Circolo dei giuristi di Lugano

La sicurezza informatica nello Studio legale

Silvano Marioni, CISSP

Lugano, 21 novembre 2007

La sicurezza segue le tecnologie

Nei prodotti di massa gli aspetti di sicurezza vengono dopo l'evoluzione della tecnologia

Il progetto della sicurezza

- La sicurezza non è un prodotto ma un processo
  - La sicurezza informatica non concerne la tecnologia ma i rischi e i differenti modi di gestirli
- La sicurezza è una catena con la criticità dell'anello più debole
  - È necessario pensare alla sicurezza con una visione globale considerando tutte le componenti che garantiscono la sicurezza
- I temi fondamentali sulla sicurezza non cambiano nel tempo
  - È importante identificare i concetti di sicurezza che restano immutabili nel tempo e adattarli ai cambiamenti delle situazioni

Le basi della sicurezza

Anti-Blocking-System

La tecnologia

È una componente importante per facilitare e automatizzare la protezione dei beni

Le basi della sicurezza

I processi

Sono le regole che definiscono quali sono gli obiettivi di sicurezza
e come bisogna comportarsi nelle diverse situazioni

Legge federale sulla circolazione stradale
(LCStr) **741.01**

del 19 dicembre 1958 (Stato 1° maggio 2007)

L'Assemblea federale della Confederazione Svizzera,
visto gli articoli 34ter, 37bis, 64 e 64bis della Costituzione federale[1;2]
visto il messaggio del Consiglio federale del 24 giugno 1955,
decreta:

Titolo primo: Disposizioni generali

Art. 1

Campo d'applicazione

[1] La presente legge disciplina la circolazione sulle strade pubbliche, come anche la responsabilità civile e l'assicurazione per i danni cagionati dai veicoli a motore o dai velocipedi.

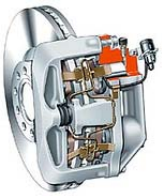
Le basi della sicurezza

Le persone

Sono l'elemento fondamentale per la sicurezza, per la capacità di comprendere, valutare e decidere in situazioni nuove o impreviste

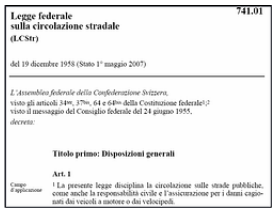
La sicurezza efficace

tecnologia



+

processi



Legge federale
sulla circolazione stradale
(LCStr)

741.01

del 19 dicembre 1958 (Stato 1° maggio 2007)

L'Assemblea federale della Confederazione Svizzera,
visto gli articoli 34quinquies, 37ter, 64 e 64bis della Costituzione federale[1];
visto il messaggio del Consiglio federale del 24 giugno 1955,
decreta:

Titolo primo: Disposizioni generali

Art. 1

Campo d'applicazione

[1] La presente legge disciplina la circolazione sulle strade pubbliche, come anche la responsabilità civile e l'assicurazione per i danni cagionati dai veicoli a motore o dai velocipedi.

+

persone

Che cosa è la sicurezza informatica

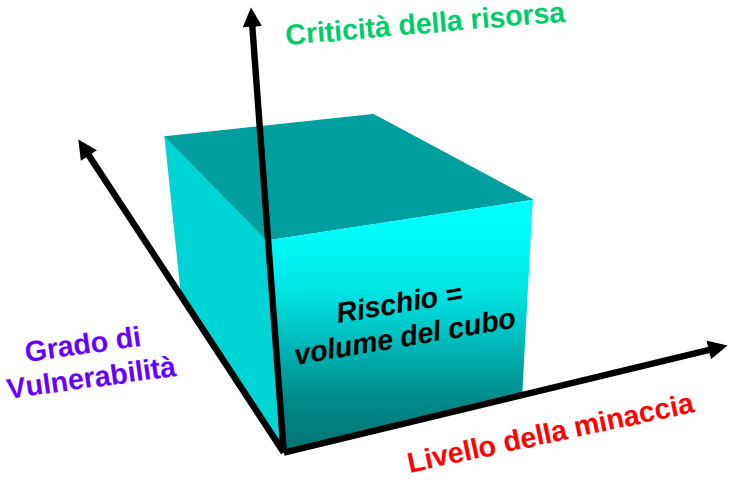
- La sicurezza informatica è la protezione
  - dei sistemi informativi,
  - dei dati,
  - dei servizi
- per prevenire o fronteggiare eventi di natura dolosa, colposa o ambientale
- in modo da ridurre al minimo il rischio di eventualità e/o impatto di un incidente

Che cosa è il rischio

- Il rischio è una funzione della **probabilità** di una **minaccia** che risulta favorita da una **vulnerabilità,**
  e l'**impatto** che questo evento negativo ha su una **risorsa**

Rischio = f(Probabilità, Impatto)

Quantificare il rischio



Tipi di rischi

	persone	processi	tecnologia	ambiente
interni	errori, uso illegale del software, frodi, spionaggi, hacker	fughe di notizie, procedure incomplete, ruoli e responsabilità non chiari	guasti hardware, problemi software, accessi non autorizzati	incendio, animali nocivi
esterni	ricatti, hacker, social engineering, accessi non autorizzati, phishing	problemi con fornitori e/o outsourcer, problemi legali o di regolamenti	cadute di corrente, problemi di telecomunicazione, virus, attacchi	allagamenti, terremoti, attentati

Ieri: attacchi fatti per farsi notare

- ATTENZIONE:VIRUS NON RILEVABILE SUBITO DA NORTON
- Informiamo tutti coloro ai quali abbiamo certamente spedito della posta nei mesi passati che il virus "sulfnbk" è stato trovato nel ns. disco rigido ma non è stato attivo fino ad oggi. Esso è programmato per divenire attivo: A causa del ritardo di attivazione esso non è rilevabile dai comuni antivirus quali McAfee o Norton.
  Quando diventerà attivo sopprimerà tutti i file e le cartelle del vs. disco fisso. Il virus si propaga per e-mail e s'infiltra nel disco C: \WINDOWS\COMMAND.

  Per trovarlo e sopprimerlo seguite le istruzioni seguenti:
  cliccate su AVVIO, scegliete TROVA, scegliete FILE O CARTELLE
  andate a "CERCARE IN" e selezionate "DISCO FISSO (C)“
  sulla linea del nome del file scrivete: SULFNBK.EXE
  se il programma viene trovato cliccatelo col tasto destro MA NON APRITELO!!!!
  nel menù FILE cliccate "ELIMINA“
  chiudete la finestra "risultato della ricerca“, Vuotate il cestino

  Ora siete al sicuro, ma la cattiva notizia è che se avete trovato tale file sul vostro computer, rischiate di aver contaminato coloro a cui avete mandato e-mails da molti mesi.

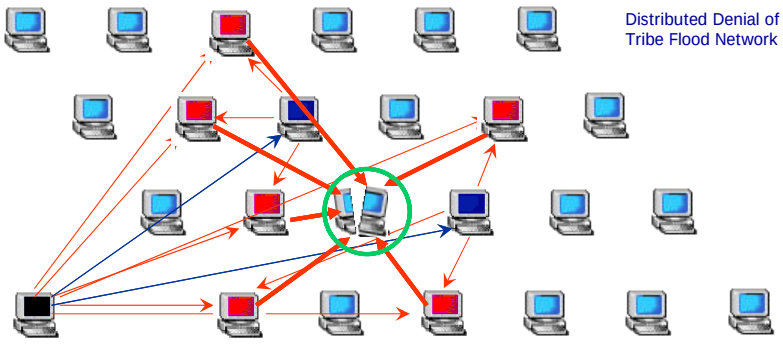
Oggi: attacchi nascosti (e rassicuranti)

- Gentile utente abcd@xyz.ch,
  sono l'avvocato Gianluca Gentili titolare dell'omonimo studio Legale, mi trovo costretto a riscriverle perchè continuano ad arrivarmi dal suo indirizzo email abcd@xyz.ch messaggi dal contenuto sconveniente.
  Non sono un esperto in materia, tuttavia il sistemista del nostro studio sostiene che questi invii da parte sua sono probabilmente involontari e causati da un worm informatico. Dice inoltre che è possibile rimuovere questo worm con il software antivirus scaricabile dall'indirizzo www.xxx.com
  Io non ho né le competenze né il tempo per verificare l'esattezza di questa supposizione, purtroppo mi trovo costretto a DIFFIDARLA dal continuare questi invii offensivi alla mia posta di lavoro. Se riceverò UN SOLO ALTRO MESSAGGIO di questo genere procederò a denunciarla senza ulteriore avviso.
  Le ricordo che i reparti di polizia informatica hanno i mezzi per risalire alla vera identità del proprietario di un indirizzo di posta, per quanto registrato con dati di fantasia o internazionale. Per cui non creda di poter continuare a infestare la mia casella email con queste cose.

  in attesa di un suo sollecito riscontro,
  Studio Legale Gentili e soci
  Via Carlo Magno 12
  Parma

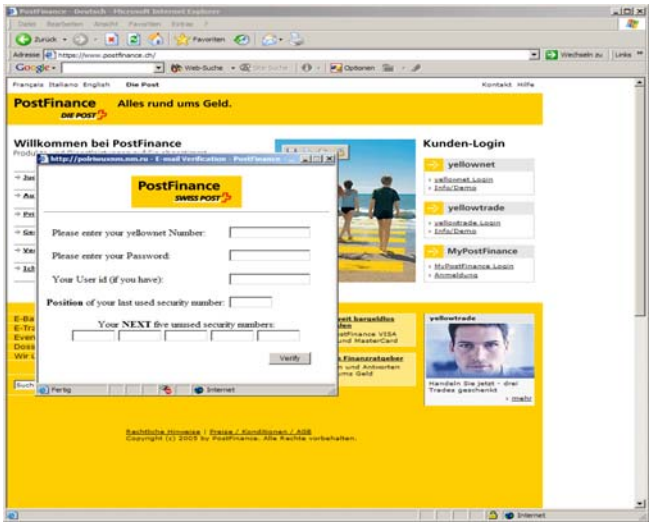
Un esempio di uso dei PC compromessi: le reti Botnet

Per attaccare siti, per inviare spam, per cliccare banner pubblicitari, ecc.

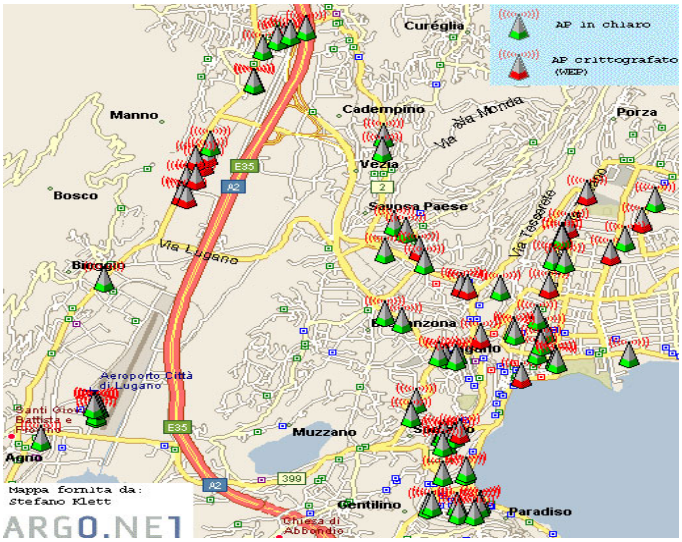


Distributed Denial of Services
Tribe Flood Network 2000

Phishing, un esempio di Social Engineering



La tecnologia da sola non basta



Reti wireless a Lugano

(dati 2004)

Nuovi strumenti di memorizzazione

Chiave USB 8Gbyte Fr. 99.-

Lettore MP3 8Gbyte Fr. 319.-

8 Gbyte corrispondono a:
- 8'000 pagine dattiloscritte
- 3'000 pagine archiviate elettronicamente
- 200 elenchi telefonici

I principali fattori di rischio

- Ignoranza
  - Non si conosce l'esistenza di un particolare rischio o problema
- Indifferenza
  - Si riconosce che il problema esiste ma si è convinti che non ci riguardi
- Due esempi
  - Uso della posta elettronica
  - Controllo accesso al proprio PC

Posta elettronica

- Sistema di comunicazione capillare, rapido e economico
- Limiti tecnologici
  - Il testo del messaggio è in chiaro
  - Il mittente può essere alterato
  - Non si conosce il percorso del messaggio
- Abitudini consolidate
  - Diffusione di messaggi « giocosi »
  - Invio documenti importanti per posta elettronica
- Rischi
  - Occupazione impropria dello spazio disco aziendale
  - Diffusione di programmi malefici
  - Possibili furti di informazioni

Uso della posta elettronica

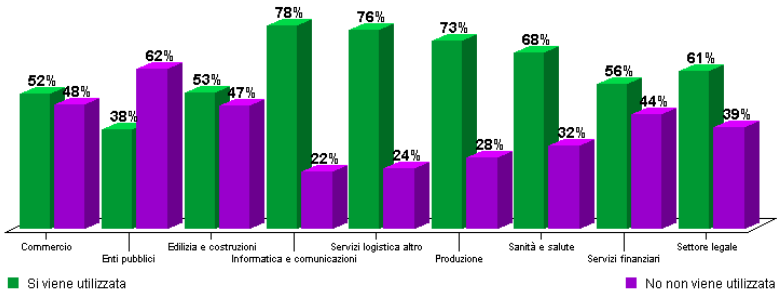


Figura 20 : percentuale di utilizzo della posta elettronica per inviare e/o ricevere documenti aziendali importanti suddivisa per settore di attività

Controllo accesso al proprio PC

- Identificarsi come utente utilizzando la password di accesso
- Limiti tecnologici
  - È possibile non autenticarsi (non usare la password di accesso)
  - Nessun contesto operativo diverso tra utente amministratore e utente normale
  - Alcune applicazioni richiedono l'utente amministratore
- Abitudini consolidate
  - Non usare la password o usare una password debole (o su bigliettini)
  - Lavorare come utente amministratore
- Rischi
  - Accesso al PC da parte di terzi
  - Maggiore vulnerabilità ai codici malefici

Misure tecniche di sicurezza

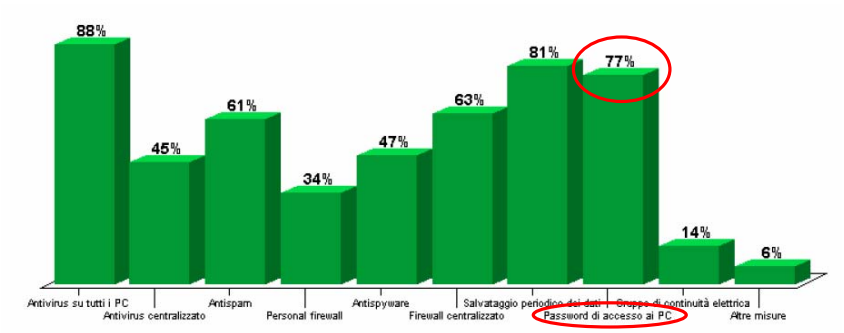


Figura 29 : percentuale delle misure tecniche previste per l'infrastruttura informatica aziendale
(Il totale della percentuale supera il 100% perché la domanda permetteva scelte multiple)

Come proteggersi: utilizzare correttamente gli strumenti tecnici

- Sicurezza fisica
  - Apparecchiature in aree protette, controllo accessi fisici
  - blocco chassis, cavo antifurto
- Controllo dell'accesso alle risorse
  - Identificazione, autenticazione e autorizzazione
  - Abilitare le password di sistema
  - Abilitare la password a livello hardware
  - Mettere una password di avvio e eventualmente cifrare i dischi per i PC portatili
- Salvataggio dei dati
  - Fare regolarmente il backup dei dati, gestione dei supporti di dati, (archiviazione, etichettatura, distruzione)
  - Organizzare i dati in modo centralizzato (server)
- Integrità dei dati, non ripudio
  - Firma elettronica

Come proteggersi: utilizzare correttamente gli strumenti tecnici

- Protezioni dei sistemi
  - Non usare utenti con diritti di amministratore
  - Bloccare l'istallazione di software da parte degli utenti
  - Aggiornare il software con gli ultimi patches
  - Istallare un antivirus e tenerlo aggiornato
  - Istallare un personal firewall
  - Utilizzare un programma anti spam
  - Blocco delle unità esterne (dischetto, USB, ecc.)
  - Configurare correttamente il software
- Protezione del perimetro di rete
  - Firewall, segmentazione, intrusion detection,
- Protezione delle comunicazioni
  - Inviare informazioni critiche in modo cifrato
  - Virtual Private Network

Come proteggersi: definire le regole

- Protezione del posto di lavoro
  - Uso dei mezzi informatici da parte dei collaboratori
  - Uso della password, controllo accesso ai sistemi, ecc.
- Protezione delle informazioni aziendali
  - Proprietà e utilizzo delle informazioni aziendali
  - Trattamento delle informazioni critiche e conformità alla legislazione
- Protezione delle comunicazioni
  - Uso di internet e della posta elettronica
  - Eventualità di possibili controlli

- Diventano importanti
  - I regolamenti aziendali
    - Per definire e controllare i processi aziendali
  - Le leggi
    - Per definire il quadro giuridico delle azioni

Regolamenti sull'uso dei PC per settore

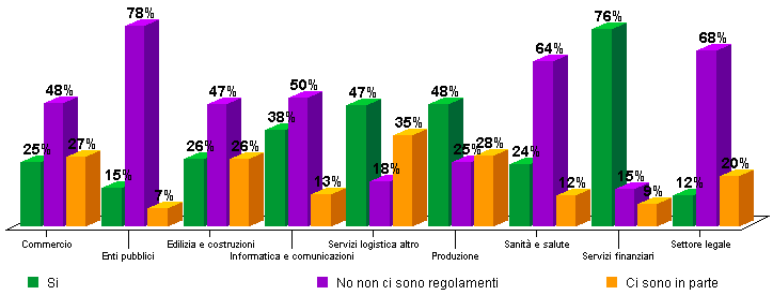


Figura 27 : percentuale di aziende con regolamenti che disciplinano l'uso dei PC e di Internet da parte dei dipendenti suddivisa per settore di attività

Regolamenti sull'uso dei PC per dimensione

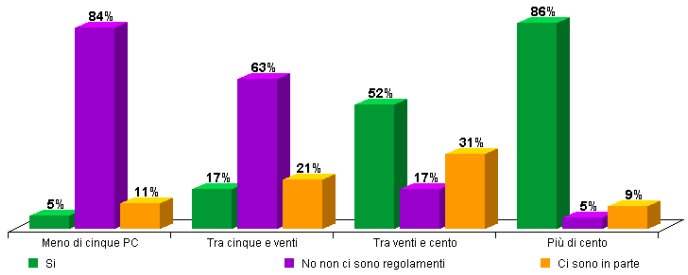


Figura 28 : percentuale di aziende con regolamenti che disciplinano l'uso dei PC e di Internet da parte dei dipendenti suddivisa per dimensioni

Come proteggersi: conoscere per reagire

- Conoscere
  - Essere a **conoscenza** e **consapevoli** dei rischi che si possono incontrare
- Capire
  - Saper **riconoscere** le situazioni critiche a rischio
- Reagire
  - Decidere il tipo di **reazione** secondo la situazione
- Diventano importanti
  - Le competenze e i comportamenti del personale
    - Informazione
    - Formazione

Competenze sull'uso dei PC per settore

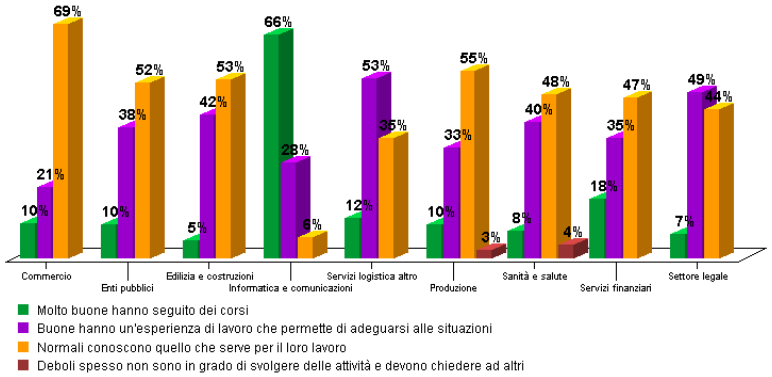


Figura 22 : percentuale sulle competenze dei dipendenti sull'uso dei PC e di Internet suddivisa per settore di attività

Competenze sull'uso dei PC per dimensione

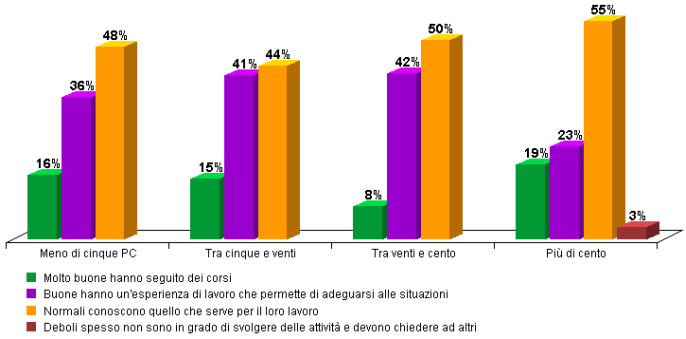


Figura 23 : percentuale sulle competenze dei dipendenti sull'uso dei PC e di Internet suddivisa per dimensione

Conclusioni

Riassumendo

- La sicurezza informatica non concerne solo la tecnologia ma i rischi e i differenti modi di gestirli
- È un progetto che riguarda persone, processi e tecnologia
- Deve garantire che vengano soddisfatti i requisiti fondamentali della sicurezza per ridurre al minimo l'eventualità e/o l'impatto di un incidente

Referenze

- MELANI – Sicurezza dell'informazione
  http://www.melani.admin.ch/index.html?lang=it
- Sicurezza informatica a casa nostra
  http://www.acsi.ch/sicurezza
- Inchiesta SUPSI sulla sicurezza informatica nella Svizzera italiana
  http://www.dti.supsi.ch/isi
- Minacce informatiche dalla A alla Z
  http://www.sophos.it/sophos/docs/itl/marketing_material/sophos-a-to-z_it.pdf