

Glossario

servizi di Sicurezza Informatica offerti

Copyright LaPSIX 2007

Glossario servizi offerti di sicurezza Informatica

SINGLE SIGN-ON

Il Single Sign-On prevede che la parte client di un sistema venga riconosciuta solo una volta nel corso di una sessione al momento di accesso ad una applicazione basata su server: questa abilitazione iniziale offre all'utente la possibilità di accedere a tutti i server a cui il client è autorizzato dall'amministratore, senza quindi bisogno di imputare successivi login.

Un sistema basato su Single Sign-On semplifica le operazioni di accesso alle applicazioni ma non rappresenta il massimo in termini di sicurezza in quanto, secondo una definizione proposta da Cryptonet, il passo da singolo punto di accesso (single point of access) e singolo punto di attacco (single point of attack) è breve. Alcune soluzioni prevedono che un Single Sign-On offra sì la possibilità di imputare un solo login per sessione ma che questo sia autorizzato a partire da sistemi di strong authentication come possono essere i certificati di identità digitale emessi da una Pki, chiave personale di identificazione.

COMPUTER RISK ANALYSIS

Metodologia che utilizza strumenti tipicamente software per eseguire l'analisi del rischio informatico. L'analisi procede su successioni di moduli destinati all'identificazione e valutazione degli asset e all'analisi della vulnerabilità e delle minacce al sistema informatico e quindi al calcolo del rischio. I moduli di analisi possono realizzare attività di identificazione dei servizi e del flusso di dati, mappatura e valutazione degli asset, con conseguente rilevazione del grado di vulnerabilità ed esposizione al rischio. I software specifici sono in grado di automatizzare l'elaborazione e di produrre report dettagliati.

VULNERABILITY ASSESSMENT

I sistemi di vulnerability assessment sono in grado di effettuare esami in profondità per rilevare problemi che possono rappresentare vulnerabilità della sicurezza nei sistemi informatici.

I sistemi di vulnerability assessment vengono aggiornati continuamente per poter simulare l'attacco con i più recenti prodotti sviluppati dall'industria del crimine elettronico

Il servizio di Vulnerability Assessment ha come obiettivo la valutazione del livello di protezione e dell'efficacia dei sistemi di sicurezza adottati e quindi di prevenire eventuali attacchi basati su quelle vulnerabilità

ETHICAL HACKING

E' un servizio di ricerca delle vulnerabilità basato su una metodologia con cui lo specialista, come un hacker, cerca di impossessarsi di un sistema: ciò consente in una fase successiva di attuare le azioni necessarie per difendere adeguatamente il sistema. L'attività di hacking etico è a fini costruttivi e comporta l'utilizzo di competenze, inventiva e creatività al fine di penetrare un sistema informativo per preservarne la sicurezza. L'Ethical Hacking si avvale di una metodologia operativa che comporta due tipi di simulazione: la prima, dall'esterno, mediante l'uso della rete Internet, riproduce il modus operandi di un hacker/cracker; la seconda, dall'interno, ricalca l'attacco effettuato da persone con un accesso o una conoscenza delle risorse interne dell'azienda. La documentazione finale, consegnata al committente, è pertanto costituita dagli elementi provati e fornisce indicazioni sulle possibili strade da intraprendere per un miglioramento del livello di sicurezza.

INTRUSION DETECTION

I servizi di Intrusion Detection, che rientrano nelle attività di monitoraggio di una rete, servono ad individuare tentativi d'attacco del network o più in generale alterazioni delle configurazioni dei sistemi informativi in rete. Questi strumenti consentono di controllare in maniera costante eventuali intrusioni analizzando la rete con un meccanismo automatico in tempo reale. Le capacità di rilevamento delle intrusioni, comprendono diverse attività tra cui attività di Exploits, che indica un tentativo di accedere o compromettere i sistemi della rete; attività di DoS (Denial-of-Service), che indica il tentativo di usare ampiezza di banda della rete locale; attività di Reconnaissance, che serve ad indicare se qualcuno sta mappando la rete per identificare potenziali bersagli; attività di Misuse, che indica il tentativo di violare le regole aziendali. Con sistemi di Intrusion Detection gli utenti possono rilevare e interrompere le attività di rete non autorizzate sia che provengano dall'interno che dall'esterno della rete.

FIREWALL

Firewall significa "muro di fuoco".

E' uno degli strumenti principali della sicurezza informatica, progettato per impedire accessi non autorizzati a/dai reti private. Il suo utilizzo tipico quindi è quello di impedire agli utenti provenienti da Internet l'accesso non autorizzato ad una Intranet. Un firewall si occupa di filtrare i dati che passano da un computer ad un altro sulla rete, quindi applica un modello di sicurezza di tipo "perimetrale", per tenere fuori tutto ciò che non è necessario far entrare. Per reti private o Intranet con medi e alti livelli di complessità, o con necessità di particolari sicurezze, sono utilizzati anche firewall che creano serie di divisioni 'interne', per evitare che accessi non autorizzati a una macchina mettano in pericolo il resto del sistema. Il firewall divide il traffico in ammesso, rifiutato o ignorato, stabilisce un insieme di regole che definiscono a quali servizi esterni possono accedere gli utenti della Intranet e a quali servizi della Intranet o rete privata possono accedere Pc/utenti dall'esterno. Un firewall può essere un dispositivo hardware oppure un software posto come già detto fra la rete locale (Lan, local area network) ed Internet, con protezioni di vario livello. Livello di Rete, denominato screening router, che esamina ogni pacchetto di dati per valutare se farlo passare dalla rete locale oppure bloccarlo. A livello dell'Applicazione, denominato server proxy, che comunica con server esterni alla rete per conto degli utenti interni alla rete locale. Livello di Circuiti, simile al server proxy, ma crea un circuito tra client e server. Il Dipartimento della Difesa statunitense ha pubblicato un manuale per la sicurezza delle reti, chiamato "Orange Book" dove sono definiti i requisiti minimi di un firewall e le classi di sicurezza che vanno dal livello D (il più basso) al livello A (il più alto), suddivise ognuna in sottoclassi, per un totale di sette livelli di sicurezza

VPN - Virtual Private Network

Nel momento in cui si vogliono collegare tra loro, in modo sicuro, due o più filiali della stessa azienda, è necessario prevedere una connessione che possa garantire la sicurezza dei dati trasferiti da una sede all'altra. La soluzione è una Vpn (rete privata virtuale) che realizza una connessione permanente per ogni singola sede, un canale riservato e sicuro. Per Vpn si intende un collegamento che appoggiandosi su una connessione pubblica rende disponibili tutti i servizi della rete interna anche ad utenti remoti. Il riconoscimento avviene attraverso una procedura di autenticazione. Virtual Private Network vuol dire creare una rete aziendale su tutto il territorio per scambiare dati ed informazioni. Una rete privata virtuale costituisce un collegamento a livello dell'infrastruttura di rete, piuttosto che a livello delle applicazioni. La rete privata virtuale può essere realizzata secondo due tipologie. La prima collega una filiale periferica alla sede centrale ed è caratterizzata da router e firewall che trasformano in dati cifrati tutto il traffico che li attraversa. Il secondo tipo di VPN è rappresentato dal collegamento tra il notebook sul campo oppure il Pc a casa, verso una filiale o verso la sede centrale. Il collegamento può essere attivato mediante un qualsiasi ISP (Internet service provider). I vantaggi della Vpn sono: convenienza, gli utenti remoti possono collegarsi alle risorse di rete via Internet provider al prezzo di una chiamata locale; flessibilità, nuovi utenti vengono aggiunti con facilità senza nuove apparecchiature o linee dedicate; affidabilità, le Vpn sfruttano i mezzi delle infrastrutture della rete pubblica; sicurezza, le Vpn utilizzano sistemi di cifratura per proteggere il traffico privato.

WEB/MAIL CONTENT FILTERING

Si tratta dei sistemi per il controllo dell'utilizzo aziendale dei servizi Internet, delle politiche di corretto uso del servizio di posta elettronica e per il filtraggio di traffico E-mail. Mediante lo strumento di content filtering si effettua una cernita fra i siti a cui si può accedere o meno: il servizio in genere si basa su una lista di indirizzi Internet e quindi di Url a cui non è possibile accedere. Questa lista è divisa per categorie ed ogni categoria è attivabile singolarmente. A fronte di un tentativo di accesso di un utente verso uno dei siti presenti nel content filtering, in genere la connessione viene bloccata.

PENETRATION TEST

I servizi di Penetration Test consistono in un'attività preventiva: servono ad individuare eventuali vulnerabilità nei dispositivi hardware e software di una rete. Questa attività consente di predisporre misure necessarie per prevenire eventuali rischi di blocco dei sistemi informativi a seguito di attacchi o tentativi di intrusione. Effettuare un test di penetrazione significa cercare, dall'esterno del perimetro di difesa, di violarlo ricorrendo a tecniche di hacking. Dal momento che difficilmente si è in grado di effettuare questo tipo di operazione si deve ricorrere a consulenti esterni.

PKI (Infrastruttura a chiave pubblica)

In crittografia una infrastruttura a chiave pubblica, in inglese public key infrastructure (PKI) è una serie di accordi che consentono a terze parti fidate di verificare e/o farsi garanti dell'identità di un utente, oltre che di associare una chiave pubblica a un utente, normalmente per mezzo di software distribuito in modo coordinato su diversi sistemi.

Le chiavi pubbliche tipicamente assumono la forma di certificati digitali.

FIRMA DIGITALE

La firma digitale, o firma elettronica qualificata, basata sulla tecnologia della crittografia a chiavi asimmetriche, è un sistema di autenticazione di documenti digitali analogo alla firma autografa su carta. La firma digitale è un sistema di autenticazione forte in quanto si basa sull'uso di un certificato digitale memorizzato su di un dispositivo hardware.

USER ACCESS MANAGEMENT

Gestione centralizzata del profilo utenti.

SECURITY AUDITING

E' un'attività che si può ricondurre alla categoria di servizi di Vulnerability Monitoring, con la peculiarità di essere svolta su server e servizi perimetrali.

L'Internet security auditing è quindi un'attività che viene condotta al fine di rilevare eventuali vulnerabilità nella rete aziendale sia dei sistemi operativi che degli applicativi installati.

Vengono verificate anche le policy di sicurezza aziendali.

BIOMETRIA – TECNICHE BIOMETRICHE

La Biometria è un metodo matematico per misurare i dati biologici, è la scienza che usa la tecnologia digitale per identificare gli individui attraverso le loro caratteristiche fisiche. Le impronte digitali, la voce, la faccia, l'occhio di ciascun individuo sono caratteristici dell'individuo e unici. Quindi potenziali chiavi 'uniche' per accedere a servizi protetti da un sistema di sicurezza: basta digitalizzare una di queste caratteristiche e inserirla in una banca dati. Un identificatore biometrico cattura un'immagine della caratteristica da utilizzare per il riconoscimento, la elabora e la archivia per confronti successivi e all'occorrenza si interfaccia con il sistema di controllo che confronta le immagini con quelle presenti nel database. Ad esempio l'iride è una caratteristica assolutamente unica. Per il processo di riconoscimento dell'iride la tecnologia si avvale anche di alcune raffinatezze come registrare e misurare i tempi di dilatazione e contrazione della pupilla per accertare che davanti al sistema di sicurezza ci sia la faccia di un essere umano e non la foto del suo occhio.