

Autenticazione, verso l'ascesa

Secondo gli ultimi dati pubblicati da Forrester le aziende si stanno interessando alle più evolute tecniche di autenticazione di impiegati e clienti

La security aziendale, un argomento tanto strategico quanto complesso che nel corso degli ultimi anni ha animato, e non poco, i dibattiti dei salotti buoni del mondo IT. Tanto per capirne la portata basta fare una breve e superficiale ricerca sul Web, in pochi minuti il vostro desktop traboccherà di prontuari, consigli, indicazioni più o meno perentorie sul cosa fare, in termini di prodotti, policy e configurazioni e sul cosa non fare, sui prodotti da scegliere o non scegliere nel mezzo di un'offerta sempre più ampia e complicata... Orientarsi, insomma, è assai complicato soprattutto per aziende come quelle italiane non proprio ben predisposte verso l'innovazione tecnologica. La posta in palio però è assai alta dato che i dati critici e le infrastrutture da proteggere sono sempre di più, pena: pesanti e spesso irreparabili danni per il business e i processi aziendali...

recentemente la voce autorevole di Forrester Research, storico analista di mercato che ha chiamato in causa circa 200 manager di altrettante aziende interrogandoli, manco a dirlo, sullo stato delle loro policy di sicurezza nel 2005. I risultati, se da una parte confermano una situazione di sostanziale eterogeneità in tema di strategia di approccio alla sicurezza, specie in fatto di autenticazione degli utenti nelle varie reti aziendali, dall'altra cominciano a evidenziare qualche importante segno di apertura nei confronti di tecnologie innovative e promettenti come i progetti di Enterprise single sign-on, ovvero soluzioni che consentono di ridurre i costi legati all'help desk e offrire praticità agli utenti, permettendo loro di effettuare il sign-on una sola volta per accedere a tutte le risorse online.

Password protagonista

Sui 147 manager che hanno risposto alle domande degli uomini di Forrester, circa l'84 per cento è convinto che una buona strategia di autenticazione basata su password sia sufficiente per proteggere e rendere sicuri gli accessi degli impiegati alla rete. Le password, dunque, continuano a dominare lo scenario dell'autenticazione dato che

nicchie di aziende che si dicono sempre più pronte, o che addirittura stanno già sperimentando, più evolute tecniche di autenticazione come quelle basate sulle one-time password, Otp, ovvero sulle password monouso, sui certificati digitali o ancora meglio sulla biometria come nel caso del riconoscimento delle impronte digitali, dell'iride... Nello specifico, infatti, corrisponde a circa un terzo degli intervistati il gruppo di coloro che utilizzeranno entro il 2005 i cosiddetti on-time tokens, soluzioni basate sulle password monouso come nel caso del SecurID di Rsa Security o dello Unified Authentication Token di VeriSign. Due soluzioni che offrono avanzata sicurezza sia quando l'utente è online e connesso alla rete, sia quando è off-line, sostituendo le password con un passcode one-time che cambia in continuazione. In questo modo, dunque, le organizzazioni possono eliminare la necessità di implementare policy per il cambiamento delle password, riducendo gli errori da parte degli utenti e il numero di chiamate all'help desk. Tuttavia, per una più forte politica di autenticazione dei clienti B2C e B2B a più alto valore, sempre più aziende, ha spiegato ancora Forrester, sceglieranno di puntare sui certificati

Network & Security

A fare il punto della situazione su un così delicato tema ci ha pensato



solo l'8 per cento delle aziende chiamate in causa smetterà di imporre politiche di password in fatto di autenticazione degli impiegati nel corso di quest'anno e solo il 6 per cento di queste continuerà a permettere ai propri clienti di effettuare transazioni online senza il beneficio di regole disegnate per produrre password ancora più rigide.

Nello specifico, comunque, l'utilizzo delle password sembra essere più apprezzato nel caso delle autenticazioni di personale interno, è come anticipato il caso dell'84 per cento del campione analizzato, mentre nel caso delle autenticazioni di clienti che intendono transare online, buone politiche basate su password vengono utilizzate dal 67 per cento dei manager interpellati.

Interessanti sviluppi

Si è detto, dunque, delle politiche di autenticazione basate sull'uso di password "tradizionali" e del loro ruolo da protagoniste all'interno delle aziende alle prese con la sicurezza degli accessi alla rete. Tuttavia, dalla ricerca condotta da Forrester emergono alcune interessanti e promettenti

digitali che appaiono più semplici da distribuire rispetto agli Otp Token fisici. Inevitabile, poi, un cenno sulle ancora più innovative autenticazioni biometriche, come le impronte digitali o il riconoscimento dell'iride. Dopo una lunga permanenza nel cosiddetto limbo del "single digit", ora il 13 per cento degli intervistati chiederà ai propri dipendenti di autenticarsi attraverso il riconoscimento delle impronte digitali o dell'iride.

Ultimo, ma non meno importante, infine, il discorso sulle soluzioni Enterprise single sign-on che l'offerta spesso integra nella sua gamma di soluzioni di autenticazione forte. In questo caso si tratta di prodotti che permettono agli utenti di effettuare il sign-on una sola volta per accedere a tutte le risorse online. Alla domanda "quanto la vostra azienda è disposta a usare un simile prodotto entro la fine del 2005?" ben il 19 per cento del campione ha risposto che lo sta già usando o è in fase di testing, l'11 per cento riscontra una buona predisposizione e l'8 per cento si dice pronto a utilizzarlo. Solo il 27 per cento ha, invece, detto di avere riscontrato una chiusura totale verso questa tecnologia. Il tutto vuol dire che l'ascesa di simili soluzioni potrebbe cominciare a far sentire nel breve periodo i suoi effetti benefici all'interno del business di grossi vendor come Computer Associates e Citrix Systems.

a cura di Marco Lorusso