I-ware Lab II

presenta

La convergenza tra informatica e telecomunicazioni in azienda

ISO 27001 nelle PMI

Appunti da casi reali

Alessandro Fiorenzi

a<punto>fiorenzi<at>infogroup<punto>it

Infogroup S.p.A: Security Management ,TLC e Sicurezza per Gruppo Banca CR Firenze

CTU Tribunale Firenze, Specialista in Informatica Forense

Firenze 3 ottobre 2007

ENTE CASSA DI RISPARMIO DI FIRENZE

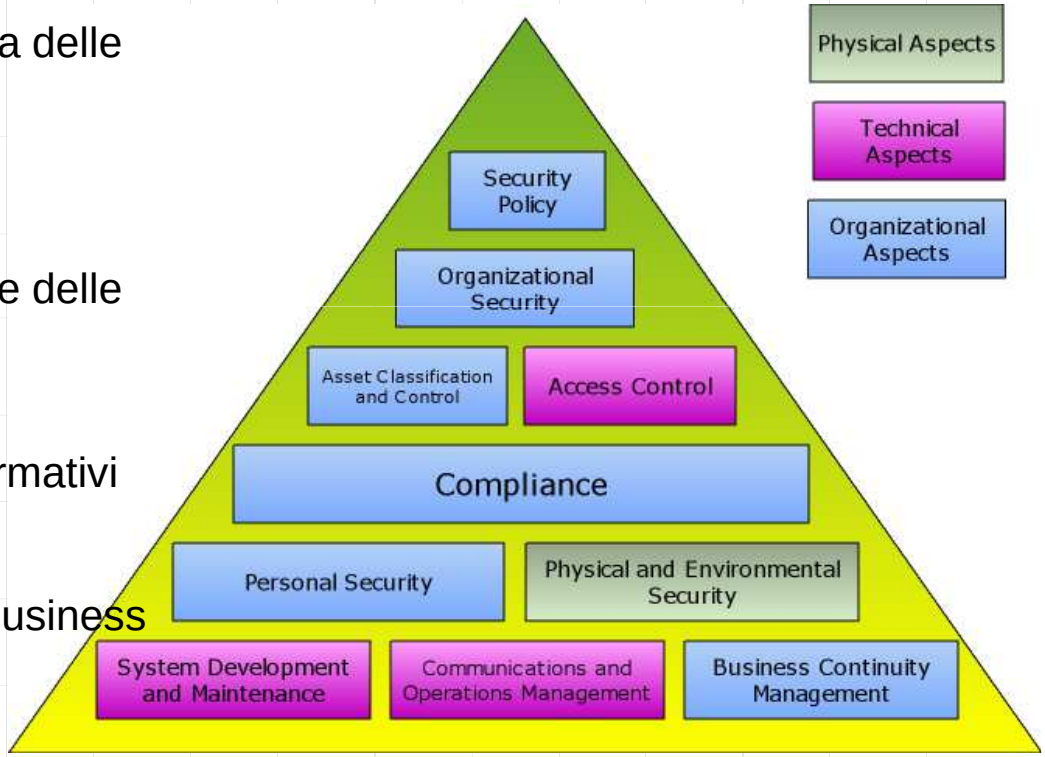
FIRENZE TECNOLOGIA

COSEFI - Consorzio Servizi Formativi alle Imprese ASSINDUSTRIA FIRENZE

INFOGROUP S.p.A. Informatica e Servizi Telematici

Le Aree ISO 27001

- Politica di sicurezza
- Organizzazione della sicurezza delle Informazioni
- Gestione dei beni
- Sicurezza delle risorse umane
- Sicurezza fisica e ambientale
- Gestione delle comunicazioni e delle operazioni
- Controllo Accessi
- Acquisizione, sviluppo e manutenzione dei sistemi informativi
- Gestione degli incidenti della sicurezza delle informazioni
- Gestione della continuità del business
- Conformità



I Ware Lab

ISO 2700x

No a:

montagne di regole che bloccano, rallentano il business dell'azienda

Si a:

Sicurezza Informatica: "l'adozione di misure tecniche e organizzative per salvaguardare la riservatezza, integrità e disponibilità dei dati e quindi del business"

Inserire la sicurezza informatica in azienda da: Affidabilità, Certezza e Continuità all'Attività dell'Azienda

Maggiore solidità del business aziendale e processi più snelli e rapidi

Modello di Gestione

- Plan – Do- Check- Act in sintonia con le 11 aree ISO
  - Plan
    - Quale livello di sicurezza vogliamo per i nostri dati, per il nostro business?
  - Do
    - E' l'ora di sviluppare i piani in strumenti e processi, dove non ci sono gli strumenti ci possono essere le policy
  - Check
    - Controlliamo periodicamente se il livello pianificato è stato raggiunto o no
  - ACT
    - Lo sforzo fatto per ora è sufficiente?, sono raggiunti gli obiettivi della fase "Plan"
    - Vogliamo fare di più ?, possiamo fare di più ? Cosa?

Policy di sicurezza

- E' una linea guida all'utilizzo dei sistemi informatici aziendali
  - Pdl/server/cellulari/palmari: regolamentarne l'uso
  - Supporti Magnetici: come viene gestita la dismissione o la riparazione
  - Utilizzo rete aziendale
  - Utilizzo della rete Internet (cosa si può e cosa non si può fare p.e home banking)
  - Utilizzo della posta Elettronica (non usarla su newsgroup o mailing list)
  - Etc..

Organizzazione della sicurezza delle Informazioni

- Ruoli e funzioni: dovrebbe esserci già
  - Chi all'interno dell'azienda può fare cosa: il mansionario/incarico
  - Documentazione dei processi in carico a un ruolo/funzione

Controllo Accessi

L'ufficio personale è corretto acceda ai documenti del marketing?

L'accesso ai dati, deve
essere regolato in ragione del ruolo
o funzione all'interno dell'azienda

Gestione dei beni

- Cosa sono i beni o asset aziendali?
  - Strumenti logici/fisici (pdl, server,software)
  - Dati logici/fisici (database, nastri dischi)
- Quali sono gli asset importanti per il nostro business?
  - Mettiamo delle priorità su gli asset da proteggere: prima i dati e poi l'hardware, i dati sono il cuore dell'azienda una volta perso non si recuperano, l'hardware si
- Quale è il livello di rischio a cui gli asset sono esposti?
  - possiamo accettare che un server si fermi e che in 36 ore ce lo sostituiscano? O vogliamo di più?
  - siamo disposti ad accettare di perdere i dati e doverli recuperare da un backup di 10 giorni prima o vogliamo avere una maggiore reattività?

Conformità normativa

Tutto quello che abbiamo definito fino ad ora deve rispettare la legge

Diritto Penale
Diritto Civile
Testo Unico Privacy 196/03
Resp. Amministrativa Dlgs. 231/01
626/94 Sicurezza sui luoghi di lavoro
Legge 300/70 Statuto lavoratori
Norme dei paesi in cui l'azienda opera
Direttive Abi/Banca Italia
Etc…

Sicurezza delle risorse umane

Il fattore umano può essere un anello debole della catena di sicurezza:

- Social Engeneering,
- Virus,spyware,phishing
- Foto, mp3,p2p, skype, chiavette usb
- Uso non conforme degli strumenti aziendali
- Etc…

Educare alla sicurezza i propri dipendenti e collaboratori:

- Responsabilizzare i collaboratori: i dati gestiti rappresentano la linfa vitale dell'azienda
- Gli strumenti aziendali servono per svolgere il proprio lavoro e non per altre attività
- Un comportamento azzardato può mettere a rischio la riservatezza delle informazioni aziendali, la sicurezza del network aziendali
- Ognuno è responsabile penalmente dei comportamenti illeciti adottati anche in azienda (terrorismo, pedopornografia, copyright, compromissione sistemi informatici, etc…)

Sicurezza Fisica

Nessuno vi sta chiedendo
di costruire fortknox
Ma certamente di proteggere con opportuni valichi le aree dell'azienda in cui sono registrati i dati e le aree in cui sono presenti i terminali

Gestione Sistema Informativo 1/3

Servono linee guida che definiscano un modello di gestione delle componenti del sistema informativo

- Policy di accesso alle risorse internet, posta, fileserver, (Vedi i ruoli e i diritti di ogni ruolo)
- Policy di configurazione e installazione server e pdl
  - Le installazioni di default sono un pessimo strumento di sicurezza : semplicemente cambiando la directory c:\windows in c:\azienda
  - Configuriamo correttamente il backup per avere i dati aggiornati agli ultimi n-giorni
  - Configuriamo correttamente l'antivirus per non avere problemi con aggiornamenti non scaricati
  - Patch management: Sistema Operativo e software applicativi
  - etc…)
- Policy di Hardening dei sistemi server e pdl ovvero mettere in sicurezza i pdl e i server con i relativi servizi attraverso opportune configurazioni
- Policy di Firewalling
- IDS/IPS

Gestione Sistema Informativo 2/3

Mantenere La SEMPLICITA’

Un’architettura semplice si ha minori costi di gestione

Non esistono Prodotti che fanno tutto

Il costo non è un sinonimo di qualità (mailscanner)

Esistono molte soluzioni OpenSource di ottima qualità

Gestione Sistema Informativo 3/3

- ogni scela tecnica o organizzativa deve rispondere a principi di tutela di:
  - Confidenzialità

    la protezione dei dati e delle informazioni scambiate tra un mittente e uno o più destinatari nei confronti di terze parti (cifratura)
  - Integrità

    la protezione dei dati e delle informazioni nei confronti delle modifiche del contenuto effettuate da una terza parte (hash md5/sha1)
  - Disponibilità

    la prevenzione della non accessibilità, ai legittimi utilizzatori, sia delle informazioni che delle risorse, quando informazioni e risorse servono

Comunicazioni e Operazioni

Non dobbiamo inventare niente di nuovo: solo aggiungere al nostro modo di lavorare il concetto di sicurezza

La Sicurezza è un tassello che si aggiunge ai processi aziendali in essere

Le scelte aziendali devono essere condotte valutando il rischio, anche indiretto, che ne può derivare per i dati dell'azienda

Anche i rapporti con fornitori devono essere improntati a principi di sicurezza quando questi accedono ai nostri dati (p.e. la manutenzione dei pdl o dei server, i dischi contengono i nostri dati)

Business Continuity Plan

Non riguarda solo le grandi aziende.

Tutte le aziende si possono trovare con un problema che ne blocca l'operatività: p.e. la mancanza di corrente elettrica

Il BCP è il piano con cui l'azienda si prepara a fronteggiare incidenti come gli incendi, i terremoti per mantenere la continuità operativa

Ma quanto mi costa? 1/2

La sicurezza è oggi irrinunciabile, come l'airbag in una auto

Dati CSI Survey 2007:

- Incidenti
  - Il 46% delle aziende ha avuto almeno
- un problema di sicurezza negli ultimi
- 12 mesi
  - Il 41% ha avuto da 1 a 5 incidenti
  - Il 11% ha avuto da 6 a 10 incidenti
  - Il 26% più di 10 incidenti
  - Il 10% non lo sa
- Perdite di denaro dovute ad attacchi in $
  - $ 21.124.750 Frodi Finanziari
  - $8.391.800 Virus e Spyware
  - In media un'azienda usa perde nel 2007 $ 345.000

Ma quanto mi costa? 2/2

Per ridurre i costi legati alla sicurezza :

- Formazione del personale
  - seminari, workshop, etcc.
- Monitoraggio dei sistemi
  - Non tutti si possono permettere Operation Manager di Microsoft ma tutti possono installare con linux un log server in modalità syslog e registrare gli eventi anche dei sistemi Widnows con NT-Syslog tutto software OpenSource
- Verifiche della sicurezza periodiche
  - Fatte da personale interno se ci sono le competenze
  - Fatte da consulenti/aziende esterne soprattutto quando c'è necessità di riportare lo stato di sicurezza a terzi
  - Metodologia Standard, con valutazione del rischio (OSSTMM)
- Outsourcing della sicurezza
  - Gestione dei sistemi di sicurezza perimetrale
  - Gestione dei sistemi di backup e antivirus
  - Monitoraggio dei sistemi
  - Alerting in caso di infrazioni ai sistemi (RTSM)

Cosa è un Incidente Informatico

Con questo termine si identifica generalmente un tentativo, riuscito o no, di sfruttare una o più vulnerabilità allo scopo di penetrare i sistemi attaccati, o condizionarne il funzionamento.

Gli incidenti possono essere causati da individui, da virus o altri programmi maliziosi, o da difetti del software che si manifestano in particolari condizioni di funzionamento.

Tipi di Incidente Informatico

- Attacco al sistema informativo
  - Virus, spyware, keylogger etc…
  - Attacco a server pubblici posta web etc…
- Attacco al know-how aziendale
  - Furto informazioni di server interni
  - Diffusione di documenti riservati progetti, forniture esclusive etc..
  - Modifica dati aziendali

Gestire e analizzare un Incidente

Non è un compito da amministratori di sistema

Sono richieste competenze di anali forense

Meglio avvalersi di consulenti forensi esterni

Azioni:

- Analizzare le circostanze e i sistemi coinvolti
- Congelare le evidenze secondo standard forensi riproducibili in sede giudiziale
- Coinvolgere la Polizia delle Telecomunicazioni
- Esposto alla Procura della Repubblica in caso di illeciti civili, penali o del lavoro.

Incidenti Informatici

- Tenere traccia di tutti gli incidenti per una valutazione delle misure adottate
- Sensibilizzare il personale a non sottovalutare gli incidenti occorsi
- Fare un'analisi dei motivi scatenanti degli incidenti informatici in ottica PDCA

Domande?

Grazie

Alessandro Fiorenzi

a<punto>fiorenzi<at>infogroup<punto>it