Giornata della Sicurezza Informatica in Sardegna
Mercoledì 5 Novembre 2008
Auditorium Sardegna Ricerche - Pula

Linee guida per la sicurezza informatica nelle piccole e medie imprese

Claudio Telmon – CLUSIT

ctelmon@clusit.it

Clusit
Associazione Italiana
per la Sicurezza Informatica

CLUSIT: gli obiettivi

- **Diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini**
- **Partecipare alla elaborazione di leggi, norme e regolamenti che coinvolgono la sicurezza informatica, sia a livello nazionale che europeo**
- **Contribuire alla definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza**
- **Promuovere l'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà**

I Rapporti Internazionali

In ambito internazionale, Clusit partecipa a svariate iniziative in collaborazione con:

- **...**
- **ENISA (European Network and Information Security Agency)**
- **...**

Attività orientate alle piccole e microimprese

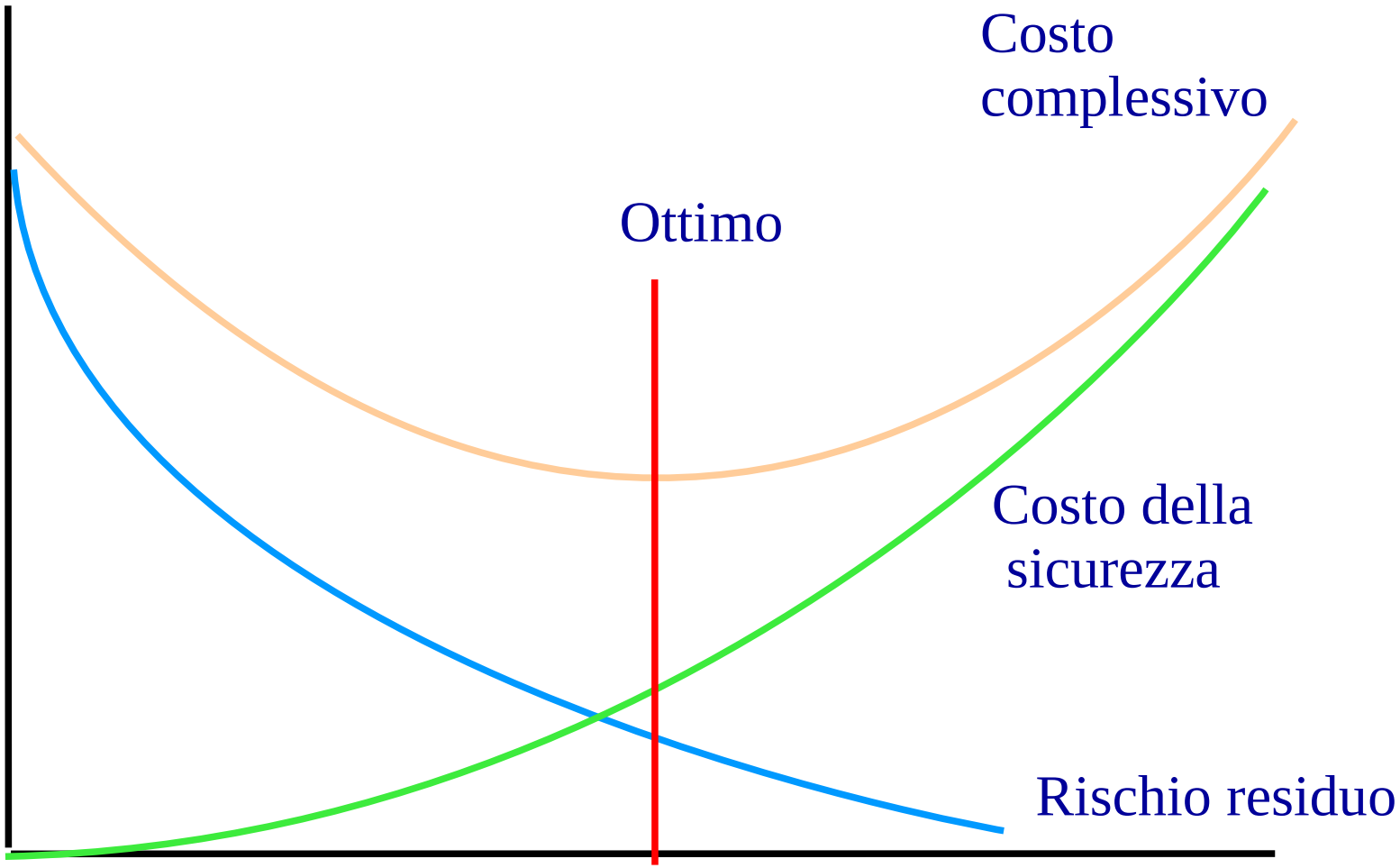
- Gruppo di lavoro ENISA sull'analisi delle esigenze e aspettative delle microimprese
- Opuscolo in fase di pubblicazione con CNA
- Collaborazioni con Confesercenti e Confcommercio (non ancora concretizzate)
- ...

Una conclusione fondamentale: una piccola o microimpresa ha esigenze diverse da quelle di un cittadino/genitore e da una grande impresa

La sicurezza è uno strumento di gestione del rischio

- E' l'imprenditore a conoscere le proprie risorse di valore, ma spesso non lo sa...
- Il rischio è parte dell'impresa, ma:
  - in Europa, per molti la piccola impresa non è qualcosa che deve crescere, ma qualcosa che va bene finché da da lavorare alla famiglia
  - le piccole imprese sono spesso fornitori di imprese più grandi; le esigenze (normative) di gestione del rischio delle grandi ricadono anche sulle piccole; in questi casi non sono nell'interesse della piccola impresa
- La sicurezza non è un problema tecnologico: le tecnologie non mancano

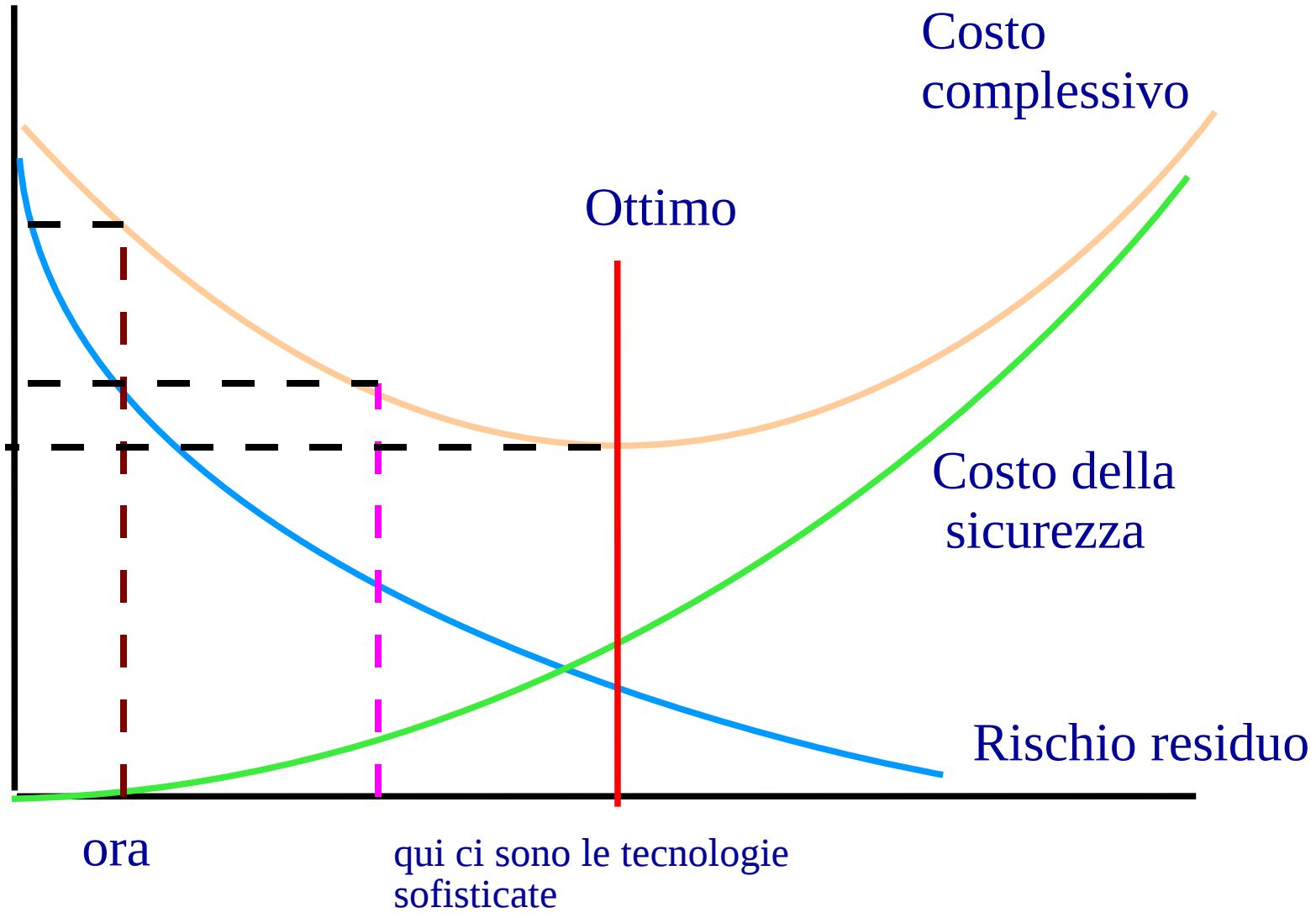
MiniMax


Costo
complessivo
Ottimo
Costo della
sicurezza
Rischio residuo

Problemi del MiniMAx

- Il calcolo del rischio nei sistemi informativi è un concetto teorico
  - per di più è diverso da impresa a impresa
- Gli investimenti devono essere “ottimali”: spendere nella tecnologia sbagliata non riduce il rischio
- A forza di investire, la complessità e quindi il rischio possono aumentare
- Cosa ce ne facciamo dello schema?

MiniMax


Costo complessivo
Ottimo
Costo della sicurezza
Rischio residuo
ora
qui ci sono le tecnologie sofisticate

Il problema della competenza

- Il grafico minimax ha un altro problema con le ME: il costo “minimo” delle competenze
  - è un problema trascurabile per le grandi imprese
  - costituisce un minimo fisso che per una microimpresa è paragonabile alla somma degli altri costi della sicurezza (e dell'informatica in generale)
  - non è facilmente accessibile: le microimprese sono TANTE

Soluzione: lavorare con le associazioni

- Microimprese simili hanno rischi e sistemi informativi simili
- Le loro associazioni imprenditoriali/professionali (o anche i commercialisiti?) possono aiutare a scalare i costi su numeri più grandi
- Lo scambio di informazioni aiuta a stimare i rischi (e non è dannoso per la concorrenza)
- Quindi: non affrontare questi problemi da sole

I punti fondamentali

- Individuare risorse e minacce
- Evitare la perdita accidentale di dati
- Aggiornare i sistemi
- Contrastare i codici maligni
- Separare le attività
- Attenzione alle frodi
- Cautela con la posta e la navigazione
- Protezione della rete locale e wireless
- Conformità alle norme (e gli standard?)
- Cura del comportamento del personale

Individuare risorse e minacce

- **Spesso l'imprenditore non ha chiaro il ruolo degli strumenti informatici nella sua azienda**
- **Le risorse sono informazioni, non i computer, su quelle si investe:**
  - gli elenchi di clienti e fornitori;
  - la rubrica telefonica e gli appuntamenti;
  - la fatturazione;
  - le comunicazioni con i fornitori, ad esempio via posta elettronica;
  - i rapporti con la banca, con l'Agenzia delle Entrate e con altri Enti pubblici;
  - la documentazione per la gestione del personale e per la conformità alle normative;
- **Anche su palmari, cellulari, portatili...**
- **Quali minacce sono realistiche? Non sempre l'imprenditore lo sa, poche le sa il tecnico**
  - **nessuno dei due conosce le probabilità**

Evitare la perdita accidentale dei dati

- Pochi fanno backup regolari
- Meno li gestiscono correttamente
- C'è quasi una cultura di “rassegnazione” favorita dalle frequenti reinstallazioni
- Eppure, si sa che i dischi si guastano...
- Ma anche:
  - si perdono i cellulari
  - si rubano i portatili
  - si rubano per sbaglio anche i backup
  - ...

Aggiornare i sistemi

- Vuole dire “installare gli aggiornamenti”, non “installare l'ultima versione”
  - con la notevole eccezione di Windows 98
  - anzi, le nuove versioni hanno nuovi problemi
- Non solo del sistema operativo, anche delle applicazioni
- Non attivare gli aggiornamenti automatici solo se c'è una vera gestione alternativa
- Mailing list del GARR-CERT
  http://www.cert.garr.it/mailing.php3

Contrastare i codici maligni

- L'antivirus non basta più
  - Antispyware, personal firewall...
- E' importante un componente che intercetti le modifiche al sistema (generalmente antispyware)
- Le suite integrate possono andare bene
  - attenzione ai costi per componenti inutili
  - attenzione al carico del sistema
  - non sono ottimali su tutti i componenti
  - semplificano la gestione
  - non diversificano

Separare le attività

- Forse la singola misura più efficace in assoluto
  - la meno adottata, perché è anche la più scomoda
- Troppe applicazioni fatte male
  - sono cambiati i sistemi ma non gli sviluppatori
  - ma a volte basta correggere dei diritti
  - un compromesso su un'applicazione è meglio che cedere tutti i diritti
- Le applicazioni da ufficio non hanno bisogno di privilegi particolari
- Certo, i giochi e il P2P sono un'altra cosa...

Attenzione alle frodi

- E' più un problema culturale che tecnico
  - riportare il concetto del “mattone” a Internet
  - immaginare di essere turisti in un paese straniero
  - chi si fa imbrogliare nel mondo reale (es. da falsi impiegati) si farà imbrogliare anche su Internet
  - in compenso, su Internet si fanno imbrogliare anche altri
  - ragionare bene su qualsiasi cosa che chieda informazioni e soldi
  - comunque le frodi non si eliminano

Cautela con la posta e la navigazione

- Sono i canali principali attraverso cui adesso sono attaccate le piccole imprese
  - a meno di usi “promiscui” come il p2p
- Evitare le eccessive integrazioni se non sono necessarie
  - possono essere utili i plug-in che aumentano i controlli
- Imparare i “segnali” del browser
- Valutare di appoggiarsi a fornitori
  - es. per la posta
  - evitare i tecnofili entusiasti ;)

Protezione della rete locale e wireless

- Firewall e personal firewall sono ormai in tutti i router/modem e S.O.; si tratta di usarli
- E' attiva (e a volte usata) anche molta connettività wireless:
  - Wi-Fi
  - bluetooth
- Anche qui, si tratta di configurare quello che c'è e disattivare quello che non si usa

Conformità alle norme

- Le norme sono scritte spesso con in mente grandi aziende e contesti specifici
  - alle piccole imprese capitano fra capo e collo
  - emblematica l'evoluzione della normativa sul trattamento dei dati personali
- Aziende simili hanno problemi simili
  - di nuovo, sfruttare le associazioni
- Conformità a norme e standard derivano anche dall'essere fornitori
  - anche gli standard sono pensati nell'ipotesi di una disponibilità illimitata di competenze
  - o disponibilità di personale...

Cura del comportamento del personale

- In una piccola impresa non c'è posto per politiche complesse
- Servono:
  - chiarezza, condivisione, commitment
  - la politica scritta serve come tutela legale
- Preparazione del personale
- E' necessario ricordarsi che i ruoli sono meno definiti
- Social engineering: è un problema, ma le lene riescono a imbrogliare anche gli imbroglioni...

Grazie!