le campagne interne di Security Awareness verso i dipendenti

L'esperienza della ASL NAPOLI 2 NORD

Di Imma Orilio
CIO & INNOVATION PROGRAM MANAGER

"This tops the list of recommendations for upgrading your online security."

ART. 1 – CONVINCERE IL CAPO CHE INTERNET E' COSA BUONA!

SICUREZZA INFORMATICA

• OBIETTIVI

- il **controllo** del diritto di accesso alle informazioni;
- la **protezione** delle risorse da danneggiamenti volontari o involontari e l'**integrità** delle informazioni mentre esse sono in transito sulla rete;
- La **confidenzialità**, che consiste nell'assicurare che solo le persone autorizzate abbiano accesso alle risorse scambiate :
- La **disponibilità**, che permette di mantenere il corretto funzionamento del sistema d'informazione :
- Il **non ripudio**, che permette di garantire che una transazione non possa essere negata :
- L'**autenticazione**, che consiste nell'assicurare che solo le persone autorizzate abbiano accesso alle risorse e la **verifica** dell'identità dell'interlocutore

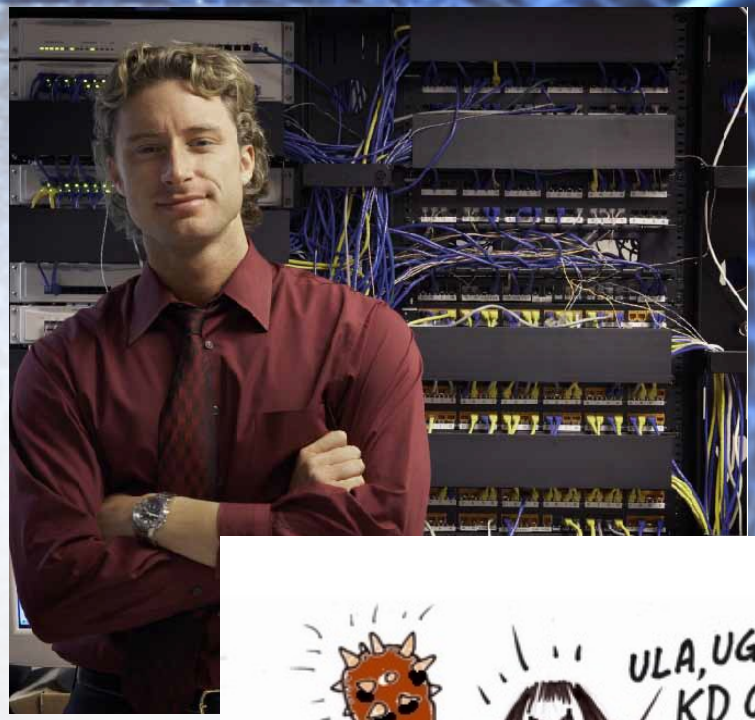
• STRUMENTI

- **Prevenzione**: è necessario implementare delle misure per prevenire lo sfruttamento delle vulnerabilità del sistema.
- **Detezione**: è importante rilevare prontamente il problema; prima si rileva il problema, più semplice è la sua risoluzione.
- **Risposta**: è necessario sviluppare un piano appropriato di intervento in caso di violazione con individuazione delle responsabilità e le azioni da intraprendere.

Il ruolo dell'Amministratore

- **educare e rendere consapevoli** dei rischi derivanti dall'uso non appropriato del web in ambito lavorativo.
- **ridurre il rischio** che in ufficio il social network venga utilizzato in modo indebito attraverso chiare regole di disciplina da aggiornare periodicamente, in cui indicare chiaramente quali sono i comportamenti:
  - tollerati,
  - da evitare,
  - in grado di generare una verifica.

- In merito alle modalità di **verifica**, bisogna sempre tener presente che i controlli a distanza sono vietati. Tipicamente, viene individuata una categoria di siti adeguati per svolgere l'attività aziendale e una categoria di siti proibiti perché non adeguati all'attività aziendale.



L'impatto sulla PA del web 2.0

Le applicazioni Web 2.0 per la pubblica amministrazione sono interessanti su vari fronti tra cui:

- fare crescere la partecipazione politica dei cittadini;
- fornire strumenti semplici ai cittadini con cui contribuire al miglioramento dei servizi;
- creare relazioni aperte e trasparenti tra cittadini e amministrazione;
- costruire un'amministrazione più semplice e interconnessa tramite software a basso costo.

L'impatto sulla PA del web 2.0

L'e-government tramite il Web 2.0 è strategico per raggiungere la modernizzazione del servizio pubblico verso l'utente in termini di:

- semplificazione delle procedure;
- orientare l'utente nella scelta e nell'uso dei servizi;
- i cittadini collaborano per fornire nuovi servizi;
- i cittadini criticano il funzionamento dei servizi;
- trasparenza degli atti amministrativi;
- servizi più usabili.

E verso i funzionari pubblici in termini di:

- integrazione, efficienza e innovazione;
- collaborazione interistituzionale;
- knowledge management tramite social bookmark, RSS, blog;
- gestione risorse umane;
- aggiornamento.

Vulnerabilità del web 2.0

Le soluzioni tradizionali di sicurezza informatica non sono adeguate a questa problematica perché:

- Firewalls e antivirus non possono bloccare tutti gli eventuali attacchi al livello applicativo poiché la porta 80 deve essere disponibile per essere utilizzata;
- gli strumenti di scansione della rete non identificano le vulnerabilità a livello applicativo;
- gli sviluppatori di applicazioni Web non hanno conoscenze adeguate di sicurezza applicativa.

I rischi per la sicurezza dalle applicazioni web 2.0

Nell'ambito della elevata interazione tra client e server il punto debole della sicurezza consiste nella possibilità di modificare i messaggi scambiati tra client e server al fine di creare pericoli.

Mettendoci nell'ottica dell'azienda che vuole consentire l'accesso al web 2.0 per i propri utenti, e concentrandoci sulle problematiche di sicurezza che queste scelte possono indurre, ci si può focalizzare su due categorie di problemi:

1) **Malware Intrusion**
2) **Data Extrusion**

I rischi per la sicurezza dalle applicazioni web 2.0

1) **Malware Intrusion** - sono i contenuti che possono essere scaricati dagli utenti attraverso il canale del SN: hyperlink, file o applicazioni che contengono o puntano a contenuti malevoli che, una volta eseguiti dall'host interno all'azienda, rischiano di compromettere la sicurezza dell'intera rete.
2) **Data Extrusion** - riguarda i dati di proprietà dell'azienda che devono essere trattati solo in un contesto controllato secondo le policy definite, ma che possono essere resi pubblici attraverso la pubblicazione nel SN, causando potenziali problemi alla reputazione e alla proprietà intellettuale dell'azienda. Si pensi alla condivisione di informazioni tecniche e non solo, come si vede spesso nei blog.

Per affrontare entrambi i problemi occorre adottare tecnologie in grado di analizzare in dettaglio i contenuti dei flussi di traffico.

Cosa fare?

Le minacce tipo Malware Intrusion si affrontano “architetturalmente” partendo dal perimetro della rete aziendale, in modo da eliminare all’ingresso eventuali malware veicolati attraverso la connessione al SN. Tipicamente i sistemi in grado di realizzare questo tipo di filtraggio sono:

- Network Intrusion Prevention;
- Network Antivirus;
- Url Content filtering;
- Mail content inspection.

fino alle tecnologie di protezione degli host tipo:

- Host Antivirus;
- Host Intrusion Prevention.

La minaccia tipo Data Extrusion o Data Leakage, al contrario del Malware Intrusion, deve essere affrontata cercando di applicare i controlli di sicurezza il più vicino possibile ai dati, tipicamente sulle macchine degli utenti:

Esiste il web sicuro?

Alcune linee guida per realizzare applicazioni web sicure:

- controllo delle operazioni di autenticazione dell'utente, aggiornamento delle politiche di autorizzazione alle risorse, verifica della robustezza delle password;
- riduzione delle superfici esposte all'attacco, tramite un elenco chiaro ed esaustivo delle componenti logiche e strutturali dell'applicazione e delle divisioni con relative interfacce, eliminazione di componenti inutili ma potenzialmente dannosi, riduzione della possibilità di manipolazione dell'input durante il passaggio tra le varie componenti
- struttura dell'applicazione con componenti e ogni componente deve essere blindato per non offrire risorse ai maleintenzionati;
- controllo dei privilegi permessi all'utente per l'accesso alle funzioni dei componenti;
- controllo degli input provenienti dall'utente prima di eseguirli, sia input espliciti tramite form sia impliciti come gli header Http e altri dati provenienti dai server;
- scrittura attenta dei messaggi di errore per non mostrare informazioni in grado di far scoprire struttura e comportamenti dei componenti sensibili;
- costante aggiornamento dei sistemi;
- gestione della sessione utente, apertura mantenimento e chiusura per evitare furti degli id sessione e la contemporanea presenza dello stesso utente in più sessioni differenti;
- gestione dei file log dell'applicazione per il tracciamento delle sessioni, del comportamento dell'utente e della comunicazione tra le componenti;
- creazione di un sistema di avviso in caso di condizioni anomali;
- difesa da denial of service.

I rischi per il datore di lavoro

- Diffusione dei *malwares* in crescita costante: si calcola che, nel solo anno 2008, su internet siano circolati circa 15 milioni di *malwares*, di cui quelli circolati tra i mesi di gennaio e agosto sono pari alla somma dei 17 anni precedenti, e tali numeri sono destinati verosimilmente ad aumentare (dati riferiti a “Sicurezza, in una classifica i bug più pericolosi”, sito “Punto-informatico.it).

… gli obblighi reciproci.

I dipendenti hanno l'obbligo di:

- Non causare danni o pericoli ai beni e agli strumenti ad essi affidati…
- Non utilizzare a fini privati materiali o attrezzature di cui dispongono per ragioni d'ufficio…

I datori di lavoro devono:

- Informare specificamente i lavoratori circa attività permesse e vietate …
- Rispettare il principio di proporzionalità, pertinenza e non eccedenza nelle eventuali attività di controllo.

...perché un Disciplinare per l'utilizzo di Internet e della posta elettronica?

L'esigenza di adottare un Disciplinare che regoli l'utilizzo di internet e della posta elettronica (e, più in generale, dei dispositivi e delle attrezzature informatiche utilizzati sui luoghi di lavoro) come già accennato, nasce dal ricorso sempre più frequente a tali strumenti nell'organizzazione e nell'espletamento dell'attività lavorativa.

… premesso che:

- In applicazione di quanto disposto dagli artt. 2104 e 2105 c.c., l'utilizzo di tali indispensabili risorse deve avvenire nell'ambito dei doveri di diligenza, fedeltà e correttezza che devono caratterizzare l'operato del lavoratore all'interno del rapporto di lavoro, in modo che siano adottate tutte le cautele e le precauzioni necessarie per evitare le possibili conseguenze dannose che un utilizzo non avveduto degli strumenti in questione può provocare.

- Il datore di lavoro, a norma degli artt. 2086, 2087 e del richiamato art. 2104 c.c. può riservarsi di controllare l'effettivo adempimento della prestazione lavorativa e il corretto utilizzo degli strumenti di lavoro, rispettando, nell'esercizio di tali prerogative, la libertà e la dignità del lavoratore (art.4 L. 300/1970).

e che inoltre …

- L'art. 10 del Codice di comportamento dei dipendenti delle PP.AA., allegato al C.C.N.L. del 22/01/2004, stabilisce che *"Il dipendente non utilizza a fini privati materiale o attrezzature di cui dispone per ragioni di ufficio"*. Tale disposizione, in quanto richiamata dal Codice Disciplinare del C.C.N.L. del comparto (che all'art. 44, comma 1, lett. i) e l) prevede a carico del lavoratore di avere cura dei locali, mobili, oggetti, macchinari, attrezzi, strumenti ed automezzi a lui affidati e di non valersi di quanto è di proprietà …

Ma soprattutto

… dell'Amministrazione per ragioni che non siano di servizio), costituisce non solo norma di valenza etico-comportamentale, ma altresì un vero e proprio obbligo, la cui inosservanza è passibile di sanzione penale e/o disciplinare.

MA VI SONO DELLE VERE E PROPRIE NORME CHE REGOLANO L'USO DELLA POSTA ELETTRONICA E LA NAVIGAZIONE SU INTERNET DA PARTE DEI DIPENDENTI PUBBLICI?

Esisteva una disposizione normativa relativa all'uso privato delle linee telefoniche d'ufficio, contenuta nel decreto del Ministro della Funzione Pubblica del 31/3/1994, con la quale fu adottato il Codice di comportamento dei dipendenti della P.A. ai sensi dell'art. 58 bis del D. Lgs. N. 29/1993. Si trattava, come già accennato, dell'art. 10 che, alla prima parte del comma 5, prevedeva che "salvo casi eccezionali dei quali informa il dirigente dell'ufficio, il dipendente non utilizza le linee telefoniche dell'ufficio per effettuare chiamate personali".

PERO'…

La necessità di ampliare questa limitata facoltà di deroga collegata al requisito dell'eccezionalità ha indotto successivamente il Ministro della Funzione Pubblica a rivedere l'impostazione iniziale dell'art. 10. Infatti, il successivo Codice di comportamento dei dipendenti pubblici di cui al D.M. del 28/11/2000 ha previsto al comma 3 dell'art. 10 che il dipendente "salvo casi d'urgenza, non utilizza le linee telefoniche d'ufficio per esigenze personali". Tale disposizione di carattere puramente amministrativo, a parte il riferimento alle sole apparecchiature telefoniche, non sembra comunque tale da escludere, totalmente, la responsabilità civile e penale nel caso di uso illecito delle linee telefoniche da parte del dipendente pubblico.

Per quanto riguarda l'orientamento dottrinale e giurisprudenziale in materia, la dottrina penale è divisa in ordine alla natura giuridica della posta elettronica e alla possibilità dei dirigenti dell'ufficio di controllare l'uso che i dipendenti fanno, in genere, degli strumenti tecnologici a loro disposizione.

La migliore dottrina ritiene che, almeno sino a quando il dipendente non acceda alla sua casella ed apra il messaggio di posta elettronica, il messaggio stesso debba considerarsi come "corrispondenza chiusa" e, come tale, tutelata ai sensi dell'art. 616 c.p. Questa tesi è stata sostenuta in giurisprudenza, implicitamente, da una decisione del T.A.R. Lazio, Sez. I, n. 9425 del 15/11/2001, in relazione ad una *mailing list* in ambiente pubblico secondo cui "la corrispondenza trasmessa per via informatica e telematica, c.d. posta elettronica, deve essere tutelata alla stregua della corrispondenza epistolare o telefonica ed è, quindi, caratterizzata dalla segretezza".

Tale tesi è peraltro sostenuta dal Garante della Privacy (vedi parere del 12/7/1999) secondo cui, appunto, la posta elettronica sarebbe protetta ai sensi dell'art. 616, comma 4, c.p.

La peculiarità del sistema universitario

- La rete telematica dell'Università degli Studi di Palermo fa parte dell'infrastruttura di rete telematica nazionale denominata GARR (Gruppo Armonizzazione Reti della Ricerca) di cui utilizza i servizi di collegamento e di interoperabilità, al fine di garantire un'infrastruttura di rete che faciliti la ricerca, la didattica e l'amministrazione, consentire il buon funzionamento della rete VoIP (Voice over IP) e delle altre attività istituzionali dell'Ateneo.

Provvedimento n. 13 del 1° marzo 2007 del Garante della Privacy – Linee Guida per posta elettronica e internet

… rischio che, a seguito di un legittimo controllo, il datore di lavoro possa entrare in possesso di notizie e dati inerenti alla sfera privata del lavoratore. In tal senso, prevale la logica preventiva: la prevenzione degli abusi viene ritenuta dal Garante di gran lunga preferibile all'individuazione degli stessi.

aslnapoli2nord

AZIENDA SANITARIA LOCALE **NAPOLI2NORD**

www.aslnapoli2nord.it • info@aslnapoli2nord.it

grazie