NETLINK S.a.s.

Analisi dei Rischi dei Sistemi Informativi (Risk Analisys)

Dott Paolo PAVAN
Netlink S.a.s.

Di quale sicurezza si parla?

- Sicurezza del sistema Informativo
  - client/server
  - internet/intranet
- Sicurezza della rete
- Protezione da Internet
- Riservatezza e Integrità dei Dati
- Applicazioni Sicure
- Ambiente Controllato

Conoscenze preliminari

- Approfondite conoscenze tecniche su:
  - sistemi
  - servizi implementati
  - networking (Internet)
  - sicurezza
  - legislazione informatica/telematica

Schema dell'analisi di sicurezza

Analisi preliminare

- Impostare l'analisi in base alla tipologia di azienda e all'importanza che la sicurezza può avere per l'azienda.
- Analizzare processi aziendali di produzione, il personale impiegato e servizi offerti dall'azienda
- Valore delle informazioni trattate stabiliscono in che proporzione si deve investire in sicurezza
- Identificare i reali bisogni di sicurezza dell'azienda in relazione all'attività e alle risorse umane
- Quantificare costi e tempi per l'adozione delle necessarie misure di sicurezza

Analisi in pratica

- Esigenze in termini di sicurezza
- Tipologia di dato trattato
- Traffico di rete
- Hardware a disposizione
- Software utilizzato
- Servizi che si vogliono offrire

Conoscenza degli standard internazionali di sicurezza

- Riferimenti Internazionali
  - ISO/IEC 17799
  - ITSEC (da Orange Book - CTSEC)
  - Common Criteria
- Normativa Italiana
  - L.675/96
  - D.p.R.318/99
  - ex delibera AIPA 51/2000
- Valutare i tool di supporto all ’attività di analisi dei rischi:
  - CRAMM,COBRA,RiskWatch,Risk &Recovery Pac

Metodologie di IT Risk Analysis

Derivazione BS7799-1 e 2
It Security nel Regno Unito over ITSEC

- **CRAMM**, Central Computer and Telecommunication Agency (CCTA) Risk Analysis and Management
  - http://www.ccta.gov.uk
  - http://www.crammusergroup.org.uk/cramm.htm
- Obbligatoria per gli organismi governativi del Regno Unito in tema di sicurezza. **CRAMM** prevede una fase iniziale di Risk Analysis nella quale il rischio IT viene valutato sulla base del:
  - valore dell'asset da difendere,
  - del livello della minaccia
  - della gravità della vulnerabilità
- ed una successiva fase di Risk Management dove vengono individuate le contromisure adeguate alla gestione dei rischi valutati precedentemente.
- Il metodo è corredato di uno **strumento software** per la gestione delle varie attività ed anche per la produzione dei report finali con i suggerimenti per il top management riguardo le contromisure da adottare. **CRAMM** è concettualmente compatibile con BS7799 e con **l'approccio ITSEC** relativo ai livelli di assurance e alle funzionalità di sicurezza

NETLINK S.a.s.

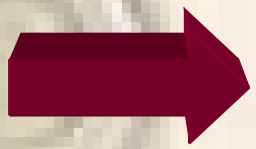
Servizi aziendali per la Sicurezza

- **Valutazione di sistemi ICT secondo gli standard Europei**: monitoraggio dei beni e delle risorse aziendali tramite l'applicaizone degli standard Europei
- **Risk Management: considerazione nalla fase di gestione aziendale della minacce come fatto strutturale e non episodico**
- **Analisi del rischio di sistemi ICT: riduzione del rischio a livelli accettabili sulla base dei beni da proteggere (**CRAMM o Risk Watch**)**
- **Pianificazione del Disaster recovery: il DR esprime la capacità in termini di risorse tecniche ed umane di ripristino totale del sistema in qualunque caso. E' fondamentale pianificare le attività da effettuare in caso di necessità.**
- **Firma digitale: per la trasmissione di documenti, aventi valore legale per autenticare un mittente, garantire integrità (hashing del documento) e riservatezza (crittografia)**
- **Tutela dati personali: la Legge 675 del 31/12/99 impone che i dati personali e esensibili siano custoditi e controllati in moda da ridurre al minimo i rischi di:**
  - distruzione, perdita anche accidentale, di accesso non autorizzato, di trattamento non consentito,di trattamento non conforme alla finalità della raccolta.
- **Sicurezza Globale: riassume un po' tutti i servizi visti e li incorpora in un'unica attività di controllo/analisi**
  mediante l'elaborazione di un piano per la sicurezza informatica dell'azienda suddiviso in fasi:
  - Determinazione del fabbisogno di protezione;
  - Analisi del Rischio;
  - Individuazione delle contromisure e loro piano di realizzazione.
  - Ceritificazione e conformità agli standard delle contromisure adottate

Applicazione della CRAMM

- In ambito di sicurezza dei sistemi in rete vige una regola:
  - "la forza di un network informatico è uguale alla debolezza dei punti di unione meno forti."
- L'analisi di questi punti relativamente più deboli può essere eseguita usando semplicemente la logica e l'esperienza o, usando una metodologia automatizzata come la CRAMM secondo la procedura presentata:

- Viene assegnato un valore ben preciso a tutte le parti del sistema, sia fisiche che logiche.
- Attraverso questa procedura le parti maggiormente vulnerabili vengono identificate.
- Ad ogni anello debole viene assegnato un valore rappresentante il grado di probabilità che questo si spezzi.
- Viene assegnato un altro valore che quantifica il danno associato all'evento.



I rischi che fanno parte del sistema possono così essere identificati. In ogni caso questa è una procedura praticamente obbligatoria se si vuole veramente fronteggiare l'eventualità di truffe informatiche.

Approcci metodologici

- Impostare l'approccio o sul bene aziendale o sul processo aziendale
- Valutare le analisi sulla base di:
  - quantitative: dati ottenuti e misurati
  - qualitative: dati estrapolati
- Scelta dei metodi di conduzione del test
- Scelta dei software e dei supporti cartacei (documentazione) da utilizzare.

Raccolta informazioni

- Inventario dei beni esistenti e del loro stato di sicurezza
- Analisi logica (software) e fisica (hardware) di sistemi e apparati rete
- Raccolta informazioni con il personale addetto ai sistemi (programmatori, amministratori di sistema, ecc ecc)
- Esecuzione di penetration test, portscanning e e verifiche di integrità locale dei sistemi.

Cosa viene sottoposto a controllo?

Classificazione dei sistemi e delle Risorse

- Valutare con precisione quali sono le risorse che l'analisi deve comprendere:
  - Hardware (Apparati di rete, computer...)
  - Software (Applicativi utilizzati)
  - Dati
  - Persone: tecnici di sistema, sviluppatori ed utenti finali
  - Storage: dischi, nastri magnetici

Classificazione dei Servizi

- Identificare i servizi informatici che devono essere erogati
- Identificare i punti di criticità di questi servizi
- Identificazione delle vulnerabilità dei servizi
- Identificare i sistemi di sicurezza idonei alla protezione di questi servizi.

Classificazione dei Dati

- Tipologia di dati trattati
- Presenza o meno di dati sensibli
  - Applicazione normativa L 675/Dpr 318
- Protezione da violazione o accessi non desiderati
- Backup giornaliero dei dati
- Procedure di restore Rapido dei dati (BCP e DRP)

Classificazione della Rete

- Tipologie e Topologia di rete
  - le tecniche di sicurezza variano a seconda del tipo di rete utilizzato (ma oggi tutti usano Ethernet)
- Grado di condivisione e interscambio risorse
- Necessità di accesso in rete locale e a Internet
- Numero di Host
- Volume di traffico e tipologia di traffico
  - consigli per l'ottimizzazione della rete
- Presenza di servizi raggiungibili dall'esterno
  - DMZ
  - Firewall
  - VPN

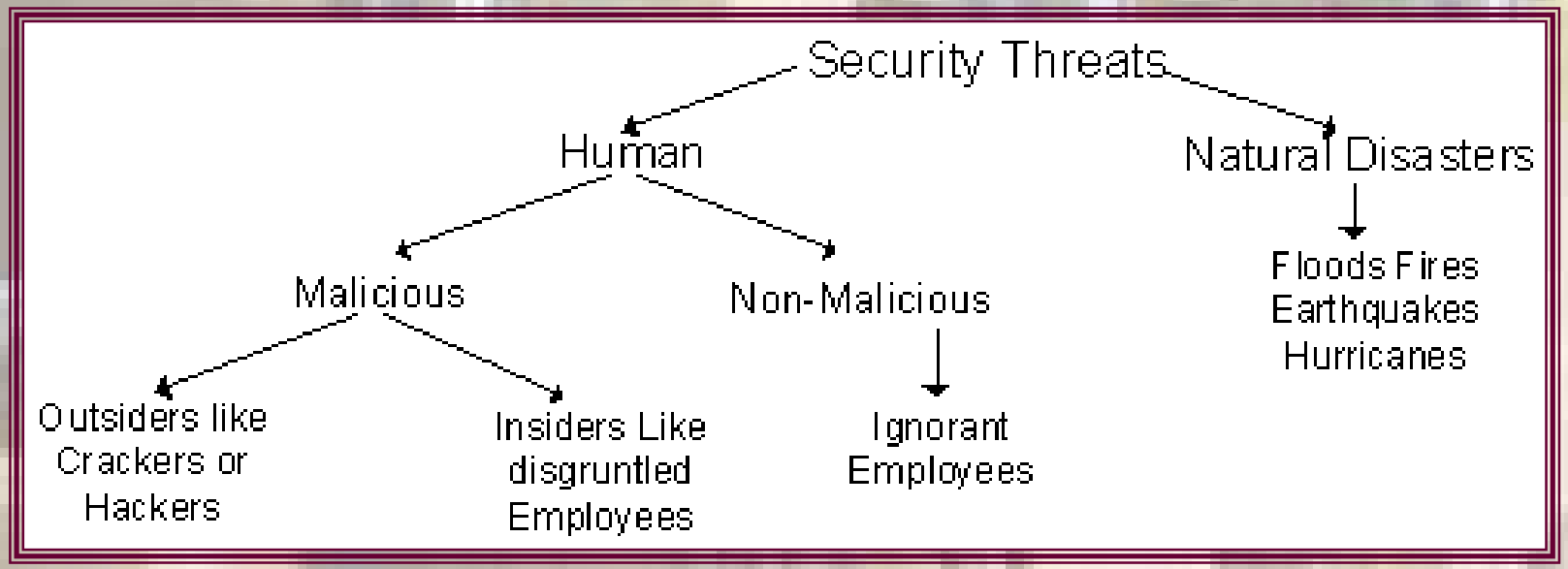
Classificazione degli Utenti

- Identificare utenti esterni e utenti interni
- Stabilire i processi di comunicazione e interscambio dati tra utenti esterni ed interni
- Identificare con precisione le priorità degli utenti sulle diverse parti del sistema
- Identificare il profilo di un ipotetico “attacker” interessato ai nostri dati

Valutazione delle possibili minacce

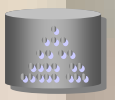
- Identificazione e catalogazione delle reali possibili minacce:
  - Accessi non autorizzati da parte di persone esterne al sistema
  - Violazione di privilegio
  - Scoperta involontaria di informazioni
  - Scarsa protezione dell'hardware
  - Interruzione di servizio

Origine delle Minacce



NETLINK S.a.s.

Censimento delle Risorse nel Dettaglio

Risorse	Rischi	Soluzioni
 Utenti Mobili	• Furto o perdita Laptop • Attacchi Dial-up (ISDN/PSTN)	• Encrypted File System (EFS) • PPTP, IPSEC, L2TP • PGPNet
 Sistemi	• Attacchi Esterni (Rete e Internet) • Falsa identità • DoS, Flooding e Spoofing • Sniffing	• Armoring & Hardening • IDS • PPTP, IPSEC, L2TP • Kerberos, PKI • SSL/TLS, S/MIME
 LAN / WAN Intranet	• Network Intrusion • Exploit root Account • Furto della password • Modifica Utenti • Modifica Dati • DoS, Spoofing o Flooding	• Firewall e ACL Router • IDS • Network Auditing • Kerberos • Smart Cards, Biometrics • Policy Users
 Extranet	• Autenticazione degli estremi • Connessione criptata • Furto di dati • Aggiramento Firewall	• Public Key Infrastructure (PKI) • Integrated CA • Tunneling • IPSEC, SSL/TSL, S/MIME
 Storage/Dati	• Risorse varie e distribuite • Complessità del sistema • Monitoraggio oneroso	• LDAP • Sistemi per la Gestione integrata dei dati e delle risorse • Crittazione dei dati e dei filesystem

Quantificazione dei Costi

- Risorse Hardware
  - costo dell'host firewall
  - struttura a norma (cablatura, armadi, climatizzazione per controllo temperature)
  - sistema ridondante
  - doppia tecnologia
- Risorse software
  - scelta del tipo di firewall
  - caratteristiche del firewall
- Risorse Umane
  - installazione sistema di protezione
  - mantenimento del sistema di protezione
  - aggiornamento del sistema di protezione

Scelta del firewall

- Scelta del software in relazione alle necessità
  - firewall hardware: scarsa configurabilità alta stabilità
  - Firewall software: più difficile da gestire ma più funzionale
    - supporto almeno 3 reti (int, ext e DMZ)
    - supporto crittografia per controllo remoto
    - supporto VPN
    - Funzioni di proxy, DNAT e Masquerading
    - Sistema di ripristino immediato

Impostazione delle contromisure

- Armoring dei sistemi e della rete
- Aggiornamento dei sistemi e riduzione delle vulnerabilità
- Installazione di Firewall e ACL Router
- Monitoraggio continuo del sistema:IDS
- Impiego massiccio della crittografia
- Formazione del personale