TRUSTEDSEC

Date: December 11, 2023
Subject: Azure Cloud Penetration Test

Background

In November 2023, TrustedSec was contracted to perform a Azure Cloud Penetration Test of 3Cloud Azure Cloud Environment. Testing was conducted remotely from TrustedSec offices in Fairlawn, Ohio, targeting the Azure Cloud users with social engineering. The objectives of this assessment were to identify potential security deficiencies, recommend mitigation strategies to reduce the impact to critical business data, and assist in securing the overall network environment. The following phases encompassed the breadth of testing performed:

- Azure Cloud Penetration Test

The Azure Cloud Penetration Test scope for the Azure Cloud Environment was restricted to Azure Cloud users provided by 3Cloud. The assessment represents a point-in-time analysis of the target environment and the systems that were accessible during the testing period.

The engagement started on November 06, 2023 and was completed on November 17, 2023. The testing process began with an information gathering phase, in which the TrustedSec engagement team conducted steps designed to gather pertinent information surrounding the target environment. Manual and supporting automated testing techniques were then used to assess the target areas and gauge the level of impact to the business in relation to any discovered vulnerabilities. Controlled exploitation, where possible, was performed to measure the effectiveness of 3Cloud's ability to detect, deflect, and defend against potential system compromise.

Based on the severity of the deficiencies discovered during the course of this engagement, the overall security posture of 3Cloud maintained a relatively high level of maturity.

The assessment was performed utilizing methodologies based on industry best practices, such as the Open Web Application Security Project (OWASP) Web Security Testing Guide and Penetration Testing Execution Standard (PTES).

Cloud Penetration Test Methodology

TrustedSec's Cloud Penetration Test is a combination of traditional penetration testing, coupled with testing specific to either the Microsoft (Azure) or Amazon (AWS) Cloud platforms. While some aspects of traditional penetration testing methodologies are

applicable to these environments, the overall attack surface is different from traditional networks and could result in missing important issues. Testing can range from unauthenticated, which assesses the external cloud perimeter only, to assumed-access testing, which would simulate a breach or other internal cloud environment access.

TrustedSec uses platform-specific security testing guidelines, along with the Penetration Testing Execution Standard (PTES), a standard that has gained wide adoption within the information security community, as a methodical way to approach a Cloud Penetration Test. PTES defines a penetration test as the ability to attack and organization as an adversary, with a goal of affecting a company's potential to generate revenue. Additionally, TrustedSec utilizes, OWASP top 10, NIST SP800-210 (General Access Control Guidance for Cloud Systems), and platform-specific frameworks such as the CIS Microsoft Azure Foundations Benchmark, and CIS AWS Foundations Benchmark.

Conclusion

The assessment deliverable outlines the discovered vulnerabilities, affected systems, and the associated recommendations, based on the assessment scope. This information will aid 3Cloud in adequately mitigating the threat to business processes, to ensure the protection of Personally Identifiable Information (PII), and to secure critical business data. With this information, 3Cloud's partners can be assured that 3Cloud has performed due diligence, from an Information Security standpoint, by engaging an experienced, trusted, and independent third-party to evaluate the security of the network and/or application environment.

Use of This Document

This document has been prepared solely for the use of 3Cloud (the 'Client') and its officers, directors, and employees (collectively with the Company, 'Client Entities'). Client shall own all right, title, and interest in and to any written summaries, reports, analyses, and findings or other information or documentation prepared for Client in connection with TrustedSec, LLC ('TrustedSec') consulting services to Client. TrustedSec specifically disclaims any and all liability for any damages whatsoever (whether foreseen or unforeseen, direct, indirect, consequential, incidental, special, exemplary, or punitive) arising from or related to reliance by anyone, any guidance in this report, or any contents thereof.