Doutor em Sociologia pela USP. Técnico de Planejamento e Pesquisa do Instituto de Pesquisa Econômica Aplicada (IPEA). Docente da Escola de Direito e Ciências Sociais da Universidade Positivo (EDCS/UP), pesquisador do Centro de Pesquisa Jurídica e Social (CPJus/UP), com foco na área de direito do trabalho
Brasília - DF
http://lattes.cnpq.br/4974657023940666

Carlos Henrique Jorge
Graduação em Análise e Desenvolvimento de Software pela Pontifícia Universidade Católica do Paraná (PUCPR). Especialista em Redes e Segurança de Sistemas pela PUCPR. Mestrando em Computação Aplicada pela Universidade Tecnológica Federal do Paraná (UTFPR)
Curitiba - Paraná
http://lattes.cnpq.br/1168590081404267

Dalton Issao Ito
Bacharel em Ciência da Computação pela Universidade Federal do Paraná (UFPR). Bacharel em Direito pelo Centro Universitário OPET. Especialista em Direito Digital pelo IBMEC, em Planejamento e Gestão de Negócios pela UNIFAE e em Direito de Família e Sucessões pela Universidade Anhanguera. Master Business Administration para *Data Protection Officer* pela IESB. Mestrando em Direito, Tecnologia e Desenvolvimento pela Universidade Positivo (UP)
Curitiba - Paraná
http://lattes.cnpq.br/4421914353219521

Mariana Espindola de Souza
Mestre em Meio Ambiente Urbano e Industrial pela UFPR e Engenheira Ambiental da Sanepar
Curitiba - Paraná
http://lattes.cnpq.br/0567162521455940

RESUMO: O objetivo deste trabalho é estudar os riscos da automação em plantas indústriais de saneamento e os riscos nos processos dessas empresas em um cenário de internet das coisas. Com o avanço da tecnologia e a convergência entre a Tecnologia da Informação (TI) e a Tecnologia Operacional (TO) plantas industriais, principalmente as relacionadas às infraestruturas críticas ganharam maior atenção, uma vez que permitem a automatização e um potencial aprimoramento de processos; a melhoria da gestão e da qualidade de serviços prestados em razão da geração de dados, sobre os quais é possível extrair decisões estratégicas. O avanço dos meios de comunicação tem permitido a quebra de paradigmas relativos à distância física entre as plantas industriais e os operadores, possibilitando muito mais do que a geração e o envio de dados, mas o controle remoto de estruturas complexas de operação, gerando forte preocupação com a segurança cibernética.

Com o acesso e a capacidade de controle de recursos industriais de forma remota exige planejamento e implementação de recursos de segurança adequados, principalmente em se tratando de infraestruturas críticas, com potencial de gerar danos de grandes proporções à sociedade, como o serviço de saneamento, com potencial de causar graves danos ao meio ambiente e à saúde da população. O investimento por empresas de saneamento e a regulamentação de melhores práticas por órgãos estatais competentes, passam a ganhar protagonismo neste ambiente.
PALAVRAS-CHAVE: Tratamento de Água e Esgoto, Crimes Cibernéticos, Riscos Cibernéticos, Internet das Coisas (IoT), Infraestruturas Críticas.

THE IMPORTANCE OF INVESTMENTS ON INFORMATION SECURITY FOR SANITATION SERVICE OPERATORS: AN ANALYSIS OF REPORTED INCIDENTS

ABSTRACT: The goal of this paper is to study the risks on the automation of the sanitation industries plants and the risks on the processes at these companies in a scenario of internet of the things. With the improve of technology and the convergence between Information Technology (IT) and Operational Technology (OT), industrial plants, especially those related to critical infrastructures, have gained greater attention, since they allow automation and a potential improvement of processes; the improvement of the management and quality of services provided due to the generation of data, on which it is possible to extract strategic decisions. The advancement of the means of communication has allowed the challenge of paradigms related to the physical distance between industrial plants and operators, allowing much more than the generation and sending of data, but the remote control of complex structures of operation, generating strong concern with cybersecurity. With access and the ability to control industrial resources remotely, it requires planning and implementation of adequate security resources, especially in the case of critical infrastructure, with the potential to generate large-scale damage to society, such as the sanitation service, with potential to cause serious damage to the environment and the health of the population. Investment by sanitation companies and the regulation of good practices by competent state regulation, start to gain prominence in this environment.
KEYWORDS: Water and Sewage Treatment, Cyber Crime, Cyber Risk, Internet of Things (IoT), Critical Infrastructure.

1 | INTRODUÇÃO

A água é essencial para o desenvolvimento do homem da agricultura e de toda cadeia produtiva e econômica, isto é, para o meio ambiente. De acordo com Omotayo e Telukdarie (2019), o consumo de água deve crescer duas vezes mais que o crescimento da população, e em 2025 estima-se que 2/3 da população global irá viver em áreas que exista escassez de água seja pelo alto consumo, seja pela quantidade de população e disponibilidade hídrica da região ou pelas mudanças climáticas.

Para conseguir acompanhar a demanda, as empresas buscam por melhor eficiência nos processos de tratamento juntamente com novas ferramentas e tecnologias, isto é, a

aplicação de tecnologias, que embarcam a indústria 4.0, internet das coisas e similares, aplicada ao saneamento, desta forma estas empresas tornam-se vulneráveis aos processos e riscos que utilizam.

Conforme Vitry et al. (2019), a digitalização pode criar novas vulnerabilidades se sensores, comunicadores e componentes de controle que formam a inteligência não forem implementados de forma adequada.

A digitalização dos processos diários tem sido cada vez maior nos últimos anos, empresas já nascem totalmente digitais, e em um mundo cada vez mais conectado, onde segundo estimativas, em 2020 existiam cerca de 50 bilhões de dispositivos conectados à internet (DAVIS, 2018), as empresas de infraestrutura crítica também se modernizaram, digitalizando e integrando a internet muitos processos que em um passado recente tinha uma execução apenas manual, analógica e isolada.

Neste contexto, a segurança cibernética vem ganhando relevância devido a este crescimento digital e também a incidentes de segurança sendo divulgados na grande mídia. Muitos destes incidentes têm como origem externa à organização impactada, que podem ser dissimulados ou assumidos e podem trazer impactos físicos ou não, que variam desde desfiguração de websites, perdas financeiras, parada de um serviço ou ainda a indisponibilização de uma infraestrutura crítica para o país (TAQUARY, 2019).

O objetivo deste artigo é expor a realidade dos eventos de segurança cibernética e segurança da informação aplicada a operadores de saneamento, que estão ocorrendo em outros países, e as ações recomendadas por entidades especializadas, tendo por objetivo a maior atenção e investimentos a fim de mitigar a possibilidade de ocorrência de eventos dessa natureza.

2 | MATERIAIS E MÉTODOS

A fim de cumprir os objetivos e justificativas propostas, foi realizado estudo de caso exploratório dos incidentes cibernéticos ocorridos em operadoras de saneamento, com uma pesquisa de abordagem mista e não experimental.

A partir da leitura e análise documental foram analisados os elementos essenciais para a elaboração de procedimentos internos, de modo a orientar e recomendar ao usuário as melhores práticas adotadas.

3 | A INDÚSTRIA BASEADA EM TECNOLOGIA DA INFORMAÇÃO

A evolução da indústria permitiu o desenvolvimento da sociedade, suprindo grande parte de suas necessidades garantindo produção de escala, redução de custos tornando produtos acessíveis a grande parte da população dentro de um nível adequado de qualidade. Tudo isso se deve em grande parte ao desenvolvimento da tecnologia e a sua

adequação aos processos.

Em um primeiro momento, o desenvolvimento da tecnologia foi baseada em equipamentos e maquinários, fundamentais para o desenvolvimento da própria humanidade como conhecemos hoje. Atualmente, vivenciamos uma etapa que passa quase despercebida por aqueles que não estão envolvidos diretamente com a tecnologia, a era da informação. Com o ganho de escala na cadeia de produção, cresceram os números de variáveis e informações com que os gestores passaram a lidar para tomadas de decisões estratégicas que garantam não apenas a continuidade no ganho de escala mas principalmente para a manutenção do funcionamento e do controle da cadeia de produção.

O desenvolvimento da sociedade em termos da tecnologia da informação, como é facilmente perceptível nos dias atuais, é decorrente do próprio desenvolvimento da tecnologia digital que presencia o surgimento, o desenvolvimento e a popularização de soluções capazes de coletar e processar informações que permeiam por todas as etapas de produção independente do setor em que esteja inserido, o que inclui o de saneamento.

As vantagens decorrentes da tecnologia da informação, por outro lado, podem ter criado outros problemas. As atuais tecnologias de água e inovações como *Big Data*, *IoT*, *Cloud Computer* e a automação do processo industrial criam grandes quantidades de dados, expondo a indústria aos crescentes riscos de segurança cibernética (SKIBA, 2020).

Além de uma infraestrutura corporativa com a arquitetura da Tecnologia da Informação (TI) tradicional e com foco nos dados e informações, as fornecedoras de água e esgoto contam com a tecnologia de automação (TA), que são compostos por sistemas físico-cibernéticos na produção de seus produtos finais, seja diretamente no tratamento de água e esgoto, ou então no monitoramento da distribuição e em alguns casos na medição do consumo.

O custo de infraestrutura, operação e manutenção de um sistema de fornecimento de água e esgoto é grande, na faixa de centenas de bilhões de dólares anualmente pelo mundo e com expectativa de continuar crescendo. A digitalização poderia não apenas aumentar a flexibilidade e eficiência do sistema, mas também permitir o fornecimento de novos serviços à sociedade (VITRY et al., 2019).

Por muitos anos os sistemas SCADA (*Supervisory Control And Data Acquisition*) e a TA em geral foram isolados de redes corporativas e da internet, porém com o avanço da tecnologia, muitas organizações planejaram convergir as redes de TI e TA. Esta convergência tem por objetivo a redução de custos de manutenção, coleta e análise de dados integrada (HASSANZADEH et al., 2020). Nos últimos anos, a IoT direcionou o crescimento de sistemas físico-cibernéticos, liderando a convergência entre TI e TA. Este casamento melhora a performance, inovação e redução de custos, porém aumenta o número de vulnerabilidades e a superfície de ataques cibernéticos por atores maliciosos (COLELLI et al., 2019).

Quando novas tecnologias como Internet of Things (IoT) são integradas nas

infraestruturas críticas nacionais, novas ameaças cibernéticas surgem e que requerem soluções específicas de segurança (ANI et al., 2019). Os sistemas SCADA estão começando a ser conectados à internet, assim, sendo expostos às ameaças de segurança que podem parar sua operação normal. Há um crescente número de incidentes cibernéticos em diversas infraestruturas críticas, como consequência, pesquisadores estão focando em aumentar a segurança e a confiança operacional destes sistemas (PLIATSIOS et al., 2020). Uma vulnerabilidade em um sistema de controle industrial pode ter efeitos catastróficos se descoberto e subsequentemente explorado por um atacante, particularmente se este dispositivo é utilizado por uma infraestrutura crítica (THOMAS et al., 2020).

Diferente de outros setores que fazem parte da infraestrutura crítica de um país, as empresas de saneamento não possuem padrões e regulamentações para a utilização de tecnologia da informação e segurança cibernética no seu ambiente produtivo, além de ter um orçamento muito menor do que o setor elétrico, petroquímico ou bancário, e tem um impacto similar em caso de um incidente de segurança cibernético pela má utilização da tecnologia.

Conforme Vitry et al. (2019), os incidentes em empresas de saneamento podem não apenas levar a um roubo de dados dos clientes ou solicitações de resgates de dados, mas também podem afetar processos físicos no tratamento de água ou coleta de esgoto controlados remotamente. De acordo com Robles et al. (2015), há uma falta de integração entre as atuais soluções para o gerenciamento de plantas de fornecimento de água, os fornecedores de soluções utilizam diferentes padrões, métodos, modelos de dados e de comunicação para as suas soluções, o que aumenta muito a complexidade e o risco para o negócio.

A preocupação com a segurança da informação é uma constante e apresentada como um risco de ameaça crítica para o mundo, elencada no Relatório Riscos Globais publicado anualmente pelo Fórum Econômico Mundial (WEF, 2021). Neste, a segurança cibernética é citada como um problema corrente, de curto prazo (0-2 anos), enquanto que a infraestrutura de Tecnologia da Informação é um risco, com previsão de se tornar uma ameaça crítica para o mundo, de médio prazo (3-5 anos).

A previsão de riscos evidencia que ações que já deveriam ter sido tomadas por todas as empresas que utilizem tecnologia com utilização massiva de informações, assim como deve ser adotado como um padrão de preocupação a ser adotado em todos os projetos, tendo em vista a segurança cibernética e a infraestrutura de Tecnologia da Informação.

Nos últimos anos foi possível perceber alguns passos modestos pelo próprio Governo, no sentido de propor iniciativas que visam fomentar a segurança cibernética em sistemas críticos surgem no Brasil, como o Decreto nº 10.222, que aprova a Estratégia Nacional de Segurança Cibernética (BRASIL, 2020) da qual podemos citar o seguinte trecho: "*A proteção às infraestruturas críticas, por sua relevância, merece abordagem específica. No Brasil, essas organizações a serem protegidas, escopo desta Estratégia,*

são as pertencentes ao setor de Telecomunicações, ao setor de Transportes, ao setor de Energia, ao setor de Água e ao setor Financeiro."

Em 2018 os EUA criaram o *Cybersecurity and Infrastructure Security Agency* (CISA), com um orçamento anual de 3,1 bilhões de dólares (*US Department of Homeland Security*, 2020), a agência faz parte do departamento de segurança interna dos Estados Unidos e tem como foco alertar as infraestruturas críticas americanas sobre os riscos cibernéticos e melhores práticas, trabalhando com os setores público e privado (CISA, 2021).

Ainda nesse sentido, a União Europeia emitiu a Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (UE, 2016), regulando questões relativas à segurança da informação e a segurança cibernética, indicando os Operadores de Serviços Essenciais, dentro dos quais foi incluído o fornecimento e distribuição de água potável.

Percebe-se uma clara demonstração de preocupação de governos com certas áreas de infraestrutura estratégicas, das quais merece atenção o setor de águas, de cuja relevância tem sido cada vez mais percebida pelas alterações ambientais, gerando repercussões econômicas na indústria e agricultura, mas principalmente na vida das pessoas, uma vez que se trata de um recurso que, quando escasso compromete a própria sobrevivência da humanidade.

4 | INFRAESTRUTURA CRÍTICA E OS ATAQUES SEM FRONTEIRAS

Com o avanço da tecnologia, cada vez menos a ação física e a distância deixaram de ser fatores relevantes para atingir sistemas estratégicos de um Estado e a sua população, capazes de causar grande impacto. Frances Robles e Nicole Perlroth descreveram uma série histórica de eventos que corroboram com tal constatação.

> Ataques à infraestrutura crítica datam de pelo menos 2007, quando os Estados Unidos e Israel realizaram um ataque conjunto à instalação nuclear iraniana de Natanz que destruiu cerca de 1.000 centrífugas de urânio. Nos anos que se seguiram a esse ataque, conhecido como Stuxnet, a infraestrutura crítica se tornou um alvo mais frequente para hackers.
>
> No início de 2012, os hackers russos começaram a realizar sondagens em empresas americanas de energia e concessionárias de eletricidade. Três anos depois, em 2015, eles usaram um acesso semelhante, em empresas de serviços públicos da Ucrânia para desligar a energia por várias horas na Ucrânia Ocidental e novamente um ano depois na capital da Ucrânia, Kiev.
>
> Em 2017, os hackers russos chegaram a acessar uma usina americana ao nível de manipular alguns controles, cessando suas ações um passo antes da sabotagem. No mesmo ano, hackers na Rússia foram pegos desmontando as travas de segurança em uma instalação petroquímica saudita, que são responsáveis por evitar incidentes catastróficos de grandes proporções como explosões.

> Nos últimos anos, os Estados Unidos realizaram seus próprios ataques cibernéticos contra a Rússia, com uma série de ações à rede elétrica desse país, o que os especialistas em segurança cibernética compararam ao equivalente digital da destruição mutuamente assegurada.
>
> Outros países também vem testando os sistemas americanos. Em 2013, hackers iranianos foram pegos invadindo uma pequena barragem em Nova York. Inicialmente, o temor das autoridades era o de que os hackers estivessem atacando uma barragem muito maior, a de Arthur R. Bowman, no Oregon, onde um ataque cibernético que viesse a comprometer as suas eclusas poderia causar uma calamidade. Todavia, os investigadores descobriram que os hackers estavam dentro da barragem muito menor, da Bowman Avenue, a 30 milhas ao norte de Manhattan.
>
> São os ataques a esses sistemas municipais menores, como a barragem da Bowman Avenue e a estação de tratamento de água em Oldsmar, que os especialistas em segurança cibernética dizem que mais temem. Embora as grandes empresas de serviços públicos geralmente tenham proteções complexas, as empresas menores de abastecimento de água, os fornecedores de energia elétrica e os fabricantes geralmente não têm.
>
> (ROBLES e PERLROTH, 2021, tradução livre).

Em razão dos diversos ataques cibernéticos de alto perfil, em que empresas americanas vem sofrendo, em julho de 2021, o presidente dos Estados Unidos, Joseph Biden, assinou um memorando de segurança nacional na quarta-feira, lançando uma nova iniciativa público-privada que cria “controles de desempenho” para a segurança cibernética nas empresas mais críticas da América, incluindo tratamento de água e usinas de energia elétrica. (BING, BOSE, 2021).

Ao mesmo tempo em que a tecnologia garante maior facilidade de acesso, facilitando o desenvolvimento de atividades e operações em infraestruturas críticas, as seguranças da informação e cibernética deverão ser o custo a ser cobrado. Como visto, tal facilidade é uma via de mão dupla que viabiliza também àqueles que buscam o crime dentro de um meio em que, cada vez mais, a distância física deixa de ser um fator impeditivo.

Assim como plantas americanas podem ser alvos de *hackers*, pessoas mal intencionadas ou até mesmo adolescentes com acesso à recursos tecnológicos, com o avanço dos meios de comunicação, o alvo da ação criminosa assim como o próprio criminoso, podem estar localizados em qualquer posição do globo, inclusive no Brasil.

5 I INCIDENTES DE CIBERSEGURANÇA NO SETOR DE SANEAMENTO

Como bastante debatido, uma série de ataques cibernéticos no setor de infraestrutura crítica tem sido observado mundo afora, gerando enormes prejuízos de diversas naturezas não apenas para as empresas, mas também para a sociedade em geral.

As empresas naturalmente serão afetadas não apenas financeiramente, mas a depender das dimensões do ataque, com profundos abalos à imagem e à sua reputação.

Ao mesmo tempo, a população sofrerá com a indisponibilidade do serviço que, a depender do setor, como a de energia e de saneamento, poderá sofrer prejuízos e transtornos irreversíveis.

A seguir serão elencados uma série histórica de eventos que afetaram diretamente o setor de saneamento, com danos ocorridos em maior ou menor proporção, mas que expõem vulnerabilidades à infraestrutura em cenários cujo impacto poderia ser muito maior se os criminosos assim desejassem.

5.1 Maroochy Water Services, Australia, 2000

Maroochy Shire foi o primeiro incidente cibernético registrado em uma instalação de infraestrutura crítica. Essa intrusão causou o despejo de 800 mil litros de esgoto em rios, parques e um hotel da região (HASSANZADEH, 2020).

O crime ocorreu entre 9 de fevereiro de 2000 e 23 de abril de 2000, quando um ex-prestador de serviços, que participou do projeto de implantação do sistema supervisório SCADA (*Supervisory Control And Data Acquisition*), acessou computadores que controlam o sistema de esgoto de *Maroochy Shire Council*, alterando parâmetros de sistema em particular das estações de bombeamento de esgoto causando mau funcionamento em suas operações como:

- As bombas passaram a apresentar problemas de funcionamento;
- Os alarmes não reportavam ao computador central; e
- Houve a perda de comunicação entre o computador central e as estações de bombeamento.

As consequências desse evento resultaram no comprometimento da vida aquática local, uma vez que a água se tornou totalmente poluída e o cheiro insuportável. (ABRAMS, WEISS, 2021).

5.2 Pennsylvania Water Filtering Plant, EUA, 2006

O FBI descobriu que através de um notebook infectado de um empregado, foi instalado um software malicioso em computadores de uma planta industrial. As investigações concluíram que a planta não era o alvo principal, os hackers estariam usando estes computadores para enviar e-mails para outros alvos, porém este ataque poderia alterar os níveis de produtos químicos da planta (HASSANZADEH, 2020).

Se a violação tivesse como alvo a estação de tratamento de água, as consequências poderiam ter sido muito graves, de acordo com Mike Snyder, coordenador de segurança da seção da Pensilvânia da *American Water Works Association*. Segundo o qual os criminosos poderiam ter agido com o objetivo de aumentar o nível de cloro injetado na água, tornando a água perigosa para o consumo humano. (MCMILLAN, 2006).

5.3 Springfield, Illinois, EUA, 2011

Uma bomba em um serviço público de água em Springfield, Illinois, foi recentemente destruída depois que ciberataques obtiveram acesso a um sistema SCADA que controla o referido dispositivo. A bomba queimou depois que o sistema SCADA que a controlava começou a desligar e ligar intermitentemente.

Acredita-se que os invasores tenham obtido os nomes de usuário e as senhas do sistema invadindo primeiro um computador pertencente ao fornecedor do software SCADA que controlava a planta. Os fornecedores de SCADA costumam manter uma lista de nomes de usuários e senhas para acessar os sistemas implantados dos clientes para fins de suporte. (VIJAYAN, 2011).

A notícia do ataque chegou poucas semanas após a descoberta do Trojan Duqu, projetado especificamente para roubar informações de fornecedores de sistemas SCADA. Os fornecedores de segurança acreditam que o malware estava sendo usado para coletar informações para que os hackers pudessem criar outro worm parecido com o Stuxnet, como o usado para interromper as operações na instalação nuclear iraniana de Natanz em anos anteriores a este evento. Quando o Duqu foi descoberto, alguns especialistas em segurança do sistema de controle temeram que ele pudesse ser usado para roubar credenciais de login de clientes de fornecedores de SCADA (VIJAYAN, 2011).

Softwares que controlam recursos industriais e de utilidades, como energia elétrica, água e usinas de energia, são chamados de “SCADA” ou (Supervisory Control And Data Acquisition ou “Sistemas de Supervisão e Aquisição de Dados”). Tais sistemas são vulneráveis porque raramente recebem atualizações, por controlarem sistemas críticos, empresas evitam interferir com o seu funcionamento (ROHR, 2011).

5.4 Key Largo Wastewater Treatment District, EUA, 2012

Em 2012, o ex-diretor financeiro da companhia, Sal Zappulla, acessou ilegalmente os computadores da Key Largo Wastewater Treatment District e baixou e-mails e outras informações utilizando a credencial de outro funcionário. Ele foi processado e acusado por acesso ilegal de computador e tentativa de fraudar, modificar e excluir informações da companhia (HASSANZADEH, 2020).

Zappulla se gabou de ter conseguido provar que os computadores do distrito de tratamento de águas residuais não eram seguros (JONES, 2021).

5.5 An European Water Utility, 2018

Em janeiro de 2018, a empresa Radiflow detectou um tráfego suspeito na rede SCADA de uma companhia de água da Europa. Uma série de conexões para endereços de internet foram detectadas, porém os analistas verificaram que não eram sites maliciosos. Uma investigação posterior revelou que os endereços pertenciam a um grupo de mineração

de criptomoedas. Após esta investigação, foi detectado que havia um malware na rede TO da companhia, a qual consumia 40% do tráfego total de dados da rede para a mineração de criptomoedas. Não foi encontrada nenhuma tentativa de manipulação das configurações do CLP (HASSANZADEH, 2020).

5.6 Israeli National Cyber-Directorate, Israel, 2020

O governo de Israel informou que companhias de água foram alvos de ataques cibernéticos e solicitou que as companhias trocassem imediatamente todas as senhas de seus sistemas, caso não fosse possível a alteração da senha, os sistemas deveriam ser desativados.

Foi o caso de um "ataque sincronizado e organizado" à infraestrutura civil tendo como objetivo interromper os computadores industriais que sustentam as instalações de água israelenses. (LYNGASS, 2020).

Se o ataque tivesse sido bem-sucedido, ele poderia ter causado danos significativos ao abastecimento de água aos civis. Ele também sugeriu que o hacker tinha como alvo o fluxo de cloro nas unidades de tratamento de água, o que poderia ser prejudicial à saúde pública (MARQUARDT, LEVENSON e TAL, 2021).

5.7 Oldsmar's Water Treatment System, EUA, 2021

Trata-se de incidente ocorrido na Flórida, nos Estados Unidos em 2021 no qual um hacker acessou remotamente um sistema SCADA e efetuando a alteração do nível de NaOH (hidróxido de sódio) de 100 ppm para 11000 ppm.

Não se trata de margens controladas de cloro ou de flúor, mas de níveis perigosos de soda cáustica que poderiam ter chegado às torneiras de milhares de pessoas causando graves danos à saúde da população. No caso em discussão, o invasor realizou uma tentativa de envenenamento de um sistema de abastecimento de água, por meio de uma plataforma de software de acesso remoto que encontra-se inativa há meses.

Não pode ser considerado um ataque cibernético particularmente sofisticado, uma vez que fez uso de uma ferramenta de acesso remoto chamado TeamViewer. Uma plataforma que já não estava mais sendo usada a cerca de seis meses antes do ataque ocorrer (MARQUARDT, LEVENSON, TAL, 2021).

Para especialistas em segurança cibernética, o culpado poderia facilmente ser adolescentes entediados, um funcionário insatisfeito, um estado-nação ou empreiteiros fazendo suas licitações. (ROBLES e PERLROTH, 2021),

As autoridades disseram que a trama se desenrolou quando um funcionário percebeu que alguém estava controlando seu computador. Ele inicialmente ignorou porque a planta tem um software que permite aos supervisores acessar os computadores remotamente. Mas horas depois, o funcionário percebeu que diferentes programas estavam sendo abertos e que o nível de soda cáustica mudou. A intrusão durou entre três e cinco minutos

(ROBLES e PERLROTH, 2021).

Embora a ação do hacker tenha sido impedido antes que pudesse chegar ao abastecimento de água potável, o cenário - um ataque cibernético a uma estação de tratamento de água que contamina a água de uma cidade - há muito é temido por especialistas em segurança cibernética. Em todo o país, os operadores de usinas de água, além daqueles em barragens e oleodutos e gasodutos, aceleraram a transformação para sistemas digitais que permitem que engenheiros e empreiteiros monitorem temperatura, pressão e níveis químicos de estações de trabalho remotas (ROBLES e PERLROTH, 2021).

5.8 Belle Vernon Water Treatment System, EUA, 2021

Refere-se à investigação realizada pelo FBI em razão de múltiplas tentativas de invasão ao sistema de distribuição de água de Belle Vernon na Pensilvânia. O caso ocorreu logo após o evento de Oldsmar´s na Flórida. Segundo informações da *Pennsylvania Water Action Response Network*, um grupo de agências municipais de água, dois sistemas foram vítimas das invasões cibernéticas, por meio de acesso e controle remoto. Felizmente os ataques foram detectados e a ação dos criminosos impedida.

Apesar de a Comissão de Serviços Públicos do estado passar a exigir que grandes concessionárias façam planos anuais de segurança cibernética, tal obrigação não se aplica a muitos sistemas municipais menores (OSDOL, 2021).

Scott Christensen, especialista em segurança cibernética da GrayMatter Systems, com sede em Warrendale, uma empresa que trabalha com serviços públicos, disse que o número de tentativas de hackers está aumentando (OSDOL, 2021).

6 | RECOMENDAÇÕES E MELHORES PRÁTICAS

De acordo com o exposto, fica evidenciada a atenção necessária às questões de segurança da informação e segurança cibernética, em todas as áreas, desde indústria, comércio e serviços, até mesmo no setor governamental. Ainda que seja um assunto com certo teor de novidade no Brasil, tem sido bastante debatido, com regulamentações que se encontram em fase de aprimoramento.

No setor de saneamento, setores específicos no território americano a tempos têm voltado suas atenções para o tema, vide a recorrência de eventos que atingem operadores de serviço de saneamento exemplificado neste estudo, emitindo orientações e melhores práticas a serem adotadas por tais operadoras.

O primeiro modelo refere-se à *Water ISAC* (Centro de Análise e Compartilhamento de Informações sobre Água) que é um órgão americano, formado pelas principais associações nacionais e fundações de pesquisa do setor de água e esgoto dos EUA. Em suas orientações, destacamos os fundamentos a serem implementados, e com as quais pretende-se mitigar riscos de possíveis ataques a seus sistemas. Os 15 fundamentos são:

1. Realizar inventário de ativos;

2. Avaliar os riscos;

3. Minimizar a exposição do sistema de controle;

4. Aplicar controles de acesso do usuário;

5. Proteção contra acesso físico não autorizado;

6. Instalar sistemas independentes de segurança física cibernética;

7. Implementar a gestão de vulnerabilidades;

8. Criar uma cultura de segurança cibernética;

9. Desenvolver e aplicar políticas e procedimentos de segurança cibernética (Governança);

10. Implementar a detecção e o monitoramento de ameaças;

11. Plano para incidentes, emergências e desastres;

12. Lidar com ameaças internas;

13. Proteja a cadeia de suprimentos;

14. Aborde todos os dispositivos inteligentes (*IoT, IIoT, Mobile*, etc.); e

15. Participe de Comunidades de Compartilhamento e Colaboração de Informações.

(WATER ISAC, 2019)

https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20%28WaterISAC%29.pdf

Outro exemplo de modelo a ser seguido refere-se ao sugerido pela EPA (*United States Environmental Protection Agency*) a qual desenvolveu recomendações para um programa de segurança cibernética, direcionado às empresas do setor de saneamento, as quais são elencadas abaixo.

1. Auditar sistemas de TI e identificar vulnerabilidades;

2. Manter uma lista dos maiores riscos de segurança cibernética e como eles serão abordados;

3. Assegurar que todos os sistemas de TI estejam atualizados com software antivírus e anti-malware;

4. Atualização mensal de patches de segurança em todos os sistemas de TI;

5. Implementar práticas seguras de acesso remoto;

6. Segregar as redes e controlar o acesso a redes baseadas nas atribuições do setor da empresa;

7. Monitorar atividades suspeitas na rede e estar preparado para responder se for detectado;

8. Estabelecer políticas de senhas fortes;

9. Considere uma lista de aplicações homologadas em sistemas críticos (permitir a execução apenas daqueles aprovados);

10. Melhorar a segurança física dos equipamentos de TI;

11. Segregar a empresa por área de negócio e sistemas de controle de processo, e exija credenciais de acesso para cada um;

12. Estabelecer políticas seguras para dispositivos móveis;

13. Desenvolver um plano de contingência e de recuperação para sistemas críticos de TI;

14. Desenvolver e testar Procedimentos Operacionais Padrões para o caso de comprometimento dos sistemas de controle;

15. Implementar redundâncias em seu sistema para evitar interrupções de serviço; e

16. Ministrar cursos em segurança cibernética para empregados e terceiros.

(EPA, 2021)

https://www.epa.gov/sites/default/files/2018-06/documents/cybersecurity_guide_for_states_final_0.pdf

Apesar de entidades distintas, os objetivos são os mesmos, tentar evitar que ataques sejam evitados ou pelo menos mitigados. Por essa razão as sugestões, quando olhadas sob a ótica global, possuem características convergentes.

Isso não significa que a implementação de um ou outro modelo será capaz de evitar a ação de hackers, ou outros agentes mal intencionados de mesma natureza, que pretendam explorar vulnerabilidade e comprometer a operação. O que se pretende é garantir uma segurança ao maior nível possível, dentro dos recursos disponíveis; em um primeiro momento, evitando possíveis vulnerabilidades pela simples falta de procedimentos adequados, e posteriormente pela implementação de recursos cada vez mais avançados que garantam níveis cada vez mais elevados de segurança.

O limite irá depender de vários fatores dentro da decisão estratégica de cada organização, uma vez que cada operadora de saneamento possui níveis de maturidade e estruturas de negócio, operação, tecnologia entre tantas outras, distintas umas das outras. Todos os fatores devem ser avaliados e associados ao apetite ao risco que se pretende aceitar a fim de dimensionar o nível de investimento necessário.

O fato é que infraestruturas críticas de saneamento tem por objeto recursos estratégicos como o esgoto, capaz de gerar impactos ambientais de grandes dimensões e a água é um bem essencial à vida humana.

7 | CONSIDERAÇOES FINAIS

Ainda que os governos tenham percebido a grave consequência de incidentes

decorrentes de segurança da informação, principalmente as do Estados Unidos e os dos países que compõem a União Europeia, conforme regulamentações citadas anteriormente, o Brasil, devido a diversos fatores, encontra-se incipiente tanto quanto a efetivação da segurança da informação, quanto às regulamentações e sanções aplicáveis. Tal constatação, no entanto, não exime a responsabilidade do poder público e entidades privadas atuantes em todos os setores da economia, em especial para o setor de infraestrutura crítica, como o de saneamento ambiental, energia e transporte, os quais devem tomar as ações necessárias para que incidentes dessa natureza não afetem a prestação de serviços.

Não existe sistema de segurança de informação totalmente imune a qualquer incidente de violação, o que existe é o apetite ao risco aceito pela corporação, dentro de uma relação entre a capacidade de investimento e o nível de proteção possível com os recursos disponíveis. Caberá ao setor responsável pela segurança da informação dimensionar a quantidade de recursos possível a fim de garantir um nível de proteção que permita à empresa administrar o risco aceito em uma área tão relevante como a de saneamento.

Por isso, é de suma importância que as operadoras de saneamento construam uma visão adequada de seus processos e riscos que permita avaliar o nível de segurança necessário. Somente assim será possível elaborar um planejamento dimensionado de forma adequada, com investimentos necessários para evitar os possíveis incidentes e mitigar os efeitos e danos daqueles que eventualmente possam ocorrer.

REFERÊNCIAS

ABRAMS, Marshall D.; **WEISS**, Joe. *Malicious Control System Cyber Security Attack Case Study - Maroochy Water Services*. Australia. Agosto/2008. Disponível em: <https://www.mitre.org/publications/technical-papers/malicious-control-system-cyber-security-attack-case-study-maroochy-water-services-australia>. Acesso em 21/08/2021.

ANI, U. D. et al. A review of critical infrastructure protection approaches: Improving security through responsiveness to the dynamic modelling landscape. In: IET Conference Publications. [s.l.]: [s.n.], 2019**.** doi: 10.1049/cp.2019.0131.

BING, Christopher; **BOSE**, Nandita. A Casa Branca pede às empresas mais importantes da América que melhorem as defesas cibernéticas. 28/06/2021. Disponível em: <https://www.reuters.com/world/us/white-house-calls-americas-most-critical-companies-improve-cyber-defenses-2021-07-28/>. Acesso em 21/08/2021.

BRASIL. Decreto nº 10.222, de 5 de Fevereiro de 2020. Estratégia Nacional de Segurança da Informação. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm>. Acesso em Maio de 2021.

CISA. About CISA. 2021. Disponível em: <https://www.cisa.gov/about-cisa> Acesso em Maio de 2021.

COLELLI, R. et al. An opacity approach for security exposure of IoT components in critical infrastructures. In: Conference Proceedings - IEEE International Conference on Systems, Man and Cybernetics. [s.l.]: [s.n.], 2019. DOI: 10.1109/SMC.2019.8914291.

DAVIS, G. "2020: *Life with 50 billion connected devices," 2018 IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas, NV, USA, 2018, pp. 1-1, doi: 10.1109/ICCE.2018.8326056.

DE VITRY, M.M. et al. *Smart urban water systems: what could possibly go wrong? Environmental Research Letters.* 2019, Vol. 14, nº 8. doi: 14 081001

EPA, *United States Environmental Protection Agency. EPA Cybersecurity Best Practices for the Water Sector.* Disponível em: <https://www.epa.gov/waterriskassessment/epa-cybersecurity-best-practices-water-sector>. Acessado em: 21/08/2021.

GONÇALVES, R.; SOARES, J. M. J.; LIMA, M. F. R. "An IoT-Based Framework for Smart Water Supply Systems Management." Future Internet 2020, 12, 114. https://doi.org/10.3390/fi12070114.

HASSANZADEH, A., **RASEKH**, A., **GALELLI**, S., **AGHASHAHI**, M., **TAORMINA**, R., **OSTFELD**, A., & **Banks**, M. K. (2020). *A Review of Cybersecurity Incidents in the Water Sector. Journal of Environmental Engineering* (United States), 146(5), [03120003].

JONES, Miriam. *Report: Hacking Lands Florida Wastewater Official in Hot Water*. 26/03/2012. Disponível em: <https://www.govtech.com/public-safety/report-hacking-lands-florida-wastewater-official-in-hot-water.html>. Acesso em: 21/08/2021.

LYNGAAS, Sean. *Israeli official confirms attempted cyberattack on water systems*. 28/05/2020. Disponível em: <https://www.cyberscoop.com/israel-cyberattacks-water-iran-yigal-unna/>. Acesso em: 21/08/2021.

MARQUARDT, Alex; **LEVENSON**, Eric; **TAL**, Amir. *Florida water treatment facility hack used a dormant remote access software, sheriff says*. 10/02/2021. Disponível em: <https://edition.cnn.com/2021/02/10/us/florida-water-poison-cyber/index.html>. Acesso em 21/08/2021.

MCMILLAN, Robert. *Hackers break into water system network*. 31/08/2006. Disponível em: <https://www.computerworld.com/article/2547938/hackers-break-into-water-system-network.html>. Acesso em 21/08/2021.

OMOTAYO, A.; **TELUKDARIE**, A. (2019). *Industry 4.0: Innovative Solutions for the water industry. International Annual Conference of the American Society for Engineering Management*; Huntsville, AL, USA, 2019.

OSDOL, Paul Van. *FBI investigating hacking threats at Pennsylvania water systems*. 10/05/2021. Disponivel em: <https://www.wtae.com/article/fbi-investigating-hacking-threats-at-pennsylvania-water-systems/36386504>. Acesso em 21/08/2021.

PLIATSIOS, D. et al. A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics. IEEE Communications Surveys and Tutorials, [s.l.], v. 22, no 3, p. 1942–1976, 2020. doi: 10.1109/COMST.2020.2987688.

ROBLES, T. et al. "*An IoT based reference architecture for smart water management processes." J. Wirel. Mob. Networks Ubiquitous Comput*. Dependable Appl. 6 (2015): 4-23.

ROBLES, Frances; **PERLROTH**, Nicole. '*Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town*. 08/02/2021. Disponível em: <https://www.nytimes.com/2021/02/08/us/oldsmar-florida-water-supply-hack.html>. Acesso em 21/08/2021

ROHR, Altieres. Hacker teria destruído bomba hidráulica após invadir sistema. 21/11/2011. Disponível em: <http://g1.globo.com/tecnologia/noticia/2011/11/hacker-teria-destruido-bomba-hidraulica-apos-invadir-sistema.html>. Acesso em 2/08/2021.

SKIBA, R. *Water Industry Cyber Security Human Resources and Training Needs, International Journal of Engineering Management.* Vol. 4, No. 1, 2020, pp. 11-16. doi: 10.11648/j.ijem.20200401.12.

TAQUARY, C. B. "A defesa cibernética em ambientes de infraestrutura crítica e os riscos dos ataques cibernéticos". Escola Superior de Guerra, Brasília, DF, Brasil, 2019.

THOMAS, R. J. et al. Catch Me if You Can: An In-Depth Study of CVE Discovery Time and Inconsistencies for Managing Risks in Critical Infrastructures. In: CPSIOTSEC 2020 - Proceedings of the 2020 Joint Workshop on CPS and IoT Security and Privacy. [s.l.]: [s.n.], 2020. DOI: 10.1145/3411498.3419970.

UE. Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016L1148>. Acesso em Julho de 2021.

US Department of Homeland Security. Budget-in-Brief. Fiscal Year 2020. p46. Disponível em: <https://www.dhs.gov/sites/default/files/publications/19_0318_MGMT_FY-2020-Budget-In-Brief.pdf> Acesso em Maio de 2021.

VIJAYAN, Jaikumar. *Apparent cyberattack destroys pump at Ill. water utility*. 18/11/2011. Disponível em: <https://www.computerworld.com/article/2497351/apparent-cyberattack-destroys-pump-at-ill--water-utility.html>. Acesso em 21/08/2021.

WATER ISAC. *15 Cybersecurity Fundamentals for Water and Wastewater Utilities*. 03/06/2019. Disponível em: <https://www.waterisac.org/fundamentals>. Acesso em 21/08/2021.

WEF. "*The Global Risks. Report 2021 16th Edition*". Disponível em: <http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf>. Acesso em Junho de 2021.

ÍNDICE REMISSIVO

G

H

I

L

M

O

P

www.atenaeditora.com.br
contato@atenaeditora.com.br
@atenaeditora
www.facebook.com/atenaeditora.com.br

Collection:

APPLIED ENVIRONMENTAL AND SANITARY ENGINEERING 2

Atena Editora
Ano 2022

www.atenaeditora.com.br
contato@atenaeditora.com.br
@atenaeditora
www.facebook.com/atenaeditora.com.br

Collection:

APPLIED ENVIRONMENTAL AND SANITARY ENGINEERING 2

Atena Editora
Ano 2022