	COLÉGIO ESTADUAL PROTÁSIO ALVES	
	PROFESSOR/A: **DISCIPLINA**: Ética	**TIPO DE AVALIAÇÃO:**
DATA: ___/___/2022	**ALUNO:** **TURMA:**	**NOTA:**
OBSERVAÇÕES:		

TRABALHO AVALITATIVO 2 DE ÉTICA

Com base no texto abaixo, faça uma análise crítica em relação ao usuário e ao profissional da área de informática, principalmente quanto à ética no uso dos meios eletrônicos.

"Segurança cibernética

Pesquisa global mostra que ataques digitais estão mais sofisticados e mudando de perfil. Além disso, a LGPD, aprovada em 2018 e que entrará em vigor no próximo ano, começa a agitar o mercado de cibersegurança.

Pense em algo polimorfo perverso. E pense nisso infiltrado em seu e-mail, celular, notebook, no acervo de dados de sua empresa ou instituição financeira. Agora multiplique por todo mundo, pessoa física ou jurídica, que você conhece. É essa a fórmula da encrenca em formato de realidade. Modelagens de ataques virtuais em nada diferem de todos os grandes vilões ficcionais – são mutantes e, assustadoramente, têm rápida evolução. E quem diz isso é a pesquisa Global Threat Intelligence Report 2019, da NTT Security, que revela crescimento de 156,8% nos casos de vulnerabilidade de segurança digital num prazo de apenas dois anos (de 6.447, em 2016, para 16.555, em 2018). Isso equivale a colocar sob exposição estragos equivalentes a mais de US$ 36 bilhões do PIB das 279 maiores cidades do planeta. Apenas as economias de Los Angeles, Londres, Nova York, Paris e Tóquio poderiam perder, cada uma, em torno de US$ 1 bilhão cada.

Ao explorar trilhões de logs e bilhões de ataques, a pesquisa também elenca as ameaças mais comuns. No topo do ranking estão os Web Application Ataques (32% da artilharia virtual se deu dessa maneira), quando links maliciosos chegam via um e-mail, por exemplo. Esse tipo de ameaça mostra-se uma tendência, já que dobrou de frequência desde 2017 e já bate em 1/3 das ocorrências. Depois aparecem os Ataques de Reconhecimento (16%), nos quais os cibercriminosos invadem ou tentam invadir sistemas para reconhecer vulnerabilidades, seguidos por Ataques Específicos Contra Serviços (13%), quando acontecem ações orquestradas e concentradas dirigidas a uma máquina ou rede para torná-la inacessível aos usuários. Para o CEO da NTT Security, Katsumi Nakata, uma combinação, que alia o aumento do número de dispositivos conectados à internet com o elevado número de plataformas de redes sociais ainda não reguladas gerando conteúdos não confiáveis, está na base dessa exposição exponencial. "Isso deu aos cibercriminosos muitas oportunidades de explorar as organizações", disse Nakata.

SETORES VULNERÁVEIS

Em outras palavras, não há segmento imune. Entre os setores econômicos, a preferência global dos atacantes se divide entre as áreas Financeira (17%) e Tecnológica (também 17%). Logo atrás aparecem Serviços Profissionais (12%), Educação (11%), Governos (9%) e Varejo (6%). Apesar de a bandidagem virtual curtir investidas contra os setores de Finanças e Tecnologia, eles são, também, as áreas mais bem preparadas contra esses ataques. Em

contrapartida, os setores Governamental e Varejo estão entre os mais expostos e que menos se protegem.

Mark Thomas, vice-presidente de Segurança Cibernética da Dimension Data, empresa do grupo NTT que coassina a pesquisa, diz que “claramente há muito trabalho a ser feito em todos os setores para criar posturas de segurança mais robustas de dados”. Apenas no segmento Educação, hoje o quarto campo mais visado, os ataques cresceram 459%. Muito dessa escalada está relacionada à ascensão das criptomoedas. Um sistema de pagamentos seguro e, o melhor, praticamente não rastreável colabora, e muito, para que o crime virtual compense. (...)”

Fonte: https://www.istoedinheiro.com.br/seguranca-cibernetica/