SERVIZI DI AUTENTICAZIONE

Come mettere in sicurezza dati e informazioni sensibili in modo semplice e flessibile grazie al servizio **SafeAccess** by **Namirial**

Marzo 2024

GUARDIA DIGITALE

Piazza Madonna della Neve, 5
50122 FIRENZE (ITALIA)

Indice

1. Servizi di autenticazione: qual è il problema delle password?

Come avviene per ogni innovazione, la **trasformazione digitale** porta con sé sia vantaggi che rischi: se da una parte consente di lavorare in modi nuovi, veloci e flessibili, dall'altra implica la gestione di un'enorme quantità di **informazioni** e **dati sensibili**, che aziende e organizzazioni devono necessariamente proteggere per poter lavorare in sicurezza. L'**Identity and Access Management** e la **Sicurezza Informatica**, di conseguenza, sono ad oggi più che mai fondamentali.

Gli attuali sistemi di autenticazione, basati sull'utilizzo delle credenziali, hanno tuttavia troppi difetti per garantire la sicurezza per quanto riguarda informazioni e dati sensibili. Secondo il **Data Breach Investigation Report 2022**, le credenziali sono il primo obiettivo degli hacker. Le password sono infatti piuttosto facili da rubare: a causa del fenomeno della ***Password Fatigue***, gli utenti tendono non solo a scegliere password deboli, ma anche a utilizzare le stesse per più applicazioni, "facilitando" il lavoro dell'hacker.

In **ambito lavorativo** vanno considerate ulteriori problematiche legate al **fattore umano**, come il fatto che spesso gli utenti condividono le loro password con i colleghi o lasciano incustoditi i loro PC, senza bloccare l'accesso ai file.

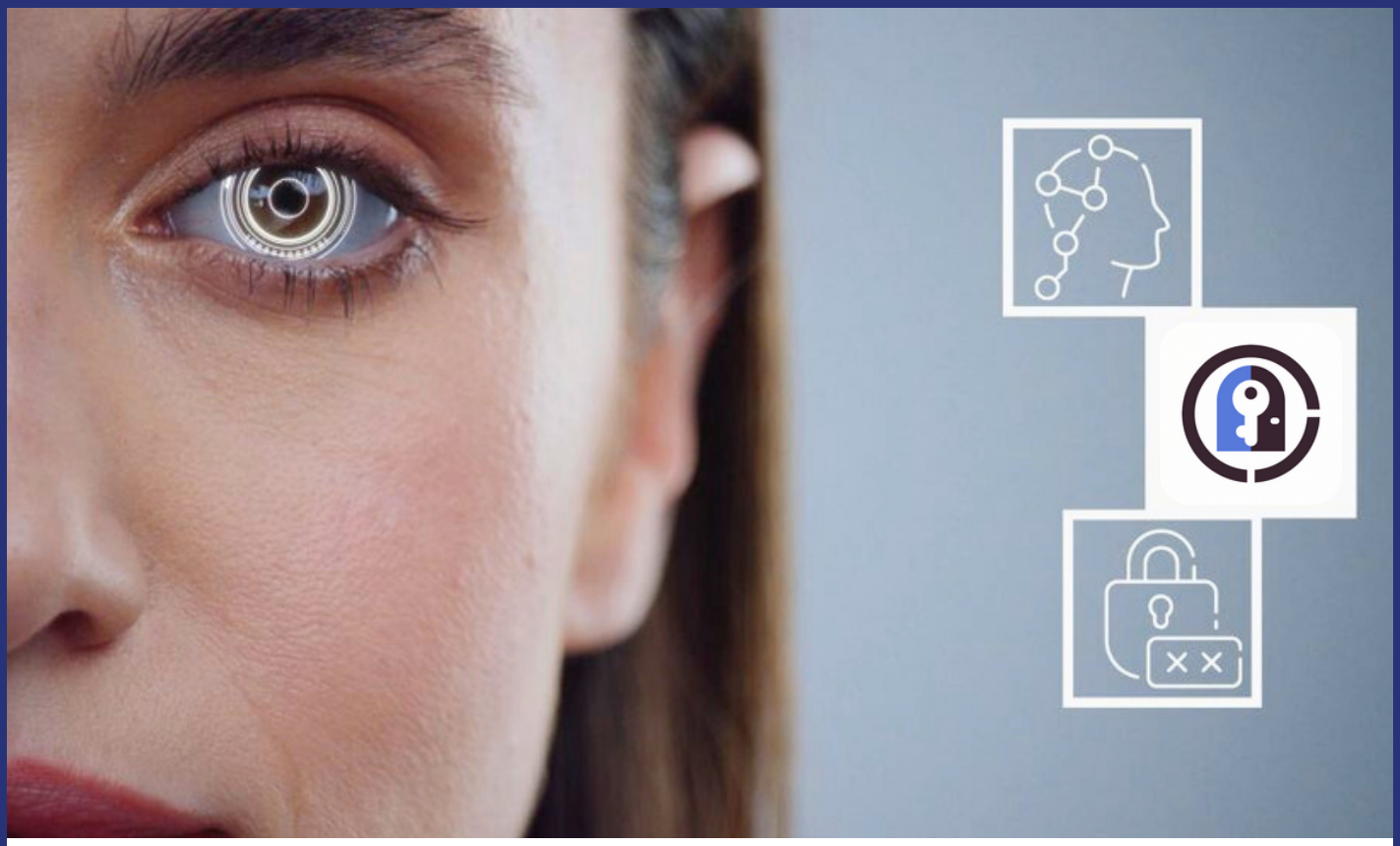
Un ulteriore problema con le password è legato al fatto che i reparti IT risultano costantemente sovraccaricati per la risoluzione dei problemi legati prima di tutto alla gestione dei *reset* delle *password*: ciò implica un dispendio non solo in termini di tempo, ma anche di costi. **Forrester**, ad esempio, stima che il costo medio di un singolo *reset* della password sia di 70 $.

Infine, ma certo non per importanza, c'è il tema della ***compliance* normativa**: nel 2020 la Commissione europea ha avviato la revisione della **Direttiva NIS** con l'obiettivo di rafforzare la sicurezza cibernetica in Europa e di garantire la continuità dei servizi digitali in caso di incidenti. La **Direttiva NIS2**, che sarà vincolante dal prossimo ottobre, ha rafforzato i requisiti minimi di sicurezza e le procedure di notifica obbligatoria degli incidenti informatici ed ha ampliato le attività richieste per la valutazione delle vulnerabilità, estendendo il novero dei soggetti interessati dalla disciplina, includendo anche i fornitori di prodotti elettronici e informatici, la grande distribuzione alimentare, i servizi postali, etc.

2. Autenticazione multifattoriale: di cosa si tratta?

Com'è possibile, dunque, proteggere al meglio informazioni e dati sensibili e mettere in sicurezza le postazioni di lavoro? Il modo migliore in cui le aziende possono superare questo tipo di problemi e rafforzare la sicurezza è abbandonare la vecchia autenticazione basata su password e passare a **metodi di autenticazione a più fattori**: la cosiddetta "autenticazione multifattoriale" o "*multi-factor authentication*".

L'**autenticazione multifattoriale** è una modalità identificativa che consiste nell'utilizzo di credenziali (username e password) con l'aggiunta di un metodo di autenticazione fisico: la sicurezza in questo modo è garantita dall'unione di due fattori, ovvero "qualcosa che l'utente sa", cioè le credenziali, e "qualcosa che l'utente ha", ovvero un dispositivo fisico, come un token o un badge, oppure "qualcosa che l'utente è o fa", ovvero una sua impronta digitale, un suo gesto o semplicemente il suo volto. In particolare, si parla di **autenticazione *passwordless*** solo quando si verifica un utente o un dispositivo con un qualsiasi metodo di autenticazione che non sia basato sulla conoscenza. L'autenticazione *passwordless* permette di proteggere al meglio informazioni e dati sensibili, riducendo il rischio di furto di credenziali.



3. La soluzione di Guardia Digitale: *Safe Access* by Namirial

La soluzione che **Guardia Digitale** ha scelto per adottare una strategia ottimale di Identity Trust è il servizio ***SafeAccess*** by **Namirial**. Basata su standard FIDO, tale soluzione rappresenta il perfetto sistema di **autenticazione *passwordless***, che consente di mettere in sicurezza le postazioni di lavoro di piccole, medie e grandi imprese, offrendo una soluzione semplice, rapida e adattabile alle esigenze di ogni specifica realtà lavorativa.

Il servizio consente un **alto livello di sicurezza** grazie all'utilizzo di un **secondo fattore di autenticazione *passwordless*** selezionabile tra un ampio ventaglio di possibilità (Token, Smart Card, Badge, Mobile App o FIDO device) a seconda delle abitudini e delle esigenze dell'azienda o dell'organizzazione.

Un esempio? Se all'interno di un'organizzazione i dipendenti utilizzano già il badge per registrare la propria presenza, è possibile utilizzare lo stesso dispositivo per consentire l'accesso sicuro alle applicazioni, facendo del badge il secondo fattore di autenticazione, in modo da facilitare l'adozione da tutte le parti coinvolte, dal reparto IT agli utenti finali.

Indipendentemente dal tipo di secondo fattore di autenticazione scelto, la soluzione SafeAccess è anche dotata di un'**interfaccia web semplice e intuitiva**, che permette all'amministratore di gestire facilmente il ciclo di vita delle credenziali. La flessibilità offerta dal servizio si riflette anche a livello di implementazione: in primo luogo perché si basa su **microservizi**, per cui ogni modulo è responsabile di una specifica operazione e possono essere installati solo i componenti necessari; in secondo luogo perché, in base alla specifica esigenza, può essere installata sia in modalità ***on-premise*** (installazione locale) sia in modalità ***SaaS*** (servizio *cloud*), garantendo la tutela di lavoratori e aziende anche per quanto riguarda lo *smart working*.

4. Servizi specifici di Namirial offerti da Guardia Digitale

Credential Provider	Un'applicazione software che permette l'accesso alle postazioni di lavoro utilizzando l'autenticazione passwordless
Credential Management System	Uno strumento in grado di gestire l'intero ciclo di vita delle credenziali in maniera sicura
Login Assistant	Uno strumento che riduce i tempi di accesso a pagine web e app desktop senza necessità di integrazioni aggiuntive sugli applicativi ai quali si desidera accedere
Hylos	Una soluzione scalabile, che permette di tracciare centralmente i log, di creare archivi cifrati e conformi al GDPR e di sviluppare report degli eventi relativi a SafeAccess
Wazuh	Una soluzione *open source* per il rilevamento di minacce, il controllo dell'integrità, la risposta agli imprevisti e il rispetto degli standard

Grazie a questi servizi, SafeAccess permette alle aziende e alle organizzazioni di autenticare e autorizzare continuamente gli utenti interni ed esterni, di utilizzare il fattore di autenticazione più idoneo per il singolo utente, di controllare rigorosamente l'accesso alle risorse locali e basate su Cloud e di monitorare e verificare attivamente l'attività degli utenti, fornendo prova di conformità. Infine, ma certamente non per importanza, Namirial offre **assistenza e consulenza costante in tutte le fasi di progettazione e di realizzazione**.

Vuoi saperne di più?
Contattaci

(+39) 055 2001319

info@guardiadigitale.it

Piazza Madonna della Neve, 5
50122 FIRENZE (ITALIA)

www.guardiadigitale.it

GUARDIA DIGITALE