

Projeto Integrador

Indústria inovação e infraestrutura

Cyber Segurança

Arthur Ramos de la Torre

Éder Gomes da Silva Júnior

Henrique Castilho Pires de Carvalho

Pedro Henrique Zafra

Rodrigo Herrera

Professor Eduardo Palhares

INTRODUÇÃO

A aparência dos Objetivos de Desenvolvimento Sustentável (ODS) foi coordenada pela Organização das Nações Unidas (ONU) com a finalidade de oferecer paz e prosperidade para as pessoas no mundo, com a erradicação da pobreza, proteção ao meio ambiente e ao clima (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2020).

De acordo com a ONU foram acertados 17 objetivos, aprovados por 193 países na Assembleia geral das Nações Unidas em 2015, cada um deles tem várias metas, totalizando 169 metas, metas essas que consideram o legado dos Objetivos do Desenvolvimento do Milênio (ODM), e a ONU pretende cumprir totalmente todos os ODS até o ano de 2030.

Visto isso, o objetivo escolhido em aula foi o: Indústria, inovação e infraestrutura, ele tem como objetivo querer construir infraestruturas, promover a industrialização de forma sustentável e estimular a inovação.

Com a escolha de objetivo feito, fomos para a escolha de um dos pilares da indústria 4.0, a cibersegurança foi setada como a que seria desenvolvida e debatida pelo grupo, como que a mesma deve e pode ser usada na região do ABC paulista de maneira mais efetiva, entender o porquê de ser um assunto que deveria ser melhor abordado e entender o porque é tão importante saber do assunto.



Cybersegurança é o exercício de proteger sistemas críticos e informações confidenciais dos ataques cibernéticos. Essa prática possui medidas traçadas para combater ameaças contra sistemas e aplicações de rede, independentemente se essa ameaça for proveniente de dentro ou de fora da empresa. (IBM,2021)

O vazamento de dados causou um custo médio de \$3.86 milhões nos Estados Unidos em 2020. Dentro deste valor, estão os gastos da descoberta e da resposta ao ataque, o tempo de inatividade e perda dos ganhos financeiros, o dano à reputação da empresa e sua marca a longo prazo, entre tantos outros.

Os responsáveis pelos ataques cibernéticos costumam direcionar o ataque às informações de identificação pessoal (PII) dos clientes, para obter detalhes como nomes, endereços, telefones, números de documentos, números de cartões de crédito e outros dados confidenciais. Posteriormente, essas informações serão utilizadas para a venda em um mercado clandestino ou para a prática de extorsão à pessoa afetada.

Agora o por que a cybersegurança é tão importante, uma abundância de termos que colocam o uso da Internet, a interconectividade das redes, e a convergência digital, na linha de frente das atenções das lideranças de vários países, a nova Sociedade da Informação e seus desafios (Canongia; M. Júnior; 2010). Um bom retrato da atualidade, a exemplificar, foi o ocorrido em julho de 2009 em que o sítio do Departamento de Defesa dos EUA foi invadido por dias consecutivos, numa ação que atualmente tem sido comum por parte dos chamados hackers, de tentativa de saturação de acesso e conexão a um determinado sítio da Internet até que o mesmo seja interrompido e seu acesso bloqueado. E, da mesma forma, sítios do governo da Coréia do Sul sofreram com ação similar, tornando lento o acesso à Internet naqueles mesmos dias do início de julho. (G1; 2010).

Outro exemplo de ataques cibernéticos, só que dessa vez mais recente, foi em março de 2021, quando houve a exploração do Dia Zero em servidores da Microsoft Exchange. A Kaspersky (Kaspersky é uma empresa tecnológica russa especializada na produção de softwares de segurança para a Internet), apontou que, cerca de 1,4 mil servidores da gigante da tecnologia foram alvos de ataques cibernéticos. Ainda, no final de fevereiro, o laboratório de cybersecurity descobriu que 12 sistemas Exchange tiveram vulnerabilidades "dia zero" exploradas. Segundo a Kaspersky, as ameaças à cybersegurança dos servidores da Microsoft aconteceram na Europa e nos Estados Unidos, partindo de diferentes grupos hackers. (Baldissera; 2021)

DESENVOLVIMENTO (Como a cidade escolhida pelo grupo está trabalhando com a respectiva ODS?)

Mesmo com a expansão de uso de internet no Brasil, o país ocupa ainda um posicionamento “ruim” em termos do ranking mundial daqueles países mais conectados na Rede, ocupando atualmente 590 lugar, segundo o World Economic Forum (WEF) (WWF apud SILVA,). Mesmo com este posicionamento no ranking mundial, segundo Alexandre Sanches Magalhães, gerente de análise do Ibope/NetRatings, o ritmo de crescimento da Internet brasileira é ativo. Em julho de 2009 foram contabilizados 64,8 milhões de internautas no Brasil, conforme dados do Ibope Nielsen Online, ou seja, um aumento de 2,5 milhões de pessoas em relação ao mês anterior. Em relação ao acesso via banda larga, o país atingiu 10,4 milhões de conexões (Canongia; M. Júnior; 2010).

Com o aumento da internet, o país necessita de uma forte segurança para a população, olhando para o momento atual o Brasil ficou no 18º lugar no

Índice Global de Segurança Cibernética 2020, levantamento feito por uma agência da ONU (Organização das Nações Unidas) que avalia as ações do governo com foco na proteção contra riscos cibernéticos. Ao subir 53 posições no ranking, o país também se tornou o terceiro melhor colocado da América, ficando atrás apenas dos Estados Unidos e Canadá. Outro fator que chamou a atenção foi a alta subida de posição no ranking, onde no ano anterior (2019), o país ocupava a 71ª colocação. (Canaltech, 2020).



ITUPublications International Telecommunication Union
Development Sector

Global Cybersecurity Index
2020

Table 5: GCI results: Americas region

Country Name	Overall Score	Regional Rank
United States of America**	100	1
Canada**	97.67	2
Brazil	96.6	3
Mexico	81.68	4
Uruguay	75.15	5
Dominican Rep.	75.07	6
Chile	68.83	7
Costa Rica	67.45	8
Colombia	63.72	9
Cuba	58.76	10
Paraguay	57.09	11

Com isso vem o questionamento: O Brasil está preparado para algum ataque? De acordo com a empresa Sophos, houve uma queda representativa no número de ataques contra empresas brasileiras no primeiro trimestre de 2021, sendo 38% (eram 67% em 2020). Entretanto, a sofisticação dos golpes e ataques vem evoluindo, tornando o ambiente muito mais perigoso. Algumas empresas como bancos, vem rodando em seus sistemas Windows XP ou Windows Server 2003, isso causa facilidade para os golpistas trabalharem. (Demartinj, 2021).

Em 2017 o Ministério Público de SP e o Tribunal de Justiça de SP decidiram desligar seus sistemas para não ter prejuízos. A WannaCry ameaçou “sequestrar” dados de hospitais, companhias e governos. O ataque causou a interrupção dos atendimentos do INSS – além de afetar os sistemas do Santander e da Vivo (Nogueira; 2020).



Atualmente no ABC Paulista, mais precisamente em São Caetano do Sul, encontramos poucos resultados, porém, observamos uma notícia do ano de 2018 no site da prefeitura municipal, no qual anunciava uma parceria com a multinacional de tecnologia Cisco Systems para a oferta de cursos profissionalizantes na cidade. A união foi testada e aprovada: a Escola Municipal recebeu da Cisco um certificado confirmando essa colaboração.

A Escola Municipal de Informática oferece cursos profissionalizantes em informática reconhecidos pela Cisco Systems. O sucesso dessa coparticipação é a garantia de melhores oportunidades de trabalho. Dentre os cursos oferecidos estava a cibersegurança.

CONCLUSÃO (RESULTADOS DA PESQUISA)

Logo após o entendimento do assunto entramos como questionamento: Como podemos adicionar e melhorar a cibersegurança em São Caetano do Sul? Com isso iremos criar um vídeo para debater sobre o assunto. Caso tenha uma boa repercussão podemos voltar e falar sobre outros assuntos que vemos problemas na região, como taxa de lixo, ciclovias etc. Também podemos trazer pessoas competentes no assunto para explicar sobre. Visto disso estamos dispostos a buscar o melhor resultado e conteúdo para explicar sobre o assunto e buscar as melhores soluções. Logo após o entendimento do assunto entramos como questionamento: Como podemos adicionar e melhorar a cibersegurança em São Caetano do Sul? Com isso iremos criar um vídeo para debater sobre o assunto. Caso tenha uma boa repercussão podemos voltar e falar sobre outros assuntos que vemos problemas na região, como taxa de lixo, ciclovias etc. Também podemos trazer pessoas competentes no assunto para

explicar sobre. Visto isso, estamos dispostos a buscar o melhor resultado e conteúdo para explicar sobre o assunto e buscar as melhores soluções.

REFERÊNCIAS BIBLIOGRÁFICAS

https://www.ibm.com/br-pt/security?utm_content=SRCWW&p1=Search&p4=43700057927479788&p5=b&gclid=EA1aIQobChMI5eOv9tXo8wIVDpXlCh3IDAsFEAAYASAAEgITcvD_BwE

http://seer.cgee.org.br/index.php/parcerias_estrategicas/article/viewFile/349/342

<http://g1.globo.com/mundo/noticia/2013/07/coreia-do-sul-denuncia-ataque-ciber-netico-do-norte.html>

<https://brasil.un.org/pt-br/sdgs>

<https://odsbrasil.gov.br/>

<https://canaltech.com.br/seguranca/brasil-sobe-53-posicoes-no-ranking-mundial-de-ciberseguranca-confira-as-razoes-189029/>

<https://canaltech.com.br/seguranca/o-brasil-esta-preparado-para-ataques-contr-a-empresas-de-infraestrutura-185633/>

<https://posdigital.pucpr.br/blog/ataques-ciberneticos>

<https://www.saocaetanodosul.sp.gov.br/post/parceria-de-prefeitura-de-sao-caetano-do-sul-com-academia-cisco-garante-ensino-profissionalizante-gratuito>

<https://olhardigital.com.br/2020/11/06/seguranca/conheca-os-maiores-ciberataques-da-historia-do-brasil/>