UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
Centro di ateneo per i Servizi Informativi
Divisione Sistemi

Contromisure alla compromissione delle utenze

Sommario

Introduzione

In un ambiente di lavoro moderno, la sicurezza informatica rappresenta una delle maggiori preoccupazioni per le organizzazioni. In particolare, in un sistema complesso e multipiattaforma di identificazione e autorizzazione (IAM) come quello utilizzato dall'Ateneo, che integra sistemi cloud come Microsoft 365, è essenziale garantire la sicurezza dei dati e prevenire la compromissione degli utenti e delle relative risorse.

Per assicurare una rapida azione in caso di dubbi di eventuali compromissioni rilevati da comportamenti anomali, è fondamentale bloccare le sessioni e richiedere un cambio password attraverso un sistema a più fattori (MFA). Questo mitiga i possibili danni a discapito di un numero più elevato di falsi positivi che possono costringere l'utenza al cambio password. Inoltre, il cambio password con sistemi MFA come AppIO garantisce la certezza dell'identità, aumentando ulteriormente il livello di sicurezza.

In questo documento, esamineremo il sistema implementato per la rilevazione del rischio alto degli utenti e la rapida implementazione della contromisura.

Descrizione del sistema:

Il sistema di rilevazione del rischio di compromissione degli utenti nel Tenant 365 Microsoft è un sistema Microsoft (Identity Protection) che attraverso regole ormai definite e standard eleva la percentuale di rischio di compromissione dell'utente fino a portarla al valore "Alto"

Il sistema di Ateneo per la gestione delle utenze (provisioning e deprovisioning) è basato sul prodotto opensource Forgerock che consente l'identificazione attraverso anche LDAP che alimenta Microsoft 365 mantenendo la password sul sistema LDAP.

La password degli utenti, quindi, è solo sul sistema LDAP on premise: questo significa che le password degli utenti non sono memorizzate nel cloud di Microsoft 365, ma solo sul sistema on premise dell'organizzazione. Ciò migliora la sicurezza del sistema, in quanto i dati degli utenti sono protetti da eventuali vulnerabilità del cloud di Microsoft 365. Tuttavia, ciò significa anche che il sistema Identity Protection deve essere integrato con il sistema on premise LDAP per funzionare correttamente e bloccare l'utente bloccando il single sign on (SSO)

La comunicazione all'utente che è sotto attacco e che nell'interesse di tutti il suo accesso è stato bloccato, avviene attraverso Appio: l'Appio è l'applicazione di messaggistica istantanea della PA che consente di comunicare con gli utenti attraverso l'accesso via SPID o CIE all'App.

L'utente per riaccedere deve semplicemente cambiare password con gli strumenti già conosciuti CF e PUK.

Quando il sistema Identity Protection rileva che un utente è a rischio di compromissione, blocca l'accesso alle risorse del tenant e dell'area riservata e invia un messaggio attraverso

l'Appio che avvisa l'utente del blocco per il potenziale attacco e lo invita a cambiare la propria password. In questo modo, l'utente è in grado di adottare misure di sicurezza tempestive per prevenire la compromissione dei dati.

Se l'utente non è in possesso dell'AppIO, in caso di mancato accesso, procederà alla verifica del blocco della propria identità digitale per comportamento anomalo su http://softwaresso.unina.it/spam/spam1.php e seguirà le indicazioni del caso.

Conclusioni

In conclusione, il sistema rappresenta un'importante misura di sicurezza per l'Ateneo

Tuttavia, è importante sottolineare che questo sistema rappresenta solo un requisito minimo di sicurezza per l'organizzazione, soprattutto per quelle che operano nella Pubblica Amministrazione come l'Ateneo. È necessario adottare ulteriori misure di sicurezza, come la formazione degli utenti e l'implementazione di politiche di sicurezza, per garantire la protezione completa dei dati e prevenire eventuali attacchi informatici. Inoltre, è importante che il sistema si arricchisca di ulteriori strumenti, già in via di acquisizione, per la generazione di tutti i necessari report da fornire in caso di reale compromissione dell'utente e strumenti che individuino attacchi perimetrali al sistema Ateneo (MITRA) contribuendo alla massima efficienza nella prevenzione di eventuali attacchi informatici.

Napoli

19-03-2023

Divisione Sistemi

Ing. Giovanni B Barone