Database di Stato violati, informazioni protette su più livelli di controllo

Agenzia cyber. Le nuove linee guida rafforzano la sicurezza su politici e imprenditori: verifica su utenze interne, ricerche eseguite e fornitori esterni

Ivan Cimmarusti

Di certo c'è che nell'esfiltrazione di dati riservati dalle più importanti banche dati dello Stato, come il Ced Interforze del ministero dell'Interno o il Siva che raccoglie le segnalazioni antiriciclaggio (le cosiddette Sos), cruciale sarebbe stato il «fattore umano». Così lo hanno definito al Viminale, dopo che l'indagine della Procura di Milano sulla società Equalize di Enrico Pazzali ha fatto luce sul ruolo di "talpe" interne alle istituzioni che trafugavano informazioni segrete su persone e imprese. Un po' come faceva Pasquale Striano, il luogotenente della Guardia di finanza, distaccato all'ufficio Sos della Direzione nazionale antimafia, che «rubava» segnalazioni finanziarie su politici o imprenditori per consegnarle, su richiesta, a giornalisti. Cruciale il caso del ministro della Difesa Guido Crosetto che, secondo i magistrati di Perugia coordinati dal procuratore Raffaele Cantone, sarebbe stato uno dei «bersagli» principali del dossieraggio.

Funzionari infedeli

Ricostruzioni investigative che hanno innescato una profonda riflessione sulle banche dati e sulle modalità con cui sono gestite. La stessa Agenzia per la cybersicurezza nazionale (Acn), organismo d'intelligence che fa capo a Palazzo Chigi ed è diretto dal prefetto Bruno Frattasi, ha preso atto, tra le altre, di una «criticità» fondamentale: la gran parte delle azioni è stata perpetrata dalla possibilità di accesso alle informazioni grazie ai permessi assegnati a funzionari della Pa che poi si sono scoperti essere «infedeli». Personaggi che avrebbero fatto un doppio gioco per scopi da chiarire e che — nel delicato caso sotto esame alla Procura di Roma — potrebbero aver ceduto informazioni riservate a soggetti esteri interessati a speculazioni finanziarie in Italia.

> **Notizie segrete sottratte e veicolate a terzi soggetti. Rischio di speculazioni finanziarie in Italia**

Nei giorni scorsi l'Acn ha varato un documento di 19 pagine con cui sono state diffuse le nuove linee guida «per il rafforzamento della protezione delle banche dati rispetto al rischio di utilizzo improprio». Si è capito che l'eccessiva ampiezza dei permessi consentiti a utenti abilitati ha innescato un fenomeno degenerato nella compravendita di informazioni riservate. Materiale utile a colpire un nemico politico o imprenditoriale e che, inevitabilmente, rischia di manipolare l'andamento del mercato.

Controllo «robusto»

Si è deciso che strutturare un controllo coerente e robusto rappresenta «la base per garantire che» l'accesso alle banche dati «sia ristretto al personale e alle utenze autorizzati». A questo scopo le identità digitali del personale devono essere nominative e individuali, non condivise tra più persone, anche per poter tracciare gli accessi e risalire in modo inequivocabile al personale interno ed esterno che li fa.

Verifica utenze

Le utenze, i relativi privilegi e le credenziali devono essere verificati, aggiornati, revocati e sottoposti ad audit periodicamente, secondo una cadenza temporale coerente con l'analisi dei rischi.

Occorre implementare un modello di gestione degli accessi centralizzato. Tutti, anche quelli da remoto, devono essere registrati e monitorati. La sicurezza dei sistemi e delle applicazioni deve essere garantita sin dalla progettazione e per impostazione predefinita.

Dovranno quindi essere definiti criteri per rilevare casi di utilizzo improprio delle banche dati da parte del personale, come ad esempio la consultazione di profili sensibili o comunque rilevanti ai fini della tutela della sicurezza nazionale, quali ad esempio dati di personalità politicamente esposte; il superamento di una soglia per le interrogazioni da parte di un singolo utente; la variazione sensibile del numero medio di ricerche effettuate da un utente calcolato su un arco temporale definito; ricerche effettuate da personale che non ricopre posizioni di impiego tali da necessitare determinate informazioni».

Particolare attenzione alla catena di approvvigionamento. Secondo l'Agenzia «i fornitori e le terze parti, specie se poco maturi dal punto di vista della cybersicurezza, possono rappresentare un punto di vulnerabilità». I fornitori, infatti, «possono rappresentare un vettore di attacco qualora compromessi da soggetti malintenzionati».

Le regole «anti-talpa»

Gli interventi compiuti dall'Agenzia per la cybersicurezza nazionale

CONTROLLO ACCESSI

Un controllo efficace degli accessi rappresenta il primo livello di difesa per prevenire utilizzi impropri.

Autenticazione. Obbligatoria per tutti gli accessi ai sistemi e alle banche dati, con meccanismi calibrati in base alla criticità dei dati gestiti.

Gestione centrale. Utilizzo di piattaforme per monitorare e verificare continuamente gli accessi, revocando le credenziali obsolete.

Tracciamento accessi. Ogni operazione deve essere registrata in log sicuri, archiviati per almeno 24 mesi

SVILUPPO SISTEMI

Il ciclo di sviluppo deve essere orientato alla sicurezza sin dalla progettazione.

Separazione ambienti. I sistemi devono operare in ambienti distinti per sviluppo, test e produzione, limitando l'accesso ai dati reali.

Superficie d'attacco. Eliminazione di componenti non necessarie (software, servizi) e integrazione di sistemi di monitoraggio e allarme già in fase di progettazione.

Identità. Introduzione di password complesse per proteggere accessi automatizzati.

CICLO DEI SISTEMI

La sicurezza dei sistemi e delle applicazioni deve essere garantita in tutte le fasi del loro ciclo di vita, dalla progettazione alla dismissione.

Manutenzione. Ogni intervento, sia locale che remoto, deve essere registrato e tracciato.

Aggiornamenti. Prima di implementare patch o aggiornamenti critici, questi devono essere testati in ambienti dedicati

Dismissione. Cancellazione dei dati e delle chiavi di crittografia dai dispositivi di memorizzazione obsoleti, con smaltimento conforme.

FORNITORI

I fornitori e le terze parti rappresentano un punto di vulnerabilità significativo.

Classificazione dei fornitori. Inventario aggiornato e classificazione dei fornitori in base ai rischi cyber associati alle loro attività.

Contratti. Ogni accordo deve includere clausole che definiscano chiaramente gli standard di sicurezza richiesti.

Diversificazione dei fornitori. Garantire che la compromissione di un fornitore non comporti la perdita completa della capacità operativa, prevedendo alternative per servizi critici.