“Incontro sulla sicurezza informatica”

Modena, 16-11-2011

Michele Colajanni
Università di Modena e Reggio Emilia
michele.colajanni@unimore.it
http://weblab.ing.unimo.it/people/colajanni

Agenda

1. Attaccanti
2. Come proteggere le persone
3. Come proteggere i sistemi
4. Proposte per l’Università

“Conoscere i propri nemici”

Conoscere gli attaccanti

- HACKER
- CRACKER
- LAMER
- BLACK HAT
- WHITE HAT
- SCRIPT KIDDIES
- MAFIA BOY
- NERD
- CYBERPUNK
- HACTIVIST
- CYBERTERRORIST
- …

ATTACCANTI ESTERNI

Motivazioni

Curiosità
Sfida
Ideologia
Vendetta
Vandalismo
Guadagno
Spionaggio
Controllo sociale
Cyberwar
…

Motivazioni (*per esterni*)

Curiosità
Sfida
Ideologia
Vendetta
Vandalismo
Guadagno
Spionaggio
Controllo sociale
Cyberwar
…

Motivazioni degli hacker “old style”

- Principî hacker
- Sfida, anche se …
  - Pochi veri hacker individuano e sfruttano vulnerabilità precedentemente sconosciute
  - La stragrande maggioranza ripete attacchi noti e documentati
- Fama all’interno di “circoli”
- Soggetti dediti ad ideare codici in grado di infettare le risorse presenti nella Rete
- C’è qualche traccia di **antisocialità** non di vera **criminalità** (anche se alcuni sono perseguiti)

Dall’hacking all’Ethical hacking

Il confine è molto labile e discutibile

1. Allo scopo di prevenire il crimine
   - entrano nelle reti, superano le barriere
   - individuano le vulnerabilità
2. Avvisano la “vittima”
3. Molte volte non vengono ascoltati, altre volte vengono minacciati o offesi. E allora “tendono ad arrabbiarsi”:
   - alzano il livello dell’attacco
   - pubblicano le vulnerabilità che hanno scoperto

Evoluzione – *secondo passo*

Anni ’90: *Crackers, Internet vandals, Black hats*

- Prevalentemente giovanile
- Spesso malintenzionata, ma non per denaro
  - Intrusioni nei sistemi
  - Scrivono e diffondono malware
  - Penetrano i sistemi informatici con uno scopo (che non è solo quello di "testare" il sistema, anzi…)

Evoluzione – *terzo passo*

A cavallo del 2000, si diffondono:

- **Professionisti del cybercrime**
  - “I giovani sono cresciuti: questo è il loro lavoro”
  - La motivazione è essenzialmente economica
- **Attaccanti interni**
  - Attaccanti occasionali ma non per questo meno pericolosi
- **Professionisti di "agenzie statali”**

Situazione molto più pericolosa

Da **attaccanti solitari** a

Piccoli gruppi che lavorano come criminali informatici

Criminalità organizzata che assume e paga bene ragazzi per compiere crimini informatici

Stima 2010: "il conto economico della criminalità informatica (*guadagno* + *danni*) è secondo solo al mercato della droga"

Specializzazioni

- Riciclaggio di denaro sporco
- Truffe
- Furti
  - Denaro
  - Identità
  - Informazioni
- Ricatti
- Spionaggio industriale
- Diffamazione e diffusione di informazioni false
- Creazione e noleggio di *botnet*
- Scrittura e diffusione di software malevolo

Crimine organizzato [Reuter 26/3/2010]

- Studenti, nerd, programmatori e hacker occupano tre piani in Kiev (Ucraina) creando software malevolo
- La società si chiama(va) **Innovative Marketing Ukraine** (IMU), e la principale motivazione del suo business era: infiltrare virus nelle reti delle principali aziende, inserirsi nei computer, acquisire informazioni
- L'azienda aveva il suo Dipartimento di Risorse Umane, il suo call center, le sue gare, feste e gite aziendali
- Gli impiegati avevano forti incentivi sul salario nel caso di successi e quindi risultava un'azienda molto competitiva
- **"Quando hai vent'anni, non pensi molto all'etica del tuo lavoro. Avevo un ottimo salario, molti incentivi e un ambiente di lavoro stimolante"** [Maxim, dipendente IMU]

Fatturati e best seller

- *Best seller*: **scareware** → fa finta di analizzare un computer alla ricerca di virus. In realtà,
  - Acquisisce informazioni
  - Infetta il computer e cancella le funzionalità dei principali antivirus, rendendolo soggetto a intrusioni esterne
  - Per "pulire" il computer, si propone la vendita di uno specifico software a 50$ (che si può acquistare solo mediante carta di credito!)
- Fatturato: $180 milioni nel 2008 operando dalla Ucraina in 25 Paesi
- Costretta alla chiusura dall'FBI

“Difendere se stessi e il personale”

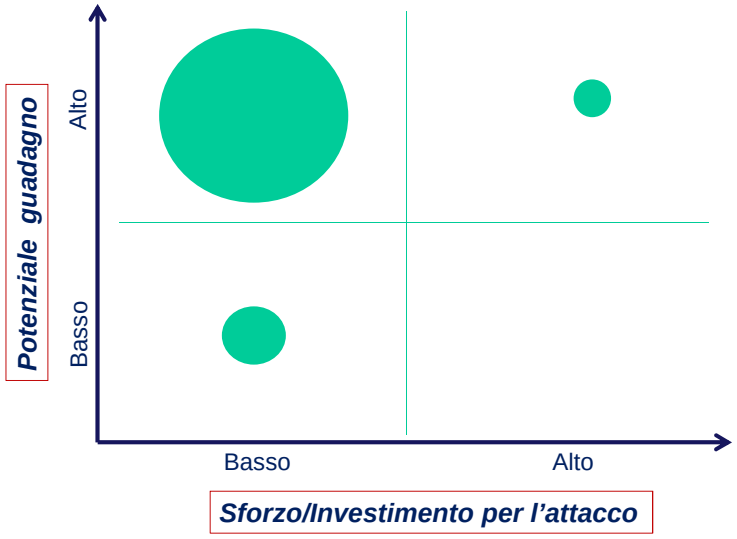
Conseguenza

- Nel momento in cui la maggior parte degli attacchi sono commessi da ***cybercriminali***, **la sicurezza diventa un problema di tipo economico**
  - Quanto l’attaccante è disposto a investire in termini di soldi, tempo e rischi?
  - Quale livello di difesa rende l’attacco non conveniente?
- **E’ più facile attaccare il sistema informatico o il personale?**
  - Social engineering, truffe, corruzione, minacce, …

Obiettivi immediati

1. **Denaro (dei dipendenti)**
2. **Informazione da trasformare in denaro**
   - Idee, Know-how di ricerca e sviluppo
   - Prototipi
   - Informazioni strategiche
   - Informazioni riservate su bandi, gare
   - Informazioni sui dipendenti
   - **Informazioni sanitarie** ←
   - …
3. **Immagine/reputazione dell'organizzazione**

Numerosità degli attacchi



Dark side: "Sappiamo tutto"
Come ci attaccheranno

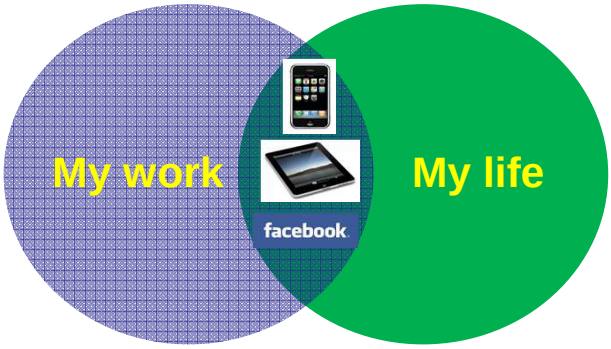
I 5 Scenari più pericolosi
(Horizon threats 2011)

1. **Contingency fails** – fiducia eccessiva in Internet per tutte le transazioni e scarsi investimenti per supportare la crescita e l'affidabilità dell'infrastruttura stessa
2. **The cloud becomes a fog** – si prendono scorciatoie per risparmiare a spese della sicurezza e della conformità
3. **Who took my boundary – il perimetro aziendale è violato dall'installazione di software non autorizzato**
4. **The mobile mainframe in your pocket – predominanza dell'uso ("superficiale") di dispositivi mobili che porta a perdita di informazioni aziendali e frodi**
5. **The avatar effect – mescolamento di vita privata e lavoro che mette a rischio le informazioni aziendali**

Vulnerabilità

- **Uso promiscuo**
  - Si usa un solo dispositivo per qualsiasi scopo. Ma i dati convivono con le applicazioni, abitudini, password, geolocalizzazione, e informazioni di ogni tipo

  →Furto dei dati da parte del cybercrime



Sappiamo tutto

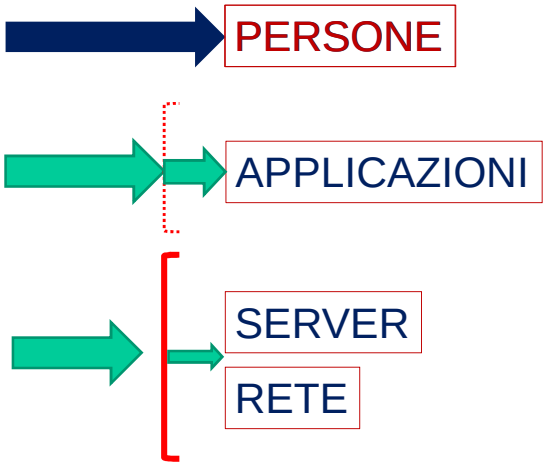
- **La portata delle minacce informatiche esistenti**
- **Il modo in cui vengono sfruttate le tecnologie digitali e i loro utilizzatori per infliggere un danno**
- **Le persone che hanno un ruolo in questo processo criminale**
- Conosciamo i vecchi e i nuovi attacchi:
  - ***Spear phishing***
  - ***Advanced Persistent Threats*** (APT)
  - ***Malware*****: "Chi dura di più, guadagna di più"**
  - **Malware specifico per sistemi mobili**

I numeri della sicurezza (*tecnologia* e *fattore umano*)

96 - 4

4 - 96

Livelli degli attacchi



Tutti gli attacchi sono multi-step e spesso condotti con strumenti diversi

1. **Contatto**
2. **Aggancio**
3. **Controllo** (del computer e/o della persona)
4. **Escalation**
5. **Azione criminale**

Possono essere attacchi mirati o di massa

Principali strumenti per condurre "attacchi di massa"

- **Botnet**
- **Malware**
- **SPAM**
- **Social engineering (*in senso lato*)**

Le botnet più grandi

- **Zeus**: (conosciuta anche come **Zbot**, **PRG**, **Wsnpoem**, **Gorhax** e **Kneber**) → milioni di computer infettati dal 2007 al 2010
- **Storm**: 1.5 milioni di computer zombie
  - XSS reflected (spam mail + social engineering)
  - Storm worm caricato dal click dell'utente
  - Controllo della botnet mediante protocolli p2p
- **Conficker**: la più grande botnet individuata fino a 2009 → da 3.5 a 10 milioni di computer infettati
- **Mariposa**: 12 milioni di computer infettati
- **BredoLab:** botnet Russa, 30 milioni di computer infettati, gestiti da circa 150 server di comando e controllo

Malware

- E' una definizione più moderna e completa del termine più comune ***virus***

MALWARE = MALicious softWARE

Siamo nel periodo del *malware latente*

- **A differenza dei virus tradizionali, che tendevano a manifestarsi, il *malware* moderno è come un parassita latente:**
  - **tende a nascondersi in profondità**
  - **non è facile estirparlo perché tende a riprodursi automaticamente in diversi luoghi e formati**

Vale la regola:

"chi più dura, più guadagna"

Il 90% del malware sviluppato nel 2010 è realizzato a fini di lucro

SPAM è un mezzo per commettere diversi tipi di crimini

Nato per motivi "pubblicitari" su larga scala, oggi lo SPAM è anche uno dei metodi più utilizzati per:

- diffondere malware
- rubare identità (*phishing*)
- tentare frodi e truffe
- acquisire informazioni in modo fraudolento
- indurre a commettere azioni (inconsapevolmente) illegali
- …

Princìpi fondamentali

- Il primo “complice” del truffatore è il “truffato”
- Le truffe funzionano se si riesce a raggiungere la “persona giusta”
- E’ importante provare a raggiungere il maggior numero di persone possibili così da aumentare la probabilità di trovare la “persona giusta” (*grazie e Internet e ai servizi basati su Internet, è facile raggiungere milioni di persone*)

“Persona giusta” – categorie *classiche*

1. Persone “più sensibili” al facile arricchimento
2. Persone con il “fiuto” dell’affare (spendere meno per un bene costoso)
3. Persone “timide”
4. Persone “timorose”
5. Persone in difficoltà economiche e lavorative
6. Persone con difficoltà relazionali
7. Ma anche persone inconsapevoli, fiduciose, ecc.

Per ogni categoria c’è la truffa adatta

Esempi di truffe (non informatiche, ma condotte mediante mezzi informatici)

- Persone che sono “più sensibili” al facile arricchimento → **Scam** (proposta di business trasmesso e percepito non proprio come fraudolento, ma come *border line*)
- Persone che hanno il “fiuto” dell’affare (spendere meno per un bene costoso) → classico **“Pacco”**
- Persone “timorose” → **Mail aggressive**, del tipo “tu hai fatto questo”, “perché non hai fatto quanto promesso”, ecc.
- Persone in difficoltà economiche → **Offerte di lavoro**
- Persone con difficoltà relazionali → **Possibilità di contatti**

Identità digitale

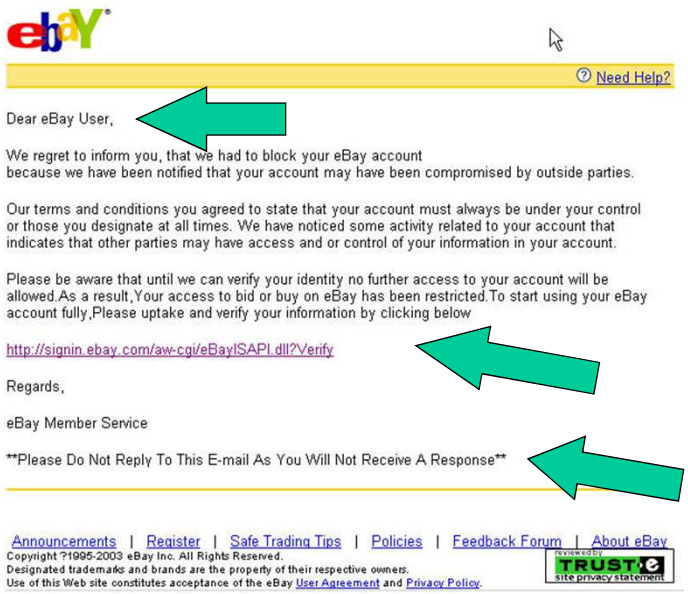
Chi siamo nel mondo digitale?

Quasi sempre una **login + password**

Phishing

- L'origine del termine si riferisce all'atto del "pescare" (*fish* in inglese) le password e altre informazioni personali dal "mare" degli utenti Internet
- Il **phishing è una forma di furto di identità** perpetrato mediante l'invio a centinaia di migliaia di destinatari di una email ingannevole, ma all'apparenza autentica, che invita a:
  - comunicare informazioni riservate via mail
  - andare su siti Web noti (in realtà, siti civetta)

Esempio di phishing



Esempio di phishing

Un tipo di attacco crescente negli USA

"Dal phishing al whaling"

- Mirato al computer (o dispositivo mobile) di un dirigente o di un dipendente dell'area "risorse umane"
- Obiettivo immediato: infettare il computer con software malevolo che non lascia tracce e non crea disturbi di funzionamento
- Obiettivi successivi:
  - Rubare informazioni
  - Usare il computer come ponte per altri attacchi interni

Take home

1. **Prestare attenzione alle mail provenienti da sconosciuti (e anche da conoscenti) contenenti**
   - **Allegati**
   - **Link**
2. **Non scaricare software da siti sconosciuti**
3. **Crittografare i dati personali riservati (soprattutto di natura sanitaria)**
4. **Proteggere idee, progetti, prototipi**
5. **Proteggere i dati finanziari e tutti quelli strategici**

White side: "Sappiamo tutto"
Come difendersi

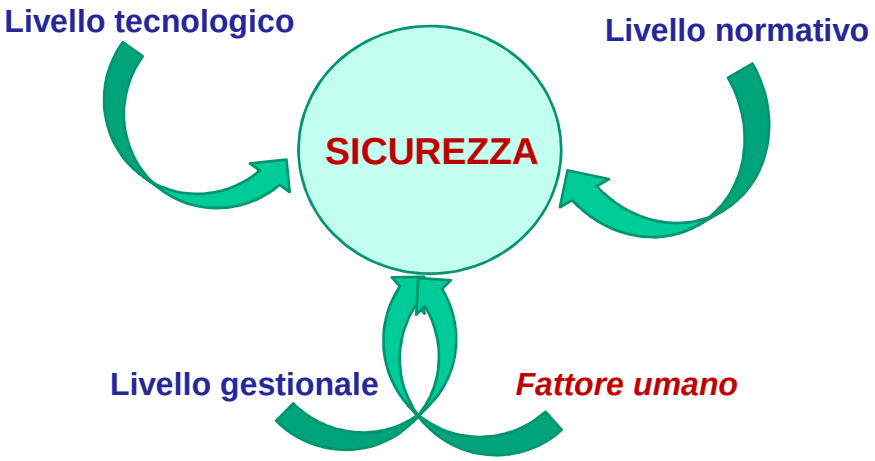
Politiche aziendali:
Tutte orientate alla Prevenzione

- Autenticazione
- Controllo azioni
- Prevenzione perdita dati (e eventuali rimedi)
- Modalità di accesso alle reti

Strumenti tecnici a disposizione

- **Principalmente orientati alla rete**
  - VLAN
  - NAT
  - Firewall
  - DMZ
  - VPN
  - Network Intrusion Detection System (NIDS)
- **Principalmente orientati ai sistemi**
  - Hardening, Patching
  - Virtualizzazione
  - Host Intrusion Detection System (HIDS)
- **Crittografia/Hashing e relative applicazioni**
  - Cifratura dei dati memorizzati
  - Protocolli sicuri (IPsec, SSL, WPA), email, Web, collegamento remoto, DNSSec, firma digitale, …

Ma la sicurezza non è solo tecnica



Approccio alla sicurezza

Tipico, ma errato	*Corretto*
• Ipotizzare che la sicurezza informatica sia un problema tecnologico • **Partire a considerare il livello tecnologico** • Cercare di soddisfare i minimi requisiti normativi • Non affrontare il livello gestionale perché è umanamente oneroso	• **Partire dal livello gestionale** che deve includere gli aspetti normativi vigenti • **Risolvere il livello tecnologico** (che deve diventare una mera implementazione delle decisioni prese a livello direttivo)

Se ci si pensa bene …

- **E’ sbagliato parlare di sicurezza informatica**
- **Il vero obiettivo è la "continuità del business”**

➢ **Noi vogliamo che la nostra organizzazione continui a procedere bene senza interruzioni e senza che furti, intrusioni, attacchi al nostro personale o azioni sleali erodano la nostra credibilità e la nostra qualità dei servizi**

Approccio corretto

- **Per la continuità del business è fondamentale sapere quali sono le informazioni e i servizi strategici, dove sono, chi può accedervi, chi ne è responsabile**
- **In questo modo la sicurezza non è un costo aggiuntivo, ma diventa un effetto collaterale** di ciò che andrebbe fatto in ogni caso per supportare la gestione dell’informazione e garantire la continuità del business

Passi gestionali fondamentali (1)

1. **Identificare le risorse in termini di:**
   - ***Sistemi***
   - ***Applicazioni***
   - ***Informazioni***

2. **Evidenziare quelle più critiche per la continuità del servizio**

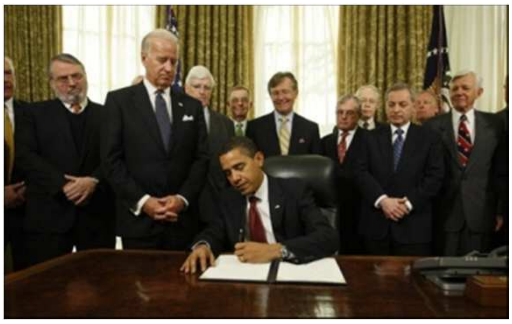
Passi gestionali fondamentali (2)

3. **Determinare quali devono essere le modalità di accesso alle informazioni:**
   - chi può leggerle? (***politiche di confidenzialità***)
   - chi può modificarle? (***politiche di integrità***)
   - quando devono essere disponibili? (***politiche di disponibilità***)
   - da dove e in che modo si può accedere? (***politiche di accesso***)

4. **Analogo procedimento va effettuato per le applicazioni:** posta, contabilità, protocollo, mandati, siti Web, ecc.

Il tutto non è "senza costi"

- Serve una conoscenza approfondita dei processi interni e delle relazioni esterne
- Servono risorse umane competenti e tempo
- Serve un forte *committment* a livello dirigenziale per tutte le direttive e le politiche di sicurezza



Una volta determinate le politiche, vi sono tante tecnologie per realizzarle

1. **Costruire "perimetri" a grana fine intorno alle risorse critiche** utilizzando tecnologie di protezione che sono commisurate al valore delle risorse e del rischio
2. **Monitorare i perimetri**, e costruire profili comportamentali "tipici" al fine di evidenziare eventuali anomalie
3. Utilizzare gli strumenti di protezione tipici della ***Ingegneria della sicurezza***. Es.,
   - Firewall, antivirus, architetture multi-livello, …
   - Autenticazione e autorizzazione
   - Crittografia
   - Hardening
   - Vulnerability assessment