Politica sulle password per PMI

La sicurezza dei sistemi e delle reti informatiche dipende in modo essenziale da una gestione corretta delle password. Definendo e attuando una «password policy», ossia dei criteri ben precisi per la gestione delle password, si stabilisce come creare, conservare e utilizzare le password all'interno dell'azienda.

Punti principali:

- Create uno schema generale di tutti gli accessi a sistemi e applicazioni dotati di protezione tramite password nella vostra impresa.
- Per tutti gli accessi a sistemi e applicazioni identificati, stabilite in una PW-Policy i requisiti da rispettare per la creazione, la conservazione e l'utilizzo delle password.
- Verificate periodicamente che la PW-Policy venga rispettata scrupolosamente.
- Sensibilizzate il vostro personale verso i pericoli posti da una gestione scorretta delle password.

Perché serve una PW-Policy?

La combinazione di nome utente e password è ancora il metodo più utilizzato per l'autenticazione e l'autorizzazione negli ambienti di lavoro digitale. È un sistema che permette, ad esempio quando si accede a una rete o a un sistema informatico o si utilizzano servizi e applicazioni, di determinare l'identità degli utenti e proteggere gli accessi. I nomi utente e le password rivestono quindi un ruolo centrale per la cibersicurezza.

Non sorprende quindi che i criminali informatici si impegnino con ogni mezzo per ottenere queste preziose informazioni tramite hacking, phishing o social engineering, allo scopo di usurpare l'identità digitale della persona in questione.

Tuttavia, l'uso delle password è ormai un'attività così comune che spesso gli utenti sono troppo poco consapevoli dei pericoli che comporta. Proprio in ambito aziendale è quindi indispensabile avere una politica sulle password chiara, che offra agli utenti istruzioni precise per prevenire errori in questo ambito.

Che cos'è una PW-Policy e come crearne una efficace?

Per «password policy» si intende un insieme di regole che mirano ad aumentare la sicurezza informatica incoraggiando il personale a creare password sicure, a conservarle con cura e a utilizzarle correttamente. La PW-Policy si inserisce tra le regole ufficiali applicate in un'organizzazione e dovrebbe essere trattata nella formazione sulla consapevolezza della sicurezza (programma di sensibilizzazione).

La PW-Policy deve essere allineata alle esigenze specifiche (il sistema nel suo complesso) e ai requisiti (livello di sicurezza) dell'organizzazione, al fine di ottenere un effetto ottimale con un impegno commisurato. In una prima fase è perciò necessario stilare uno schema generale di tutti gli accessi a sistemi e applicazioni dotati di protezione password nell'impresa, nonché stimare il livello di protezione richiesto. Tutti gli accessi così identificati saranno poi presi in considerazione nella politica sulle password, con le regole pertinenti.

Per far fronte all'evoluzione continua delle minacce, occorre verificare periodicamente l'aggiornamento e l'efficacia della PW-Policy.

Quali sono i punti più importanti della PW-Policy?

La PW-Policy disciplina ogni aspetto della gestione delle password in azienda. Fornisce agli utenti istruzioni operative concrete e indicazioni sui seguenti punti:

1. Utilizzo di password

Come accennato sopra, spesso è sufficiente conoscere una password per assumere interamente l'identità digitale di una persona. In generale, quindi, vanno prese tutte le precauzioni per impedire l'abuso di questa informazione chiave.

Le password sono strettamente personali e vanno mantenute segrete. In particolare occorre prestare attenzione ai punti seguenti:

1. Le password non devono essere trasmesse o condivise attivamente, né archiviate in posizioni aperte e accessibili.
2. La memorizzazione e la trasmissione delle password devono avvenire sempre in modo crittografato.
3. Quando si immette una password, è necessario assicurarsi che la digitazione non sia visibile a terzi.

La PW-Policy stabilisce le linee guida per l'utilizzo delle password ponendosi come direttiva da rispettare.

2. Robustezza delle password

La robustezza della password indica con quanta difficoltà un utente malintenzionato potrebbe individuare una password che non conosce semplicemente indovinandola o procedendo per tentativi. Più una password è imprevedibile, complessa e lunga, più è robusta e quindi sicura.

Una politica valida sulle password sottolinea l'importanza di creare password robuste, incoraggiando gli utenti a rendere le loro password più lunghe e imprevedibili. (Istruzioni «Password sicure» (https://www.ebas.ch/it/4-proteggere-gli-accessi-online/#passwords))

Inoltre, la creazione di password sicure dovrebbe essere supportata da strumenti tecnici, come la messa a disposizione di un gestore di password (https://www.ebas.ch/it/4-proteggere-gli-accessi-online/#passwords) , e regolamentata nella password policy.

3. Ciclo di vita delle password

Le password possono essere trasferite facilmente, e con il tempo potrebbero anche finire nelle mani sbagliate. Potrebbe ad esempio accadere che, agendo con superficialità, un collaboratore comunichi la sua password a terzi, o che la annoti in un luogo non protetto. Oppure potrebbe verificarsi un'avaria nel sistema dati, con l'involontaria pubblicazione delle password degli utenti. In linea di massima non si possono richiamare indietro le informazioni, dopo che sono trapelate.

In questi casi, cambiare le password è l'unico modo efficace per ripristinare la cibersicurezza, poiché rende inutilizzabili le informazioni che sono fuoriuscite dall'organizzazione.

Il rinnovo e la gestione delle password dovrebbero essere attività supportate da strumenti tecnici, come la messa a disposizione di un gestore di password, e regolamentate nella PW-Policy.

4. Cronologia delle password

Gli utenti hanno la tendenza a ridurre il numero di password da ricordare, p. es. riutilizzando password che hanno già utilizzato in precedenza. I criminali informatici sanno trarre vantaggio da questa abitudine, e nei loro attacchi

utilizzano regolarmente anche liste di vecchie password. Per evitare che questa pratica si riveli fruttuosa, agli utenti dovrebbe essere impedito di riattivare le vecchie password.

La password policy assicura che i sistemi conservino una cronologia delle password degli utenti ed eseguano un controllo su un loro eventuale riutilizzo in concomitanza con la modifica della password corrente.

5. Modifica delle password

Gli utenti dovrebbero avere la possibilità di modificare le loro password in qualsiasi momento e in piena autonomia. Tuttavia, è necessario garantire che le password possano essere cambiate esclusivamente dal proprietario autorizzato e non da un hacker.

La PW-Policy stabilisce le condizioni quadro tecniche e organizzative che consentono una modifica sicura della password. Ad esempio, l'introduzione dell'autenticazione a due fattori può accrescere di molto la sicurezza del processo di modifica della password.

Le password sono da sempre gli elementi di sicurezza più utilizzati per proteggere gli accessi nel mondo digitale. Non sorprende quindi che i criminali informatici si impegnino con ogni mezzo per carpirle tramite hacking, phishing o social engineering.

Una politica sulle password (PW-Policy) garantisce chiarezza e sicurezza nella gestione delle password.