

Relatório de Potenciais Vulnerabilidades e Ameaças para o Banco Pan

A equipe ITT, percorreu pelo ano a função de criar topologias a fim de manter a infraestrutura de redes do Banco Pan, de maneira organizada, segura e ágil. De todo modo, como qualquer outro programa ou estruturação, por mais minucioso e detalhado que seja seu desenvolvimento, ele pode estar vulnerável à ataques que comprometam a segurança de informação e tragam diversos riscos ao nosso cliente!

O termo “risco” deve ser classificado de diversas maneiras diferentes, mas pode ser simplificada e entendido como qualquer evento que possa ter impacto negativo sobre a capacidade da empresa de alcançar seus objetivos de negócio ou, ainda, como a combinação da probabilidade de ocorrência de um evento e suas consequências. Assim sendo, esse relatório tem como principal objetivo apontar riscos que devem ser observados, para que a empresa evite o máximo de ameaças possíveis, podendo dar continuidade a sua evolução/expansão corporativa.

Quando a equipe dissertou sobre o assunto, a grande ênfase foi de ressaltar a proteção que se deve ter em cima dos data centers, já que o mesmo foi a principal demanda dos clientes, logo, um bom plano de reestruturação de banco de dados deve ser acompanhado por uma excelente utilização de equipamentos e profissionais que consigam evitar o vazamento desses dados, afinal, dados vazados são sempre problema, mas se tratando de um banco, são infinitas vezes mais prejudiciais!

Algumas vulnerabilidades que devem ser observadas são: **Ataques DDoS**(negação distribuída de serviço) que torna os servidores da empresa indisponíveis, trazendo riscos caso não exista um sistema de segurança interno, e independente de um servidor específico para funcionar; **Sniffing ou Scan** uma varredura na rede para identificar quais sistemas e aparelhos estão sendo utilizados, e quais são os potenciais alvos da vítima selecionada, esses podendo ser em primeira instância passivos, porém visando um ataque posterior que venha a comprometer o sistema do Banco; **DNS Hijacking** trata-se de uma técnica usada pelos invasores que aproveitam a vulnerabilidade dos firmwares de roteadores na hora em que há requisição DHCP para um host, nesse momento o invasor faz o intermédio na conexão através de uma conexão insegura a um roteador público ou uma aplicação web, acessando informações cruciais para o acesso ao computador da vítima; além de existir o fator da **Má Implementação de Softwares** que podem comprometer o sistema de maneira fácil, a partir de uma errônea configuração de Firewalls e Antivírus; deixar seus sistemas, e aplicativos implementados **sem atualizações constantes** pode ser outro fator muito prejudicial a cyber segurança da empresa Banco Pan.

Demonstrado algumas vulnerabilidades e ameaças das quais o Banco Pan pode sofrer, nós do ITT gostaríamos de ressaltar a necessidade da contratação de uma boa equipe para a implementação da rede a ser utilizada, um banco seguro, também quer dizer um banco confiável e com cada vez mais clientes!

Nós somos o ITT e agradecemos pela sua atenção.

INTEGRANTES:

Rafael Afonso RM:85321

Murilo Teixeira RM:87136

Lucas Bertelini RM:89085

Gabriel Mota RM:88632

Gabriel Maciel RM:86200