PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 25 - numero 5422 di Venerdì 30 giugno 2023

Come proteggere le videoregistrazioni?

Sempre più spesso, nei contenziosi civili e penali, le videoregistrazioni vengono utilizzate come strumento probatorio. Ecco la ragione per la quale è importante che il gestore di un sistema di videosorveglianza possa garantire un'elevata affidabilità.

La sicurezza informatica delle videoregistrazioni rappresenta un aspetto fondamentale per proteggere le attività aziendali, i dipendenti ed i soggetti terzi. Ecco perché i responsabili informatici devono impostare un programma affidabile di archiviazione e protezione delle videoregistrazioni, in modo che, in caso di necessità, l'ormai famoso acronimo CIA. Confidentiality, Integrity and Availability venga rispettato.

L'utilizzo del cloud

Non v'è dubbio che l'utilizzo del cloud, magari in parallelo con sistemi locali di video registrazione, metta a disposizione uno strumento sicuro di archiviazione, che è ben più difficilmente attaccabile, rispetto ad un personal computer, installato nella portineria di un edificio. Occorre però accertarsi che il sistema cloud che viene utilizzato dia sufficienti garanzie di affidabilità, ad esempio perché certificato secondo una ormai assai popolare norma ISO.

La protezione criptografica delle immagini

La criptografia è un processo che permette di modificare i dati, in modo che non siano leggibili da chi non dispone della chiave di decodifica. In questo modo anche un eventuale sottrazione dei dati non permetterebbe al malvivente di osservare le immagini registrate. È bene comunque sapere che esistono vari algoritmi criptografici, il più semplice dei quali utilizza la stessa chiave sia per cifrare le immagini, sia per decifrarle. Sistemi criptografici più sofisticati sono raccomandati per immagini che richiedono un elevato livello di protezione.

Tre archiviazioni separati sono meglio di una!

Quando le immagini vengono archiviate anche sul cloud, è frequente il fatto che siano disponibili due video archiviazioni, rispettivamente nel cloud e presso la postazione di ripresa. La soluzione più soddisfacente è quella ridondante, in base alla quale viene effettuata una terza copia, che può essere custodita in un ambiente protetto, che non possa essere coinvolto in eventuali situazioni di crisi, che potrebbero coinvolgere le altre registrazioni.

L'autentica a due fattori

Tutti gli autorizzati al trattamento, che possono accedere alle immagini videoregistrate, devono essere dotati, come è normale, di un profilo di accesso e di una parola chiave univoca. L'utilizzo di sistemi di accesso a due fattori aumenta in maniera drammatica il livello di sicurezza dell'accesso, perché viene introdotto un ulteriore fattore, che si aggiunge alla parola chiave.

Attenti alle connessioni via Internet

Come regola generale, bisognerebbe rifuggire dall'uso di telecamere collegate direttamente via Internet, le cui immagini vengono successivamente registrate. Una soluzione particolarmente brillante, che viene già utilizzata da parecchie grandi aziende, consiste nel concentrare tutte le immagini, provenienti da un sito, in un appropriato server, laddove le immagini aggregate vengono cifrate e successivamente trasmesse nel cloud o alla stazione di comando e controllo.

Infine, è bene tenere gli occhi sempre aperti

È ormai noto che le abilità dei malviventi informatici crescono rapidamente e purtroppo spesso più rapidamente di quanto non crescano le attenzioni degli specialisti di sicurezza informatica alla individuazione e mitigazione delle minacce. Il fatto di tenersi costantemente aggiornate sui rischi afferenti alla intercettazione di dati, attacchi a sistemi di video registrazione ed immagini archiviate rappresenta sicuramente un atteggiamento proattivo, che potrà aiutare i responsabili della sicurezza informatica a bloccare tempestivamente anche le nuove modalità di attacco, che i malviventi possano aver messo a punto.

Adalberto Biasiotti

---

www.puntosicuro.it