Projeto de Formatura – 2024

PCS - Departamento de Engenharia de Computação e Sistemas Digitais

Engenharia de Computação

Tema: Desenvolvimento de um Guia de Maturidade em Cibersegurança para Pequenas e Médias Empresas (PMEs) com Soluções Open Source

INTRODUÇÃO

Em uma era de avanços tecnológicos rápidos e crescente transformação digital, o desafio de compreender em tempo real os riscos de cibersegurança e as necessidades de infraestrutura tornou-se ainda mais evidente, especialmente para pequenas e médias empresas (PMEs). Embora a digitalização de produtos e serviços tenha aberto novas oportunidades, também expôs essas empresas a vulnerabilidades, com muitas enfrentando dificuldades para implementar medidas adequadas de cibersegurança devido a altos custos, complexidade técnica ou falta de conhecimento. Reconhecendo essa problemática, este projeto busca preencher essa lacuna ao desenvolver uma ferramenta/guia para avaliar a maturidade em cibersegurança, voltados especificamente para PMEs. Utilizando conhecimentos e ferramentas open source, a iniciativa visa capacitar essas empresas a identificar suas fragilidades, criar planos de ação e fortalecer sua resiliência em um cenário cada vez mais digital.

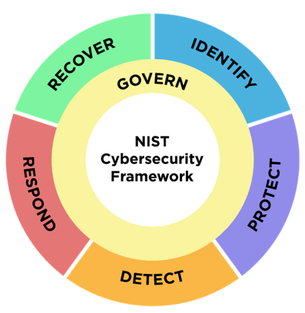
MOTIVAÇÕES E OBJETIVOS

Considerando a relevância das PMEs, que representam mais de 90% das empresas em algumas economias, garantir sua segurança e disponibilidade é fundamental. Além de seu impacto na empregabilidade e prestação de serviços, muitas PMEs têm parcerias com grandes organizações, de modo que vulnerabilidades presentes nas organizações de menor porte possam colocar em risco também suas parceiras.

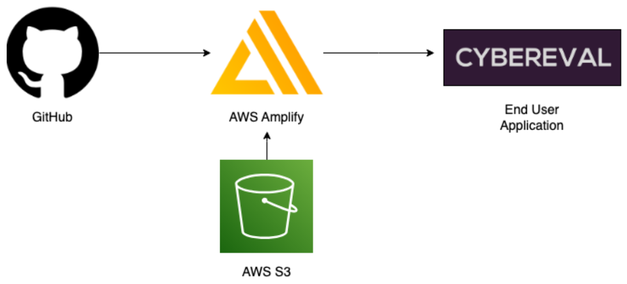
Sob uma perspectiva prática, compreender os riscos aos quais uma organização está exposta pode não ser algo evidente. É preciso considerar vários cenários e perspectivas, além de decifrar conceitos técnicos de modo a não deixar brechas que criem ou potencializem vulnerabilidades. Embora exista uma ampla disponibilidade de informações sobre cibersegurança, a diversidade de fontes na internet, as vezes com detalhes contraditórios, pode gerar confusão e desconfiança. Além disso, ao focar em PMEs e startups de tecnologia, observa-se uma lacuna na adoção de soluções open source, que poderiam auxiliar a lidar com os altos custos associados à infraestrutura de cibersegurança. Essa situação evidencia uma oportunidade de aproveitar ferramentas e informações disponíveis de maneira mais eficiente e direcionada.

METODOLOGIA

Este trabalho inicia com uma revisão bibliográfica abrangente para mapear o estado atual das práticas de cibersegurança, identificando objetivos, desafios e lacunas enfrentados por PMEs. A pesquisa inclui artigos acadêmicos, relatórios da indústria e opiniões de especialistas, destacando dificuldades comuns, como recursos limitados, falta de expertise e medidas de segurança insuficientes. Além de apontar os desafios, busca-se identificar boas práticas existentes que possam reforçar as soluções propostas. A metodologia central do trabalho apresenta uma avaliação de maturidade em cibersegurança baseada no NIST Cybersecurity Framework 2.0, escolhido por sua acessibilidade e alinhamento com outros padrões, como ISO 27000 e COBIT. Além disso, são listadas fontes confiáveis de informação e ferramentas open source que PMEs podem utilizar para melhorar sua postura de segurança, organizadas conforme as necessidades identificadas na revisão bibliográfica.



Funções do NIST CSF 2.0

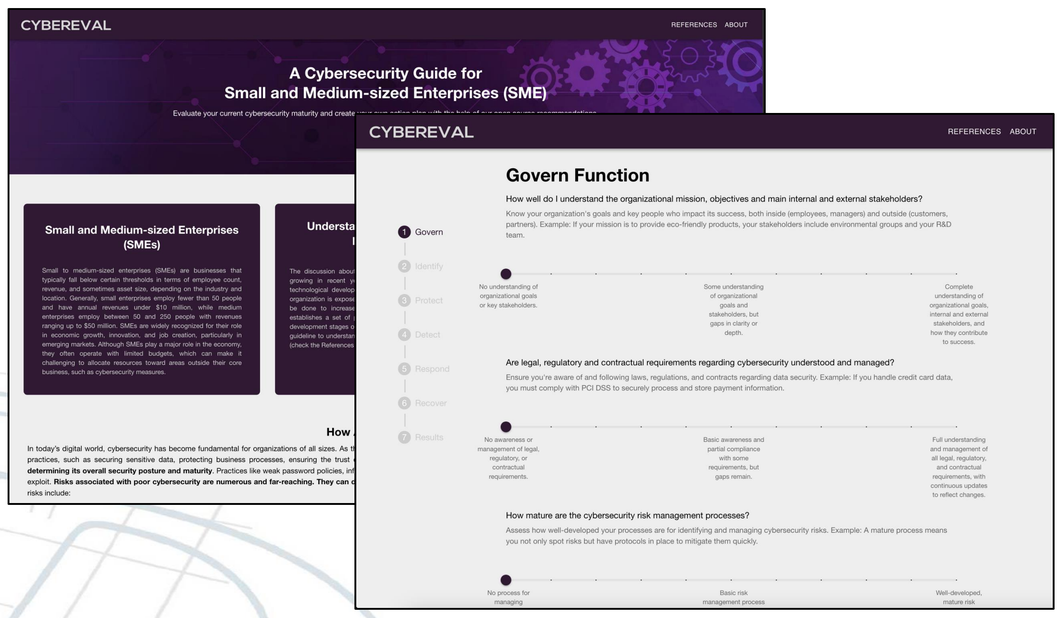


Arquitetura da aplicação web

Com base nos estudos teóricos, uma aplicação técnica é implementada. O código-fonte é versionado e armazenado em um repositório no GitHub, que está integrado ao AWS Amplify para automatizar o processo de build e disponibilização online conforme o código é atualizado. O projeto utiliza os serviços de hospedagem da AWS para tornar a aplicação acessível pela internet. Além disso, arquivos CSV armazenados no AWS S3 são usados para gerar tabelas e fornecer informações às páginas da aplicação, acessados por meio de requisições programadas.

SOLUÇÃO PROPOSTA

Este trabalho implementa uma aplicação web, baseada no guia teórico desenvolvido, como ferramenta para que organizações avaliem seu nível de maturidade em cibersegurança e criem planos de ação baseados nos resultados obtidos. A aplicação tem como objetivo tornar o conceito de maturidade em cibersegurança acessível e aplicável, oferecendo uma interface prática e amigável para usuários de diferentes níveis de conhecimento técnico. A ferramenta resultante combina os insights obtidos, fornecendo recomendações práticas e um roteiro personalizado para elevar a maturidade em cibersegurança das PMEs. Assim, o trabalho busca oferecer soluções acessíveis, práticas e adaptadas às necessidades específicas desse público, contribuindo para a redução de vulnerabilidades e o fortalecimento da segurança digital.



Funções do NIST CSF 2.0

CONCLUSÃO E PRÓXIMOS PASSOS

Tendo em vista os elementos apresentados, a CyberEval oferece contribuições relevantes para enfrentar os atuais desafios de cibersegurança. Primeiramente, ela promove a centralização de informações provenientes de fontes confiáveis, identificando os principais atores na área da cibersegurança, incluindo instituições governamentais e organizações apoiadas pela comunidade de open source. Mais precisamente, este projeto é baseado no NIST Cybersecurity Framework 2.0 e fornece esse conjunto de informações de forma mais acessível com definições, exemplos e casos de uso para auxiliar no uso da ferramenta. Além disso, a CyberEval dá ênfase ao uso de ferramentas e informações open source, permitindo acompanhar as melhores práticas do setor enquanto reduz significativamente os custos de implementação. Por fim, propõe a adaptação da ferramenta de avaliação de maturidade de cibersegurança, considerando o grau de desenvolvimento e crescimento das empresas. Essa abordagem segmentada busca resolver um dos principais desafios identificados na literatura: a dificuldade de startups, por exemplo, em adotar ferramentas devido à falta de alinhamento com suas realidades operacionais.

Em suma, este trabalho representa um passo significativo na direção de tornar a cibersegurança mais acessível e prática para pequenas e médias empresas, fornecendo ferramentas e orientações que simplificam conceitos complexos e ajudam organizações a avaliarem e melhorarem sua maturidade em segurança digital. Embora existam desafios, como a necessidade de suporte técnico especializado e a subjetividade em algumas avaliações, as contribuições realizadas são uma base promissora para o desenvolvimento de soluções mais abrangentes e personalizadas no futuro. Além disso, a possibilidade de incorporar exemplos práticos, adaptar ferramentas às necessidades específicas dos usuários e explorar o retorno sobre os investimentos em segurança são perspectivas animadoras para evoluir ainda mais a iniciativa.

A cibersegurança é um esforço coletivo que depende do engajamento de todos, pequenas mudanças podem gerar impactos significativos na proteção de dados, sistemas e de organizações inteiras. Cada contribuição individual fortalece não apenas a segurança da própria empresa, mas também de toda a comunidade, criando um ambiente digital mais confiável e resiliente para todos.

Integrantes: Rafael Yuji Yokowo
Professor(a) Orientador(a): Prof. Dr. Tereza Cristina Melo de Brito Carvalho