Image

CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

IL NIST CAMBIA LE REGOLE OBSOLETE DELLE PASSWORD

La maggior parte degli utenti online tende a utilizzare la stessa password per gli stessi account. La logica alla base di questa pratica è che è più facile da ricordarsi. Sorge però una domanda cruciale: questa comodità è sufficiente a salvaguardare le informazioni sensibili dei propri dati sensibili? Assolutamente no. Sebbene molte pratiche tradizionali relative alla sicurezza delle password possano sembrare intuitive, un numero significativo di esse deve essere più accurato, aggiornato e controproducente. È qui che entrano in gioco le linee guida NIST sulle password (National Institute of Standards and Technology), in particolare la pubblicazione speciale NIST 800-63B (agosto 2024). Anche l'Italia fa la propria parte. Andiamo verso una password più sicura.

di **Loris Taffi**
IUS/01 - DIRITTO PRIVATO
Articolo divulgativo - ISSN 2421-7123

Direttore responsabile
Alessio Giaquinto

Pubblicato, Lunedì 11 Novembre 2024

CamminoDiritto.it
ISSN 2421-7123

Abstract ENG

Online users use to adopt the same password for the same accounts. This practice is that it's easier to remember. However, a crucial question arises: is this convenience sufficient to safeguard sensitive information? Absolutely not. While many traditional password security practices may seem intuitive, a significant number of them need to be more accurate, updated, and counterproductive. This is where the NIST (National Institute of Standards and Technology) password guidelines come in, specifically NIST Special Publication 800-63B (August 2024). Italy reacts to international standards adopting the L.90/2024 concerning" Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici ". Let's move towards a more secure password.

Sommario: 1. Perché le ultime linee guida sono un tema caldo?; 2. Le regole d'oro; 3. L'informatica quantistica può essere una minaccia futura per la sicurezza alle password; 4. La riservatezza della password come diritto fondamentale dell'utente; 5. La sfida per gli Internet Service Provider; 6. Conclusioni

1. Perchè le ultime linee guida sono un tema caldo?

Le linee guida NIST sulle password proteggono le risorse informative e sono conformi ai requisiti degli standard di sicurezza. Rappresentano un insieme di migliori pratiche riconosciute a livello internazionale e approvate in tutto il mondo per migliorare la sicurezza informatica. Quando gli aggressori ottengono credenziali valide, possono accedere ai tuoi sistemi e aumentare i propri privilegi al livello di amministratore o utente, provocando una violazione della sicurezza. La violazione può avere gravi conseguenze, nel compromettere il livello di sicurezza dell'organizzazione, nel danneggiarne la reputazione con danni all'immagine e può minare la stabilità finanziaria dell'organizzazione. Per evitare ciò, le password fungono da prima linea di difesa contro le minacce informatiche. Le linee guida NIST aggiornate (SP-800-63-4) ora impongono che i fornitori di servizi cloud (CSP) e i verificatori applichino password con almeno 8 caratteri, consigliano di utilizzare password di 15 o più caratteri e suggeriscono di supportare passphrase fino a 64 caratteri per una maggiore sicurezza.

2. Le regole d'oro

2.1 Adoperare password manager

Il comportamento degli utenti gioca un ruolo significativo nella sicurezza delle password.

CamminoDiritto.it
ISSN 2421-7123

Questa pratica apre molteplici vulnerabilità, soprattutto quando la stessa password complessa viene utilizzata su varie piattaforme. Aumentare la sicurezza della password è più facile di quanto si pensi. Un modo efficace è utilizzare un gestore delle password che è uno strumento che crittografa facilmente le password, creandone di robuste. In questo caso, ridurre l'errore umano è fondamentale. I gestori di password elaborano automaticamente stringe complesse, risparmiandone la creazione manuale.

una raccomandazione intelligente per le aziende in merito alla scadenza e alla reimpostazione della password è, Invece di obbligare gli utenti a cambiare frequentemente la propria password, suggerire di farlo secondo due condizioni specifiche:

la reimpostazione della password dovrebbe avvenire quando l'utente ha prove evidenti di una compromissione nota; considerare la possibilità di reimpostare le password ogni 180 giorni, senza infastidire gli utenti. **2.2 La lunghezza della password e la complessità di costruzione**

Il NIST afferma che non l'utente non deve preoccuparsi incessantemente di includere lettere maiuscole, lettere minuscole o caratteri speciali (come!@#$%^) nelle password. Queste regole possono, paradossalmente, portare gli utenti a creare password più deboli. Invece di rendere più forti le password sicure, gli utenti spesso usano le stesse vecchie frasi e le modificano leggermente per i requisiti di ciascun sito web.

C'è una svolta sorprendente: non è sempre la complessità ma la lunghezza che conta davvero. Si potrebbe asserire che una password complessa, piena di simboli, numeri o lettere maiuscole, sia la strada da percorrere, ma anche la lunghezza dei caratteri che la compongono fa una grande differenza. Le password più lunghe sono difficili da violare. Insistere sulla complessità, come inserire caratteri speciali o lettere maiuscole, a volte può rivelarsi controproducente.

Ecco perché le linee guida NIST SP 800-63-3 richiedono un minimo di 8 caratteri per le password standard come parte del processo di gestione del rischio o di valutazione del rischio per la privacy. Ma non fraintenderci, usare caratteri speciali è comunque una buona idea, soprattutto quando si creano password casuali. La chiave è non dare regole rigide ed essere più flessibili nell'inclusione di caratteri speciali.

2.3 Scegliere l'opzione "mostra password durante la digitazione"

Fare errori di battitura durante l'immissione delle password è un comune errore. Quando i caratteri si trasformano istantaneamente in quei punti misteriosi, è facile andare in

CamminoDiritto.it
ISSN 2421-7123

confusione. Ciò può creare confusione e spingere l'utente a scegliere password più brevi e più semplici, soprattutto su siti web che limitano i tentativi di accesso e facilitano l'accesso non autorizzato. Essendo possibile, nei più comuni browser utilizzati, attivare e disattivare l'opzione per mostrare i consigli sulle password durante la digitazione dagli elenchi di password o dalle password rispetto agli elenchi, per l'utente sarà molto più sicuro digitare quelle password lunghe e complesse al primo tentativo.

2.4 Applicare il salt e l'hash alle password

Il NIST definisce l'hashing come un modo per trasformare una semplice password in un codice, una stringa di lunghezza fissa alfanumerica. Si immagini di trasformare "passAbc123" in qualcosa come "2db692bde1c8320eb7ae87bc64ac6c7f" per una archiviazione sicura. Quindi, invece di memorizzare le password effettive, vengono memorizzati queste impronte, note come hash delle password, con standard di sicurezza adeguati. Se gli hacker tentano di entrare, vedono solo questi codici e non le password reali. La nostra Agenzia per la Cybersicurezza Nazionale (ACN) in concerto con il NIST consigliano anche l'applicazione del salt che non è il sale da cucina, ma trattasi di una aggiunta di informazioni extra alle password prima di sottoporle ad hashing.

Questo elemento in più rende ancora più complicato per gli hacker decifrare il codice o eseguire attacchi a dizionario. Ad esempio: la precedente password, riportata qualche riga sopra come, assumerebbe il valore "9667b632c69db9eea2947acf9c8708167023ea7a". Tuttavia, anche la reimpostazione periodica della password, ad esempio ogni 60 o 90 giorni, è fondamentale per evitare la ridondanza delle chiavi di sicurezza. Alcuni malintenzionati preferiscono indovinare ripetutamente le password sicure finché non sono fortunati (attacco di forza bruta). E' possibile limitare il numero di tentativi effettuati nella ripetizione delle password prima che l'account si blocchi. Gli aggressori di solito hanno bisogno di molti più tentativi rispetto a chi commette errori di battitura occasionalmente. L'impostazione di un limite o l'aggiunta di un ritardo renderà le cose più difficili per l'aggressore. Ci vorrà così tanto tempo per risolverlo che non ne vale la pena.

2.5 Usare il sistema MFA (Multi-Factor Authentication)

L'MFA è anche nota come autenticazione a due fattori (2FA). Ecco come funziona: per accedere, l'utente deve dimostrare di conoscere due codici separati e distinti mostrati in due canali diversi. L'approccio metodologico dietro il sistema MFA consiste nelle seguenti idee:

esiste qualcosa che conosci, cioè la tua password; esiste qualcosa che hai, cioè il un telefono con installata la apposita app che genera il token (codice proprio di

CamminoDiritto.it
ISSN 2421-7123

autenticazione fornito dal provider del servizio); esiste qualcosa che possiedi, cioè l'impronta digitale che è la tua firma. L'utente, per autenticarsi e per autorizzare il funzionamento di un determinato servizio, dovrà adoperare la combinazione di dei tre fattori sopra descritti. Così, il sistema di log-in è protetto in maniera incorruttibile. (1)

3. L'informatica quantistica può essere una minaccia futura per la sicurezza alle password

Oggi siamo sicuramente dei pionieri nel campo della informatica quantistica. Essa, sicuramente, spalancherà le porte ad una tecnologia che ad oggi nemmeno ci immaginiamo. E' sicuramente fuori di dubbio che lo sviluppo di supercomputer quantistici porterà vantaggi significativi alla società. A differenza dei computer classici che si basano sui bit, i computer quantistici utilizzano i qubit per elaborare le informazioni. Ciò li rende molto più veloci e potenti dei computer classici. L'informatica quantistica rappresenta una minaccia potenziale per gli attuali metodi di creazione delle password, perché essa ha la potenza di calcolo per violare gli algoritmi di crittografia attualmente considerati sicuri. Ad esempio, un computer quantistico può essere utilizzato, da un malintenzionato, per eseguire un tipo di attacco per effettuare ricerche in un database composto da N elementi impiegando la radice quadrata di N tempo. Ciò significa che se si dispone di un database di 1 milione di password, un computer classico dovrebbe provare tutte le password possibili, ma un computer quantistico potrebbe trovare la password corretta in soli 1000 tentativi. (2)

4. La riservatezza della password come diritto fondamentale dell'utente

La privacy dei dati è un diritto umano fondamentale nell'UE. Il GDPR impone rigide restrizioni sui dati personali, vietandone la condivisione con paesi che non hanno un livello di protezione equivalente (una disposizione in vigore dalla Direttiva sulla protezione dei dati del 1995, predecessore del GDPR).

Sebbene la trasparenza sia fondamentale, è doveroso ricordare il valore dei singoli dati. In un sistema inondato di informazioni, il modo in cui i dati vengono condivisi diventa vitale. I protocolli che garantiscono la protezione dei dati, come la crittografia, non sono negoziabili. Il nostro Regolamento UE 2016/679 (noto come GDPR) esemplifica questo impegno, segnalando l'importanza globale della protezione dei dati e impone al Titolare del trattamento, così come al Responsabile del trattamento, (art.4 GDPR) misure tecniche ed organizzative tali da garantire un corretto trattamento del dato durante tutto il ciclo di vita. Dal GDPR è possibile estrarre rigidi divieti circa la condivisione delle password, perché ciò comporterebbe adoperare un livello di protezione inidoneo a quello imposto nell'Unione Europea. (3)

CamminoDiritto.it
ISSN 2421-7123

L'aumento esponenziale delle leggi sulla protezione dei dati in tutto il mondo nell'ultimo decennio riflette il desiderio di garantire che i dati siano conservati in modo sicuro, trattati in modo trasparente e che gli individui siano in grado di esercitare i propri diritti in relazione ai dati stessi. Sebbene queste leggi concordino fondamentalmente sui principi chiave della privacy dei dati, le normative e gli obblighi specifici variano in modo significativo tra le diverse giurisdizioni. Questa disparità è particolarmente evidente in aspetti, come le basi giuridiche per il trattamento e il trasferimento dei dati personali a livello internazionale e nelle scadenze previste per informare le autorità e i singoli individui in merito alle violazioni dei dati.

Il nostro Paese è molto attento al tema della sicurezza informatica. A giugno 2024, è stata varata la {https/URL}Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" (4). La nuova legge rafforza il perimetro della sicurezza cibernetica e contrasta i reati informatici attraverso una serie di misure innovative, con l'obiettivo di rendere il Paese più resiliente. E' possibile notare questi parallelismi:

tra la {https/URL}(5): si ricorda che la Direttiva 2022/2555, in vigore dal 17/10/2024, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (Direttiva NIS 2), prevede la presentazione da parte dei soggetti essenziali e importanti di un preallarme entro 24 ore dalla conoscenza di un incidente significativo e di una notifica entro 72 ore dalla conoscenza di un incidente significativo. I medesimi termini sono previsti dallo schema adottato dall'Italia. tra la {https/URL}(6): il Regolamento UE 2022/2554, in vigore dal 17/01/2025, mira a garantire che le entità finanziarie dell'UE possano resistere agli attacchi informatici e possano rimanere operative con attacchi in corso. L'obiettivo primario è mantenere la disponibilità e l'integrità dei servizi finanziari, con una particolare attenzione per la resilienza operativa. La legge nazionale in vigore dall'estate, infatti, inasprisce le pene per reati come l'accesso abusivo e il danneggiamento di sistemi informatici, potenzia le funzioni dell'Agenzia per la cybersicurezza nazionale (ivi inclusa la creazione di un Centro nazionale di crittografia) e affronta anche la resilienza operativa digitale nel settore finanziario, estendendo l'uso di strumenti investigativi speciali per reati informatici gravi e migliorando il coordinamento tra autorità in caso di attacchi. È chiaro, dunque, come questa nuova legge richieda degli sforzi di adeguamento maggiori a tutti gli attori coinvolti, in risposta all'esigenza impellente di rafforzare la sicurezza informatica e garantire, così, un equilibrio e una stabilità a multilivello che, attualmente, sono messi in discussione frequentemente.

5. La sfida per gli Internet Service Provider

Un Internet Service Provider (fornitore di servizi Internet), abbreviato con la sigla ISP,

CamminoDiritto.it
ISSN 2421-7123

nelle telecomunicazioni, indica un'organizzazione o un'infrastruttura che offre agli utenti (residenziali o imprese), dietro la stipulazione di un contratto (a titolo oneroso o gratuito), servizi Internet, i principali dei quali sono: accesso al World Wide Web, piattaforme di broadcasting e posta elettronica. Gli ISP dovranno essere consapevoli dell'incremento del rischio che una azione indiscriminata, attuata con mezzi tecnologici sempre più sofisticati, potrà esfiltrare ed elaborare dati sensibili in maniera molto più potente. La supply chain cammina su un filo delicato: la chiave per armonizzare con successo i requisiti di robustezza delle password risiede nell'applicare il giusto tipo di strategie in modo conforme ed efficiente. I costi per la nuova conformità potranno aumentare e potranno esserci impatti sull'utente finale, ma l'atto di bilanciamento richiede un approccio innovativo, consentendo alle aziende di condurre controlli approfonditi ed efficaci senza compromettere gli standard di protezione dei dati.

6. Conclusioni

L'elaborato "Linee guida NIST SP 800-63-3" rappresenta una componente importante delle linee guida sull'identità digitale del NIST, aggiornate ad agosto 2024. Queste linee guida, pur non essendo obbligatorie a livello planetario, sono obbligatorie per le agenzie federali statunitensi, gli enti e le imprese operanti negli USA e per le organizzazioni, le imprese e gli Enti esteri che interagiscono online con il governo federale degli Stati Uniti. Le best practices internazionali, le leggi e i regolamenti anche italiani non si limitano a enfatizzare la forza delle password, ma considerano anche il comportamento degli utenti, consigliando al tempo stesso un metodo di rafforzamento sicuro. È qui che entra in gioco la compliance aziendale, come spirito per semplificare il processo e per aiutare l'azienda a mantiene una postura IT solida.

CamminoDiritto.it
ISSN 2421-7123

Note e riferimenti bibliografici

Note e riferimenti bibliografici:

1NIST SP 800-63 Digital Identity Guidelines {https/URL}

2{https/URL}

3{https/URL}

4{https/URL}

5{https/URL}

6{https/URL}

* Il simbolo {https/URL} sostituisce i link visualizzabili sulla pagina: https://rivista.camminodiritto.it/articolo.asp?id=10774