

Le minacce arrivano dall'interno

Security Summit
Milano 25 marzo 2009

Paolo Giardini
Resp. Relazioni
Osservatorio Nazionale Privacy
e Sicurezza delle Informazioni

- Libero Professionista dal 1991, Consulente per la sicurezza delle Informazioni
- Eucip Certified - European Certification of Informatics Professionals
- Membro del Comitato Esecutivo del CCOS della Regione Umbria
- Socio Fondatore e Consigliere del GNU/LUG Perugia
- Privacy Officer AIP - Associazione Informatici Professionisti
- Responsabile Relazioni OPSI – Osservatorio Nazionale Privacy e Sicurezza delle Informazioni
- Socio CLUSIT- Associazione Italiana per la Sicurezza Informatica
- Socio AIPSI Associazione Italiana Professionisti Sicurezza Informatica
- Socio ISSA - Information System Security Association
- Socio ILS – Italian Linux Society
- Iscritto all'Albo Consulenti e Docenti FORMEZ - Dipartimento della Funzione Pubblica
- Thawte Web of Trust Notary

- Come le aziende vedono la Sicurezza delle informazioni
- Alcuni risultati tratti da analisi effettuate da istituti di ricerca ed aziende del settore
- Esempi reali tratti da casi vissuti
- Strategie e tecniche per la mitigazione del rischio
- Il ruolo del Professionista

Le aziende, specie le piccole e medie imprese ma in qualche caso anche aziende di grandi dimensioni non hanno una reale percezione del significato di “sicurezza informatica”.

I dati non vengono considerati come una risorsa da proteggere ma solo come “oggetti” da utilizzare non valutando il loro reale valore per l'azienda.

Come vedono la sicurezza le aziende ?

- Le aziende vedono gli investimenti nella sicurezza come un costo ulteriore.
- Gli obblighi di legge sono un inutile aggravio delle già tante incombenze amministrative.

Alcune frasi famose:

- “Tanto basta fare un po di documenti”.
- “Non abbiamo nulla che interessi un hacker”.
- “Abbiamo altre priorità”.

- Da sempre, o almeno da quando è nata l'informatica personale, la sicurezza è stata vista come qualcosa da comperare.
- Inizialmente era l'***Antivirus***.
- Poi, con l'avvento di Internet, sono arrivati i ***Firewall***, la medicina per tutti i mali.
- Contemporaneamente, è aumentato il potere del singolo utente che diviene *proprietario* del pc (*ne parleremo dopo*).

- Ammesso che vengano messi in pratica i dettami minimi della 196/2003, ci si limita alla installazione di un firewall, di antivirus ed alla redazione (fotocopia?) di generiche policy di sicurezza e del DPS.
- Le password spesso sono un fastidioso obbligo da evitare il più possibile.
 - Gli antivirus “si aggiornano da soli”.
 - Il firewall “lo ha installato il tecnico”.
 - Di *formazione* degli utenti non si parla.

La preoccupazione maggiore è
come “*tenere fuori i cattivi*”.

“La sindrome di Fort Apache”
è la definizione che ha creato
Corrado Giustozzi e che riassume
perfettamente la situazione.

Sono stati realizzati molti studi sugli incidenti di sicurezza verificatisi presso le aziende (Cisco, McAfee, Computer Security Institute, Sophos ed altri).

- In tutti gli studi, viene evidenziato come la causa di oltre il 50% degli incidenti di sicurezza va ricercata nei comportamenti errati degli utenti.
- Al primo posto viene l'uso personale fatto degli strumenti aziendali.
- In seconda battuta, la non osservanza delle pratiche di sicurezza (per negligenza o semplice ignoranza).

- Circa 2 terzi degli intervistati che utilizzano un PC fanno regolarmente uso di chiavette USB;
- Il 26% del campione preso in esame che utilizza un PC lo usa anche per scaricare musica o film o software;
- Il 21% degli intervistati che utilizza un PC vi carica dei giochi;
- Circa 1/3 degli utenti che utilizza un PC invia abitualmente email personali
- Più della metà degli utenti invia dati confidenziali via email
- Più della metà degli utenti usa il PC per operazioni di Internet banking
- Molto diffuso l'utilizzo di applicazioni di Instant messaging sul proprio PC di lavoro
- L'80% degli utenti mobile usano chiavette USB UMTS

Vediamo la cosa da un punto di vista capovolto.

Poniamoci delle domande e vediamo che risposte ci diamo.

Cominceremo a vedere che i “cattivi” non sono solo “fuori”, al di là della palizzata.

Proviamo a fare alcune domande

Quali informazioni sono presenti
in azienda?

Quali informazioni sono presenti in azienda?

- Spesso in azienda nessuno sa rispondere con precisione a questa domanda

Dove sono localizzate le
informazioni aziendali?

Dove sono localizzate le informazioni aziendali?

- E' un'altra domanda “difficile”.
- Nel caso migliore la risposta è incompleta
- Nel caso peggiore la risposta non è conosciuta

Chi ha accesso alle informazioni
aziendali?

Chi ha accesso alle informazioni aziendali?

- Spesso in azienda nessuno sa rispondere con precisione a questa domanda
- Troppo spesso la risposta è “tutti”!

Che valore hanno le informazioni
per la mia azienda?

Che valore hanno le informazioni
per la mia azienda?

....!

- L'azienda non è solo mura, macchinari, magazzini, dipendenti.
- Pensiamo ai dati di contabilità, contratti, analisi finanziarie, contatti marketing, informazioni sui clienti, obiettivi di vendita, offerte, accordi, brevetti, progetti, ...
- Pensiamo ai dati personali, anche sensibili, dei dipendenti.
- Vedremo che l'Azienda è le proprie *informazioni* e vive grazie ad esse.

Che valore do alle informazioni
nella mia azienda?

Facciamo un breve excursus nel mondo reale per vedere cosa ci troviamo di fronte.

Situazione

- Uno studio di Commercialista

Incidente

- Rottura del disco sul quale veniva effettuato il backup

Azione

- Non hanno trovato il tempo per cambiarlo

Risultato

- Il backup non veniva effettuato
- Hanno perso un anno di lavoro

Situazione

- Uno studio di Commercialista

Incidente

- Rottura del disco sul quale veniva effettuato il backup

Azione

- Non hanno trovato il tempo per cambiarlo

Risultato

- Non veniva effettuato il backup
- Hanno perso un anno di lavoro

NON CURANZA

Situazione

- Un Ente Pubblico Economico

Incidente

- Gli utenti lamentano estrema lentezza nelle connessioni Internet

Azione

- Vengono raddoppiate le linee con 4 ADSL da 4 Mb

Risultato

- Una successiva analisi ha mostrato come la lentezza fosse dovuta ad un elevato utilizzo della banda per *scopi privati* da parte di alcuni utenti

Situazione

- Un Ente Pubblico Economico

Incidente

- Gli utenti lamentano estrema lentezza nelle connessioni Internet

Azione

- Vengono raddoppiate le linee con 4 ADSL da 4 Mb

Risultato

- Una successiva analisi ha mostrato come la lentezza fosse dovuta ad un elevato utilizzo della banda per *scopi privati* da parte di alcuni utenti

SEMPLICISMO

Situazione

- Una azienda progetta e produce apparati ad alta tecnologia

Incidente

- Alcuni dipendenti si licenziano

Azione

- Nessuna

Risultato

- Tempo dopo viene creata una nuova azienda che produce (guarda caso) apparati ***molto simili*** a quelli prodotti dalla nostra azienda.
- Nella nuova azienda lavorano gli ex dipendenti della nostra azienda

Situazione

- Una azienda progetta e produce apparati ad alta tecnologia

Incidente

- Alcuni dipendenti si licenziano

Azione

- Nessuna

Risultato

- Tempo dopo viene creata una nuova azienda che produce (guarda caso) apparati *molto simili* a quelli prodotti dalla nostra azienda.
- Nella nuova azienda lavorano gli ex dipendenti della nostra azienda

INDUCIOSI

Situazione

- Il Presidente è in viaggio d'affari per concordare fusioni, partecipazioni ed altri accordi con alcune aziende competitor.

Incidente

- Il notebook del Presidente, custodito nel bagagliaio dell'auto parcheggiata nel piazzale di una di queste ditte scompare.

Azione

- Nessuna

Risultato

- Gli accordi si fanno, ma con risultati molto minori rispetto alle aspettative.

Situazione

- Il Presidente è in viaggio d'affari per concordare fusioni, partecipazioni ed altri accordi con alcune aziende competitor.

Incidente

- Il notebook del Presidente, custodito nel bagagliaio dell'auto parcheggiata nel piazzale di una di queste ditte scompare.

Azione

- Nessuna

Risultato

- Gli accordi si fanno, ma con risultati molto minori rispetto alle aspettative.

IMPREVEDIBILI

Ma potremmo continuare a lungo...

- La password di root data per telefono agli utenti (che si sono perse le loro password)
- La password dell'amministratore utilizzata dal tecnico esterno in assistenza remota
- Il Pc isolato infettato perché connesso ad internet con un modem umts usb dall'utente
- L'incaricato del backup che non si accorge per mesi che non vengono effettuate le copie perché il tape esterno non funziona
- Il Wireless (aperto) installato dal tecnico esterno all'insaputa dell'azienda
- La carta, riusata per fotocopie e imballaggi, con informazioni confidenziali (relazioni, contratti, pezzi di codice,...)

Dai casi che abbiamo visto emerge che gran parte dei problemi nasce per un non corretto comportamento del dipendente, sia esso utente o amministratore di sistema.

Se proviamo a stilare un elenco dei comportamenti a rischio, potremo individuare due grandi tipologie di problematiche: lato uomo e lato azienda.

Problematiche “lato uomo”

- Dipendente negligente o inconsapevole
- Dipendente scontento
- Sono tutti comportamenti riconducibili all'utente curioso, smanettone, appassionato di gadget, collezionista di musica o film, con motivi di rancore, attratto da facili guadagni

Problematiche “lato azienda”

- Problemi organizzativi
- Mancanza di policy
- Mancata applicazione o controllo delle policy
- Differenti livelli di applicazione delle policy (il dirigente che...)

Comportamenti errati legati a fattori provenienti dall'esterno

- Accesso non controllato alla rete da parte di visitatori esterni (su pc aziendale o con proprio notebook connesso alla rete)
- Accesso remoto (portale, intranet, shell, remote desktop,...) e road warrior
- Notebook personale del dipendente portato in azienda
- Uso improprio del notebook aziendale dato in uso

Comportamenti errati legati a Internet

- Navigazione “selvaggia” (distrazione dai propri compiti, siti malevoli)
- Social networks (disseminazione di informazioni; whaling)
- Tecniche di Ingegneria sociale (phishing, ecc.)
- P2P (reati sul copyright, virus)
- Instant Messaging (worm, virus, altre vulnerabilità)

Comportamenti errati legati all'uso di dispositivi connessi al PC

- Chiavette personali portate da casa
- Utilizzo masterizzatori (film, musica, giochi)
- Dischi esterni (beh, se il DVD non basta...)
- Telefonini (bluetooth, infrarossi, usb)
- Modem umts (per superare filtri)
- Ipod, lettori mp3
- Macchine fotografiche

Comportamenti errati legati a negligenza o ignoranza

- Documenti importanti su pc non sottoposti a copia
- Antivirus scaduti
- Dispersione dei documenti sulle postazioni utente
- Scarsa o inesistente prevenzione (controllo dei supporti, scansioni antivirus,...)
- Installazione di software, modifica di configurazioni
- Violazione consapevole o no delle policy

Problemi di Policy

- Pratiche di gestione errate (p.e. flusso delle informazioni)
- Scarsa attenzione generale alla sicurezza
- Nessuna policy di sicurezza
- Nessun controllo viene effettuato

Regole chiare e formazione

- Redigere Regolamento e policy,
- Prevedere corsi di Formazione
- Effettuare verifiche puntuali
- Rendere consapevoli gli utenti

- Deve indicare chiaramente cosa è consentito fare e cosa non lo è con il computer aziendale.
- Se ed in che misura ne è consentito l'uso personale.
- Come deve essere utilizzata la e-mail aziendale.
- Le Best Practice per la sicurezza aziendale.
- I controlli effettuati per la verifica del rispetto delle norme di sicurezza.

Ma è fondamentale che:

- Il regolamento sia rispettato anche dai capi.
- Tutti devono partecipare ai momenti di formazione!

Come pretendere il rispetto di una regolamento se proprio chi lo emana non lo rispetta per primo?

- Dal punto di vista tecnico esistono numerose misure che possono essere messe in atto per mitigare i rischi derivati da comportamenti errati degli utenti.
- Il problema che ogni misura messa in atto troverà qualcuno abbastanza furbo (o abbastanza ... *furbo*) da riuscire a superarla (Murphy docet).

A livello utente

- Protezione notebook
 - Crittografia; aggiornamenti costanti.
- Road warrior, utenti occasionali
 - Separazione delle reti; NAC.
- Utenti
 - Minimum right; livelli di autorizzazione.
 - Proteggere account amministratore locale
- Supporti esterni
 - Disabilitare porte USB e masterizzatori.
 - Oppure impostare rigide misure per l'utilizzo controllato.

A livello di Internet

- Navigazione
 - Blacklist e whitelist
 - Filtri su contenuti ed allegati
 - Blocco dei protocolli indesiderati
- Posta elettronica
 - Verifica dell'uso personale
 - Eventuale uso di marcatori e strumenti per il riconoscimento dei documenti riservati

Il compito del professionista

Consigliare e seguire il cliente:

- dal punto di vista tecnico
- dal punto di vista organizzativo
- dal punto di vista “legale”.
- Senza sostituirsi alla figura del consulente legale, deve quanto meno conoscere le norme e la portata della loro applicazione o disapplicazione (vedi recenti modifiche alla 196/2003, la legge 231/2001, le modifiche al codice penale, le norme sul documento informatico, la PEC, ...)

Riprendiamo le nostre domande iniziali

- Sai quali informazioni esistono in azienda?
- Sai dove sono le tue informazioni?
- Sai chi vi accede?
- Hai dato un valore alle tue informazioni?
- Hai valutato cosa comporta perdere o divulgare informazioni?
- Cosa intendi per “informazione”?

Calcolare i costi della NON sicurezza

- Presentare i problemi di tipo fiscale, penale, di immagine.
- Quantificare i fermi lavorativi.
- Valutare i danni legati al furto di informazioni sensibili (p.e. i costi della materia prima, gli accordi particolari, ...)
- Individuare i costi di ripristino.
- Portare a sostegno numeri e fatti, raccolti mediante compilazione di “rapporti di incidente”

- Ricordare che il professionista non potrà operare da solo.
- Dovrà coinvolgere la direzione e formare un gruppo di lavoro.
- Solo con il coinvolgimento, l'avallo ed il sostegno convinto della direzione sarà possibile raggiungere i risultati prefissi.

- Lo studio di Computer Security Institute

<http://www.gocsi.com/>

- Cisco: Data leakage worldwide: The high cost of the insider threats

<http://cisco.com/en/US/netsol/ns895/index.html>

- IDC White Paper - Combating the Insider Threat & Securing Privileged Passwords

<http://www.cyber-ark.com/constants/white-papers.asp>

- McAfee: le minacce interne. Studio ILM Research

http://www.zerounoweb.it/index.php?option=com_docman&task=doc_details&gid=155&origin2=dett

http://www.mcafee.com/us/local_content/reports/does_size_matter_en_v2.pdf

- ISACA, su ROI e ROSI

<http://www.isacaroma.it/html/newsletter/node/466>

- The threat within volume 2: data loss disaster

https://secure.nai.com/us/local_content/white_papers/wp_dlp_threat_within.pdf

Grazie per l'attenzione!

<http://blog.solution.it>

paolo.giardini@aipnet.it