



WHITEPAPER STRONG AUTHENTICATION

L'esigenza di verificare la reale identità di chi accede alle applicazioni web ed ai dati sensibili è sempre più sentita dalle aziende, al fine di ridurre la possibilità di accessi a persone non autorizzate. Oggi le organizzazioni devono affrontare una serie di minacce, nell'ambito informatico, sempre più insidiose rispetto al passato. Per questo motivo, molte aziende sono consapevoli di quanto sia essenziale proteggere i dati e le risorse dalle minacce informatiche - come ad esempio i furti di informazioni sensibili da parte di hacker e pirati informatici.

Internet e le reti hanno trasformato le informazioni. L'accesso ai dati si è esteso ad attori esterni alle aziende

Il notevole sviluppo della comunicazione via web e dei servizi online, tra cui quelli basati su sistemi che gestiscono dati sensibili, ed il frequente accesso ai dati da parte anche di attori esterni alle aziende, ha parallelamente generato una crescita delle frodi IT, provocando notevoli danni sia per gli utilizzatori che per i gestori dei servizi. Inevitabile, quindi, nelle aziende l'esigenza di verificare la reale identità di chi accede alle applicazioni ed ai dati sensibili, al fine di ridurre la possibilità di accessi a persone non autorizzate e di proteggere l'identità personale.

L'utilizzo di sistemi che si affidano solo a password statiche è altamente vulnerabile e a rischio di violazione

In un'applicazione web, l'autenticazione è il sistema fondamentale di protezione dei dati. Se un sistema di autenticazione non è abbastanza sicuro, allora i rischi associati possono diventare una reale minaccia per l'azienda. L'autenticazione basata soltanto su password ha certo il vantaggio di essere economica, ma i costi e le spese derivanti da un furto di informazioni aziendali sono sicuramente elevati. Le password possono essere manomesse, spesso sono gli stessi utenti a non gestire le password in maniera sicura (magari utilizzando la stessa password per più applicazioni, o condividendole con altri oppure annotandole su fogli), fino ad arrivare ai furti di password da parte di hacker esperti.

I sistemi di Strong Authentication (autenticazione a due fattori) hanno assunto un ruolo sempre più importante

Attraverso l'utilizzo di soluzioni di Strong Authentication è possibile garantire un controllo dell'identità più elevato rispetto ai classici sistemi basati solo su password e impedire così l'accesso non autorizzato a informazioni e risorse IT. Ad oggi, la Strong Authentication è il sistema più sicuro per il controllo degli accessi ai servizi online che eleva al massimo grado la sicurezza nell'autenticazione degli utenti e nelle transazioni basate sul web.

Un sistema di autenticazione si rafforza se utilizzato insieme ad informazioni personali

Una soluzione di Strong Authentication è un sistema di autenticazione a “due fattori”, che abbina un qualcosa che si sa – un elemento personale e mnemonico (username e password), ad un qualcosa che si ha – un elemento fisico che si possiede (un device/token che genera una One-Time Password). Oggi esistono ben poche limitazioni all’implementazione della Strong Authentication nei sistemi di autenticazione degli utenti.

La diffusione dei telefoni cellulari ha reso possibile la consegna diretta di informazioni

La soluzione che consente di utilizzare il telefono cellulare come token per certificare e autorizzare le informazioni richieste durante l’accesso a servizi web, è senza dubbio il sistema più sicuro – poiché ogni utente è direttamente identificato dal suo stesso apparecchio telefonico - e di più facile utilizzo – in quanto non richiede la consegna di dispositivi hardware o software.

In particolare questo sistema sfrutta un elemento (il cellulare) ormai pressoché diffuso tra le persone ed anche un abbattimento importante dei costi di gestione, non dovendo distribuire alcun dispositivo hardware come token o Smart Card.

Oggi è molto importante centralizzare la gestione dell’accesso e dell’accounting degli utenti

In una realtà aziendale è essenziale gestire centralmente gli accessi a molteplici dispositivi in modo semplice ed intuitivo, al fine di avere un controllo centralizzato delle configurazioni e dei sistemi di sicurezza. Gli utenti devono poter essere raggruppati e connessi a policy di autenticazione diverse per servizio. Inoltre fondamentale diventa il monitoraggio real-time sui diversi tentativi di accesso alle risorse.

Ants srl

Ants è una società dall’elevato know how tecnologico, focalizzata nell’area ICT e specializzata nell’ambito della sicurezza informatica e la protezione dei dati. MAST (l’innovativa soluzione open source di Ants dedicata alla Strong Authentication) permette ai propri Clienti di proteggere i dati aziendali e di verificare l’identità di chi accede alle applicazioni web, utilizzando il cellulare come un token. MAST eleva al massimo grado di sicurezza il controllo degli accessi remoti, in maniera semplice grazie all’immediatezza d’uso e alla semplicità di integrazione. Tutto questo abbattendo notevolmente i costi poiché non richiede la consegna di dispositivi agli utenti, né hardware, né software, non sono necessarie procedure speciali per la messa in produzione della soluzione e non ci sono costi d’implementazione o di mantenimento nascosti.

Per ulteriori informazioni visitate il sito: www.ants.eu



Via Alberto Da Giussano, 8 - 20025 Legnano (MI)
Tel +39 02 400 44 220 - Fax +39 02 899 50 180
info@ants.eu - www.ants.eu