

Al primo posto l'organizzazione

Integrazione, autenticazione e cultura interna ed esterna

Akhela - All in one

La chiave dell'integrazione è il primo punto da affrontare per aprire il confronto con Andrea Gaspari, Direttore Marketing di Akhela, società del Gruppo Saras specializzato in tali servizi:

"Il concetto di sicurezza nell'ambito del settore pubblico sta acquisendo sempre maggiore importanza e assumendo nuove valenze.

Ciò che diviene rilevante per gli enti pubblici è acquisire una visione che porti a evolvere dalla gestione della sicurezza perimetrale alla gestione integrata.

Per affrontare in modo integrato questo problema, Akhela mette a disposizione del settore pubblico tutti i servizi e i prodotti necessari a gestire la sicurezza informatica in un'ottica "All in One".

Operiamo partendo dalla consapevolezza che la sicurezza non è un prodotto, ma un processo continuo all'interno dell'organizzazione integrato con gli altri processi: identificato un perimetro, esiste un punto d'inizio, ma non un punto di fine, solo livelli successivi di "stato".

Akhela mette al servizio dei clienti pubblici e privati le proprie conoscenze nel mercato mondiale della sicurezza e per ogni step del processo di securizzazione si avvale di tecnologie ormai consolidate sul mercato, di strumenti innovativi e, dove necessario, creati ad hoc dai propri sviluppatori per le esigenze specifiche. Il processo di securizzazione parte da una fase di valutazione delle effettive condizioni di sicurezza dell'organizzazione e dei rischi cui essa è sottoposta, con un'analisi delle vulnerabilità e test di penetrazione nei sistemi informativi che consentano di individuare gli interventi necessari. In questa fase, ricorriamo ai cosiddetti "ethical hackers", persone abili a trovare e valutare le vulnerabilità dei sistemi aziendali, utilizzando le stesse metodologie impiegate da chi compie gli attacchi. Nella fase di assessment e analisi dei rischi, Akhela fa ricorso a soluzioni in grado di incrociare le informazioni sugli

asset dell'organizzazione e le potenziali vulnerabilità presenti sui sistemi, dando così un valore economico al rischio e consentendo di simulare diversi scenari con tecniche "what if".

L'elemento distintivo è la gestione del livello applicativo, al di là di quello fisico/infrastrutturale, che permette di avere un quadro completo del livello di sicurezza di tutto il sistema. Passando alla determinazione della policy e delle architetture di sicurezza, con la contestuale definizione di un disaster recovery plan, si entra nella fase implementativa, con la definizione di un contratto di Service Level Agreement (SLA) fra Akhela e l'ente. In realtà, è importante sottolineare che sul tema della sicurezza la relazione fra cliente e partner tecnologico deve muoversi su un piano di fiducia e fattiva collaborazione che travalichi gli aspetti meramente contrattuali. Occorre simulare scenari architetture diversi, con valutazioni di fattibilità ed impatto. Per garantire maggiore efficienza, Akhela automatizza le operazioni di hardening sui sistemi, considerandone l'allineamento ai modelli di riferimento. Sul piano tecnologico, le soluzioni più comunemente implementate per aumentare la sicurezza dell'organizzazione sono i sistemi di firewalling, in grado di verificare traffici anomali anche in presenza di connessioni criptate, i sistemi di "cassaforte virtuale" a protezione del dato (criptatura, accesso condizionato) e i sistemi a protezione delle postazioni client (antivirus, spam, spyware, etc.).

La fase manutentiva prevede la regolare effettuazione di test di penetrazione, volti a valutare che il livello di sicurezza stabilito sia costantemente mantenuto e che non siano sorte nel frattempo nuove vulnerabilità, individuando, nel caso, le soluzioni atte a neutralizzare le nuove falle.

In questa fase ci avvaliamo di sistemi automatizzati e autoaggiornanti, in grado di analizzare il livello di vulnerabilità dei sistemi su base periodica e fornire l'opportuna reportistica agli operatori, nonché di strumenti in grado di allertare questi ultimi in caso di attacchi alla sicurezza (Ids).

Akhela ricorre inoltre ai tool di gestione della Incident Analysis, per ricostruire gli attacchi avvenuti e neutralizzarne gli effetti.

Auditing e monitoraggio portano a chiudere il cerchio, riconducendo tutto alla fase di valutazione e analisi dei rischi, all'origine del processo.

Va sottolineato, comunque, che affrontare correttamente il discorso sicurezza in un ente pubblico come in un'azienda privata significa essere consapevoli che non sarà possibile raggiungere in nessun caso una sicurezza al 100%. Inoltre l'organizzazione dovrà essere cosciente del fatto che Akhela, in qualità di partner tecnologico, potrà supportarla nella gestione del processo di securizzazione e sul piano delle soluzioni It, ma non potrà sostituirsi ad essa nella fondamentale attività di sensibilizzazione delle risorse umane sui temi della sicurezza. L'ente ha infatti il dovere di agire sulla cultura interna affinché l'attenzione alla sicurezza permei l'organizzazione a tutti i livelli. Non a caso in molte circostanze viene messo in evidenza come il vero potenziale pericolo di organizzazione è l'utente interno. Secondo alcune stime, è principalmente all'interno che vengono causati i danni: il 55% del numero di attacchi si sviluppa all'interno dei sistemi informativi, ma il dato più impressionante è che il 90% del danno procurato è portato da attacchi interni. Se il punto di vulnerabilità rimane la persona umana, difficilmente si potrà intervenire sul piano tecnologico, ma bisognerà agire su quello della cultura organizzativa e della formazione. Anche su questo piano, comunque, Akhela offre la propria competenza, evidenziando le debolezze a livello di risorse umane con l'ausilio di opportune tecniche di social engineering".