Le “Best Practices” per proteggere Informazioni, Sistemi e Reti

www.vincenzocalabro.it

Goal

E’ difficile implementare un perfetto programma di organizzazione e gestione della sicurezza informatica, ma è importante che la “cultura della sicurezza” sia alla base di ogni operazione che coinvolga la struttura di rete.

Obiettivi 1 di 4

- Proteggere l’infrastruttura dai danni causati da virus, spyware ed altro codice maligno
- Fornire sicurezza alla propria connessione internet
- Installare ed attivare firewall software sui computer
- Applicare le più recenti patch di sicurezza a sistemi ed applicazioni
- Effettuare copie di backup dei dati sensibili

Proteggere l’infrastruttura dai danni causati da virus, spyware ed altro …

- Installare ed utilizzare, possibilmente in modalità “real-time”, antivirus ed antispyware costantemente aggiornati sia a casa che al lavoro.
- Impostare aggiornamenti e scansioni a cadenza regolare in orari in cui la macchina rimane accesa e scarsamente utilizzata
- E’ una buona idea installare nel computer che si utilizza a casa la versione “not for commercial purpose” dei software di protezione che si trovano installati nel proprio ambiente lavorativo

Fornire sicurezza alla propria connessione internet

- Molte aziende hanno connessioni a banda larga ed è molto importante tenere presente che questo tipo di connessioni sono sempre attive, anche di notte o quando i dipendenti non sono presenti.
- Pertanto diventa imperativo installare e tenere operativo un firewall hardware tra la propria rete interna ed internet.
- E’ importantissimo assicurarsi che le reti casalinghe dei dipendenti, soprattutto di quelli che svolgono parte del lavoro da casa, siano anch’esse protette
- Durante la fase di installazione dei firewall e di tutti gli apparati di controllo è una buona idea sostituire le credenziali di accesso di default con altre meno facili da individuare

Installare ed attivare firewall software sui computer

- Installare, utilizzare e tenere aggiornati firewall software su ciascuna macchina che si trovi all'interno del perimetro della LAN
- Nel caso di Microsoft Windows e Mac Os X ad esempio un firewall di buon livello è già incluso all'interno del sistema operativo
- E' importante che siano presenti anche firewall software nel caso un malvivente riesca a bypassare la prima protezione all'ingresso della rete
- Anche in questo caso è molto utile proteggere con firewall software in computer utilizzati all'interno della rete casalinga dai dipendenti

Applicare le più recenti patch di sicurezza a sistemi ed applicazioni

- Tutti i produttori di sistemi operativi pubblicano regolarmente patch e aggiornamenti di sicurezza che è molto importante applicare a tutti i computer aziendali e casalinghi per assicurarsi che le ultime falle di sicurezza ed exploit applicabili ai nostri sistemi vengano resi vani nel minor tempo possibile.
- Lo stesso dicasi per i software di produttività (es.: Microsot Office) che devono essere «patchati» con regolarità per evitare sgradevoli sorprese.

Effettuare copie di backup dei dati importanti

- Tenere copie di sicurezza dei dati sensibili (documenti, fogli elettronici, database, gestionali, …) possibilmente effettuate in maniera automatizzata e schedulata.
- Le copie di sicurezza dovrebbero essere conservate sia in azienda in comparti ignifughi, sia lontano dal luogo lavorativo per essere protetti in caso di incendi ed eventi imprevedibili che potrebbero danneggiarle.
- E’ necessario anche pianificare con regolarità delle prove di ripristino dei dati sottoposti a backup come parte integrante della strategia di disaster recovery.

Obiettivi 2 di 4

- Controllare l’accesso fisico ai computer ed ai componenti di rete
- Mettere in sicurezza le reti wireless
- Formare i dipendenti sui principi base della sicurezza
- Implementare account utente individuali per ciascun dipendente
- Limitare l’accesso a dati ed informazioni e la possibilità di installare applicazioni

Controllare l’accesso fisico ai computer ed ai componenti di rete

- Non consentire a personale non autorizzato l’accesso fisico o l’utilizzo dei computer aziendali. E’ consigliato anche il posizionamento degli schermi in posizioni non visibili ad esempio da visitatori o, meglio ancora, l’utilizzo di «privacy screen» per impedire la visione a tutti tranne che all’utilizzatore seduto davanti allo schermo.
- Impedire che personale non autorizzato abbia accesso ad aree ove sono presenti apparati di rete e computer senza essere accompagnati e senza che sia strettamente necessario: potrebbe già essere un buon metodo per un eventuale malvivente per ottenere informazioni di base sull’infrastruttura come marche e modelli dei prodotti utilizzati.

Mettere in sicurezza le reti wireless

- Se si utilizzano reti wireless sarebbe già un buon punto di partenza disabilitare il broadcast del SSID (Service Set Identifier) così da rendere necessario a chi voglia collegarsi conoscere preventivamente il nome della rete.
- Sostituire le credenziali amministrative di default degli access point.
- Utilizzare sistemi di criptazione dei dati il più possibile sicuri: attualmente è consigliato l'utilizzo del WPA2 con una chiave di criptazione il più possibile complessa e illogica.
- Se possibile affiancare ai suddetti metodi anche l'autenticazione con un server RADIUS e il filtraggio dei MAC address dei computer e dei dispositivi che possono connettersi.

Formare i dipendenti sui principi base della sicurezza

- Tutti coloro che utilizzano i computer o più in generale qualsiasi apparato connesso alla rete aziendale, dovrebbero essere formati sulla modalità più corretta di utilizzare e proteggere le informazioni in essa contenute.
- Già dal primo giorno di lavoro i dipendenti dovrebbero essere informati sugli strumenti utilizzati per proteggere i dati e sul fatto che una corretta «cultura della sicurezza» è parte integrante del compito da loro svolto all'interno dell'azienda.
- Inoltre è fondamentale implementare sistemi di sicurezza e comportamenti che impediscano all'utente, se non autorizzato e se non strettamente necessario, di portare al di fuori del perimetro dell'azienda dati sensibili e strategici per l'azienda stessa.

Implementare account utente individuali per ciascun dipendente

- Creare un account separato per ciascun dipendente e l'implementazione di password di elevata complessità che debbano essere sostituite con regolarità consente di proteggere l'infrastruttura oltre a rispondere ai requisiti della Legge sulla privacy.
- L'assegnazione di account utente individuali consente inoltre di poter risalire al responsabile di eventuali comportamenti scorretti o fraudolenti.
- Inoltre è opportuno limitare permessi assegnati agli account utente per consentire di svolgere esclusivamente i compiti assegnati riducendo al minimo il numero degli account amministrativi.

Limitare l’accesso a dati ed informazioni e la possibilità di installare applicazioni

- La scomoda realtà è che spessissimo gli «insiders» cioè tutti gli utenti di una infrastruttura informatica sono la prima fonte delle problematiche di sicurezza all’interno dell’azienda.
- Il motivo è che essendo già all’interno della rete le loro azioni vengono di solito considerate attendibili e ci si concentra maggiormente sulle minacce provenienti dall’esterno.
- Per questo è importante non consentire l’accesso a tutti i dati e sistemi a tutti i dipendenti. Per ogni impiegato fornire esclusivamente l’accesso a quei sistemi che contengono le informazioni specifiche che sono loro necessarie nello svolgimento di compiti specifici.

Obiettivi 3 di 4

- Considerazioni di sicurezza relative agli allegati delle email
- Considerazioni di sicurezza relative a link nelle email, chat e social network
- Considerazioni di sicurezza relative a popup web ed altri «raggiri»
- Operazioni finanziarie online in sicurezza

Considerazioni di sicurezza relative agli allegati delle email

- Sia per quanto riguarda le email lavorative che quelle personali è importantuissimo non aprire allegati a meno che quella mail non fosse attesa e il mittente non sia considerato attendibile.
- Uno dei metodi più utilizzati per diffondere spyware e codice maligno è ovviamente l'utilizzo degli allegati delle email: ma troppo spesso si abbassa la guardia dando per scontato di essere al sicuro solo perché si è installato un buon antivirus. Il miglior livello di protezione è sempre dato dal buon senso.

Considerazioni di sicurezza relative a link nelle email, chat e social network

- Sembra scontato ma è importante evitare di cliccare sui link contenuti nelle email. Lo stesso dicasi per le pagine di Facebook, per altri social network e per le chat in genere. Questo è il metodo in assoluto più utilizzato ad esempio negli attacchi di phishing che simulano l'estetica di mittenti attendibili sia nelle email che nelle pagine web a cui rimandano, per carpire le credenziali dell'utente ed utilizzarle in modo fraudolento.
- Può essere utile posizionarsi senza cliccare sul link per visualizzare il collegamento a cui rimanda (esempio nella prossima slide) ed avere un'ulteriore conferma sull'attendibilità dell'email.

Considerazioni di sicurezza relative a popup web ed altri «raggiri»

- Quando si utilizza internet, evitare di cliccare «ok» in qualsiasi popup dovesse presentarsi. Se viene visualizzata ad esempio una finestra che informa di essere stati infettati da un virus e di cliccare «ok» per scaricare l'antivirus che risolverà il problema, è preferibile cliccare sulla croce in alto a destra piuttosto che su qualsiasi altro pulsante rappresentato.
- Evitare di raccogliere drive o pennette USB provvidenzialmente lasciate incustodite da malviventi apposta per solleticare la curiosità dei passanti e in realtà probabilmente contenenti codice maligno che si avvierà in automatico all'inserimento nel pc. Disabilitare la funzione «autorun» sui computer.

Operazioni finanziarie online in sicurezza

- E ‑ commerce, e ‑ banking e transazioni finanziarie online in genere devono sempre essere effettuate utilizzando una connessione HTTPS sicura, normalmente verificabile dalla presenza di un lucchetto sulla barra del browser.
- Terminata la transazione è opportuno cancellare la cache del browser, i file temporanei, i cookies e la cronologia del browser internet.
- In generale evitare di effettuare pagamenti online con venditori di cui non si conosce l'identità o più in generale non è possibile identificarne la reale esistenza.
- Abilitare i «secure code» presso il circuito emittente della propria carta di credito per proteggere con una password ulteriore le transazioni online

Obiettivi 4 di 4

- Considerazioni di sicurezza sulla navigazione web
- Download di software da internet
- Smaltimento di computer e media danneggiati e/o obsoleti
- Come proteggersi dal Social Engineering

Considerazioni di sicurezza sulla navigazione web

- Non bisognerebbe mai navigare in internet utilizzando un account con privilegi amministrativi, altrimenti tutti i codici maligni che si dovessero incontrare potrebbero installarsi nella macchina utilizzando gli stessi privilegi.
- Per evitare la suddetta vulnerabilità è opportuno implementare un account «guest» da utilizzare appositamente per la navigazione.
- Utilizzare sempre la versione più aggiornata del proprio browser internet per evitare di essere soggetti a vulnerabilità che le ultime patch di sicurezza potrebbero aver risolto.

Download di software da internet

- Non scaricare nessun tipo di software da pagine web sconosciute.
- Solo le pagine web appartenenti a fornitori attendibili dovrebbero essere considerate affidabili per il download di software.
- L'utilizzo di programmi P2P per lo scambio di file utilizzando internet, oltre che il più delle volte illegale, ha aperto le porte alla diffusione di ogni sortacdi codice malevolo scaricato inconsapevolmente da utenti alla ricerca dell'ultimo film o album musicale. Evitare di eseguire qualsiasi file scaricato utilizzando questo metodo se non preventivamente verificato utilizzando antivirus e antispyware aggiornati con le ultime definizioni disponibili.

Smaltimento di computer e media danneggiati e/o obsoleti

- Quando si smaltiscono i vecchi computer, rimuovere gli hard disk e distruggerli per evitare che dati sensibili possano essere recuperati da terzi.
- Lo stesso dicasi quando si devono gettare vecchi media (CD, floppy disk, drive USB, carta) contenenti dati personali o sensibili.
- Capita spesso che aziende e privati vendano i loro vecchi computer e sia possibile ritrovarli su eBay con all'interno ancora tutti i dati perfettamente disponibili.

Come proteggersi dal Social Engineering

- Il social engineering è un tentativo personale o elettronico di ottenere informazioni o accessi non autorizzati a sistemi o aree sensibili «manipolando» le persone.
- Il social engineer effettua ricerche sull'azienda per reperire nomi, ruoli e tutti le informazioni sulle identità personali pubblicamente disponibili. Poi solitamente chiama il centralino o l'help desk dell'azienda stessa con una fittizia ma credibile storia che convinca la persona all'altro capo che il social engineer sia in realtà un dipendente o una persona associata all'azienda che ha bisogni di dati di accesso che il malcapitato si sente obbligato a fornire.
- Occorre essere vigili. Quando qualcuno chiama per ricevere aiuto e richiede informazioni sull'accesso ai sistemi è necessario innanzitutto identificare il chiamante chiedendo informazioni che solo un reale dipendente può conoscere. Se egli non è in grado di fornire queste informazioni, rifiutare fermamente di proseguire con la chiamata.

Grazie

www.vincenzocalabro.it