UNIVERSIDADE
FEDERAL DO CEARÁ

AUDITORIA E SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

Relatório: Ransomware

Como foi dividido

O trabalho foi dividido em bloco, o primeiro bloco foi o planejamento, no domingo dia 30 de abril foi realizado uma chamada via meet onde o ponto debatido foi sobre como seria divido os próximos passos, ficou dividido dessa forma: Relatório: Victor e Franciel, Apresentação: Gabriel, Contextualização:Victor, História E Tipos: Franciel, Como se pega e se proteger: Abner e Exemplo prático: Gabriel. O segundo bloco seria o desenvolvimento do trabalho em si e por fim o bloco de revisão do conteúdo.

Dificuldades encontradas

Por ser um conteúdo bem técnico e específico, tivemos algumas dificuldades em compreender o funcionamento exato de um ransomware, como ele se prolifera e como criar um.

Relevância do tema

Ransomware é um tema de extrema relevância nos dias de hoje, devido ao seu impacto significativo na segurança cibernética e nas vítimas envolvidas. Alguns pontos que mostram esta relevância:

Crescimento alarmante: O ransomware tem experimentado um crescimento alarmante nos últimos anos. O número de ataques e as somas exigidas como resgate têm aumentado significativamente. Isso coloca em evidência a necessidade de entender e combater essa ameaça.

Impacto econômico: O ransomware tem um impacto econômico substancial nas organizações e empresas afetadas. Os ataques resultam em perda de produtividade, custos de recuperação, pagamento de resgates e possíveis danos à reputação. As consequências financeiras podem ser devastadoras, tanto para grandes corporações quanto para pequenas empresas.

Ameaça à segurança dos dados: O ransomware coloca em risco a segurança e a privacidade dos dados sensíveis. A criptografia de dados impede o acesso legítimo e pode levar à perda permanente de informações valiosas. Isso é especialmente preocupante em setores como saúde, finanças e governo, onde a confidencialidade dos dados é crucial.

Alvos diversos: O ransomware não discrimina seus alvos. Ele pode afetar empresas, instituições governamentais, organizações sem fins lucrativos e até mesmo usuários

individuais. Todos estão suscetíveis a se tornarem vítimas, independentemente do tamanho ou da indústria em que estão inseridos.

Evolução e sofisticação: Os ataques de ransomware estão em constante evolução e se tornando mais sofisticados. Os hackers desenvolvem novas variantes e técnicas de infecção, dificultando a detecção e a defesa eficaz contra esses ataques. Portanto, é fundamental estar atualizado e consciente das ameaças em constante mudança.

Consequências sociais: Além dos aspectos econômicos e de segurança, o ransomware também pode ter consequências sociais negativas. Por exemplo, ataques a serviços essenciais, como hospitais ou infraestrutura crítica, podem colocar vidas em perigo. A interrupção de serviços vitais pode ter um impacto direto nas comunidades e na sociedade como um todo.