PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 27 - numero 5958 di Giovedì 06 novembre 2025

Furto al Louvre: gravi lacune della sicurezza

Gli investigatori stanno indagando sulle modalità di perpetrazione del furto dei gioielli al museo del Louvre e stanno scoprendo delle gravi lacune nella organizzazione della sicurezza, di cui è bene che i nostri lettori prendano buona nota.

Numerosi mezzi di comunicazione di massa, sia stampati, sia radiofonici e televisivi, hanno dato notizia del fatto che le indagini, susseguenti al furto e che hanno mirato a ricostruire lo scenario di attacco, hanno messo in evidenza delle clamorose lacune nella struttura di sicurezza di uno dei più importanti musei del mondo.

Di particolare rilevanza il fatto che le strutture museali, almeno sotto gli aspetti informatici, vengano ispezionate periodicamente dalla agenzia nazionale per la sicurezza informatica (ANSSI), che dà raccomandazioni e consigli su come migliorare la struttura di sicurezza informatica.

Durante l'ispezione effettuata nel 2014, gli esperti dell'agenzia nazionale, su richiesta dello stesso museo, avevano effettuato un controllo, rilevando che la parola chiave per accedere al servizio della videosorveglianza era " Louvre".

Non basta!

Pubblicità

La parola chiave per accedere ad un software di sicurezza di gestione di sensori di allarme, sviluppato da una grande società francese informatica, la Thales, era "Thales"!

Il fatto che spesso le parole chiave vengano scelte con scarsa diligenza è purtroppo fatto noto, che ogni esperto di sicurezza informatica conosce perfettamente e dovrebbe poter mettere sotto controllo con l'emissione di specifiche istruzioni per i soggetti coinvolti e con l'effettuazione di periodici controlli.

Nella fattispecie, stupisce il fatto che l'ispezione, effettuata 2014, aveva già messo in evidenza una debolezza, per non dire una banalità, nella scelta delle parole chiave, ma la raccomandazione migliorativa era stata evidentemente ignorata da tutti, sia dagli operatori coinvolti, sia da coloro che avrebbero dovuto sorvegliare il loro comportamento.

Ancora una volta, raccomandiamo a tutti i responsabili della sicurezza informatica di tenere questo fenomeno, potenzialmente assai grave, con i seguenti interventi:

- dare precise istruzioni al personale sulle modalità di scelta delle parole chiave,
- mettere a disposizione del personale degli applicativi, liberamente disponibile su Web, che permettono a chiunque di verificare la robustezza della parola chiave prescelta,
- imporre la periodica sostituzione della parola chiave, ad esempio ogni tre mesi,
- attivare un applicativo di controllo della storia delle parole chiave, per evitare che l'operatore possa cambiare un solo numero della nuova parola chiave, riducendo in modo drammatico la validità dell'operazione di sostituzione,
- effettuare periodici controlli, senza preavviso, chiedendo all'operatore di digitare, in propria presenza, la parola chiave prescelta, per verificare la validità,
- successivamente, si chiederà l'operatore di cambiare la parola chiave digitata e visualizzata dal controllore.

Infine, mi permetto di rammentare un suggerimento, che ho imparato frequentando l'unione delle banche svizzere- UBS. Il loro responsabile della sicurezza informatica proibisce l'attivazione di applicativi di cambio della parola chiave il venerdì!

A fronte della mia curiosità per conoscere la ragione di questa prescrizione, mi ha riferito che se la parola chiave viene cambiata di venerdì, molto spesso non viene ricordata, il lunedì mattina, perché per due giorni essa non viene digitata. L'esperienza statistica di questa grande Banca mondiale mette in evidenza come effettivamente la introduzione di questa regola ha permesso di diminuire in modo drammatico le richieste di assistenza per la sostituzione della parola chiave dimenticata, che giungevano al servizio centrale di controllo il lunedì mattina!

Come al solito, esperienza, nel bene e nel male, non ha prezzo.

Adalberto Biasiotti

Licenza Creative Commons

www.puntosicuro.it