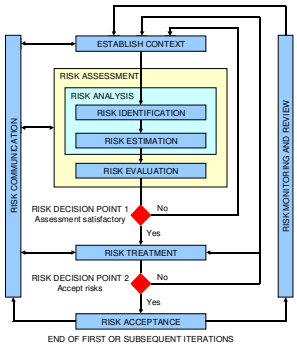
Il processo di analisi dei rischi (parte I)

Marco Domenico Aime
< m.aime @ polito.it >

Politecnico di Torino
Dip. di Automatica e Informatica

1

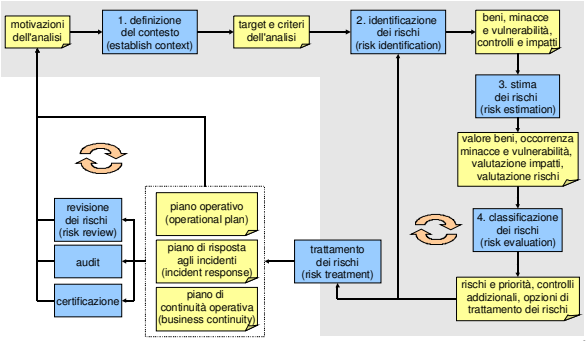
Il processo di gestione dei rischi



fonte: ISO 27005

2

Il processo di gestione dei rischi



3

Approccio

- **analizzeremo in dettaglio:**
  1. identificazione del contesto
  2. identificazione dei rischi
  3. stima dei rischi
  4. classificazione dei rischi
- **discuteremo il trattamento dei rischi**
- **accenneremo agli altri processi**

4

Approccio

- **seguiremo sostanzialmente il processo come descritto dalla norma internazionale ISO 27005**
- **identificazione e stima**
  - sono passi sequenziali, ma iterativi tenendo contono dell'iteratività dell'intero processo di analisi
  - le tratteremo unitamente prima per i beni, poi per le minacce e vulnerabilità, infine per i rischi

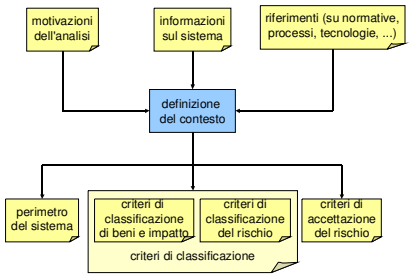
5

1. Definizione del contesto (Establish context)

- **identificare:**
  - motivazioni dell'analisi
  - informazioni necessarie alla definizione del sistema
  - lista di riferimenti rilevanti (normative, processi, tecnologie, ...)
- **definire:**
  - i criteri base dell'analisi
  - il perimetro del sistema sotto analisi

6

Definizione del contesto



7

Motivazioni per svolgere un'analisi dei rischi

- **obblighi normativi**
- **processo di certificazione**
- **valutare e migliorare l'ISMS**
- **preparare un piano di risposta agli incidenti**
- **preparare un piano di business continuity**
- **aggiornare i risultati di una precedente analisi**

8

Ulteriori motivazioni

- **aumentare la consapevolezza**
  - si responsabilizzano i dipendenti
- **identificare gli oggetti esposti, i punti deboli e le possibili contromisure**
  - molte aziende non hanno questa tabella
- **migliorare la base dati decisionale**
  - le contromisure spesso riducono la produttività: si riesce a giustificarle?
- **giustificare le spese per la sicurezza**
  - identificare i rischi maggiori dovuti a mancati investimenti in sicurezza

9

Informazioni e riferimenti

- **documentazione o responsabili per stabilire:**
  - architettura del sistema informativo:
    - componenti, sotto componenti, interfacce e connettori, bordi e barriere
  - descrizione funzionale del sistema informativo:
    - obiettivi e requisiti, descrizione funzionale, del sistema e dei suoi componenti
  - scenari di incidente
  - controlli esistenti e pianificati
  - la politica di sicurezza

10

Acquisizione delle informazioni

- **questionari**
  - distribuiti e/o usati nelle interviste
- **interviste**
  - personale di gestione e supporto
- **documenti**
  - documenti normativi (es. documentazione legale, direttive, ...)
  - documenti di sistema (es. guida utente, manuale amministrativo, documenti di progetto, ...)
  - documenti di sicurezza (es. analisi precedenti, test di sicurezza, politiche di sicurezza, piano di sicurezza, ...)

11

Esempio di questionario

- Who are valid users?
- What is the mission of the user organization?
- What is the purpose of the system in relation to the mission?
- How important is the system to the user organization's mission?
- What is the system-availability requirement?
- What information (both incoming and outgoing) is required by the organization?
- What information is generated by, consumed by, processed on, stored in, and retrieved by the system?
- How important is the information to the user organization's mission?
- What are the paths of information flow?
- What types of information are processed by and stored on the system (e.g., financial, personnel, research and development, medical, command and control)?

- What is the sensitivity (or classification) level of the information?
- What information handled by or about the system should not be disclosed and to whom?
- Where specifically is the information processed and stored?
- What are the types of information storage?
- What is the potential impact on the organization if the information is disclosed to unauthorized personnel?
- What are the requirements for information availability and integrity?
- What is the effect on the organization's mission if the system or information is not reliable?
- How much system downtime can the organization tolerate? How does this downtime compare with the mean repair/recovery time? What other processing or communications options can the user access?
- Could a system or security malfunction or unavailability result in injury or death?

fonte: SP 800-30

12

Comitato di analisi (analysis team)

- **in genere da 5 a 9 persone**
- **rappresentanti dei seguenti gruppi:**
  - sistemisti hardware
  - sistemisti software
  - programmatori applicativi
  - personale addetto all'inserimento dati
  - guardiani della sicurezza fisica
  - utenti più importanti
- **tradizionalmente a supporto dell'analista**
- **alcune metodologie supportano l'auto direzione di un comitato interno per l'analisi dei rischi**

13

Identificazione del perimetro

- **definire campo e limiti (scope and boundaries) del processo di analisi:**
  - l'oggetto dell'analisi (target of evaluation)
    - processi, componenti (hw/sw) e interfacce coinvolte
  - le risorse per il processo di analisi
    - lista dei riferimenti rilevanti (normative, vincoli legali, ...)
    - organigramma dei responsabili
  - vincoli temporali
    - data di riferimento (... cambiamenti continui ...)

15

L'oggetto dell'analisi

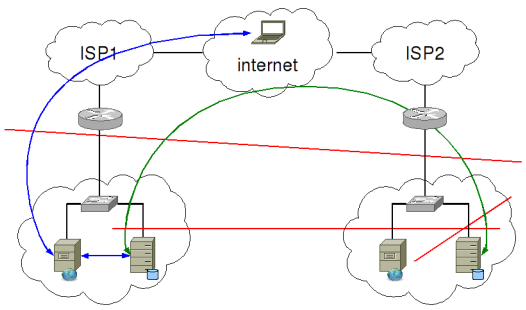
- **il sistema sotto analisi può essere:**
  - una specifica applicazione
  - l'infrastruttura IT (o una sua parte)
  - uno specifico processo business
  - l'intera organizzazione

16

Perimetro e descrizione

17

Perimetro e descrizione



18

Perimetro e descrizione

- **interno del perimetro**
  - oggetto di modellazione dettagliata
  - completezza e correttezza
  - verifica delle assunzioni
  - selezione controlli aggiuntivi
- **esterno del perimetro**
  - assunzioni a livello di interfacce

19

Rischio o non rischio?

- **ognuno di noi accetta alcuni tipi di rischio e ne rifiuta altri (es. guidare l'auto, volare in aereo, mangiare cozze, ...)**
- **ognuno mette in atto contromisure per diminuire il rischio (es. lavare bene le cozze)**
- **i sistemi informativi sono molto complessi e perciò l'analisi dei rischi deve essere metodica**

20

Come modellare e classificare i rischi?

- **possiamo definire un rischio come una relazione tra**
  - la possibilità che un incidente si concretizzi (occorrenza)
  - la stima del danno causato da tale incidente (impatto)
  - *Rischio = Occorrenza X Impatto*

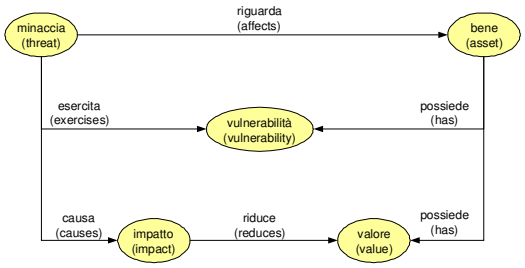
21

Come modellare e classificare i rischi?

- **a sua volta l'occorrenza è una relazione tra**
  - la concretezza della minaccia (probabilità, frequenza)
  - il grado di vulnerabilità del sistema
  - *Occorrenza = Minaccia X Vulnerabilità*
- **e le conseguenze sono una relazione tra**
  - il valore dei beni coinvolti
  - le conseguenze dell'incidente
  - *Impatto = Beni X Conseguenze*

22

Modello dei rischi (beni - minacce - vulnerabilità)



23

Come modellare e classificare i rischi?

- **criteri di classifificazione**
  - consiste nel definire delle categorie sui possibili valori di beni/impatto/rischio
- **valutazione di beni e conseguenze**
  - la valutazione dei beni e delle conseguenze è in genere espressa attraverso vettori su dimensioni multiple

24

Come modellare e classificare i rischi?

- **le metodologie offrono linee guida per**
  - scegliere un insieme di dimensioni appropriato allo specifico caso
  - scegliere una classificazione dei valori appropriata allo specifico caso
- **la personalizzazione è possibile sia sulle dimensioni considerate sia sulla scala di valori**

25

Dimensioni di classificazione

- **valore strategico dei processi informativi**
  - reputazione, perdita di clienti, fallimento di piani e deadline
- **perdite finanziarie**
  - costi operativi aggiuntivi, mancati guadagni, perdite una tantum (sostituzione beni)
- **perdite di produttività**
  - ore personale aggiuntive

26

Dimensioni di classificazione

- **aspetti legati alla safety**
  - perdite di vite umane, danni alla salute
- **aspetti legali**
  - violazione di norme (multe) e contratti (cause)
- **classificazione dei beni coinvolti**
  - tipologia, criticità, proprietà di sicurezza coinvolte (confidenzialità, disponibilità, ...)

27

Valore dei beni e impatto

- **quale relazione c'e' tra valore dei beni e impatto?**
- **l'impatto misura il danno complessivo di un incidente**
- **un incidente può riguardare**
  - un bene
  - molti beni
  - una parte di un bene
- **la valutazione di impatto è generalmente vicina al valore dei beni coinvolti**

28

Analisi quantitativa vs qualitativa

- **alcuni impatti sono quantificabili in termini di:**
  - perdita di guadagni
  - costi di riparazione
  - lavoro necessario a correggere i probelmi
- **altri impatti non sono misurabili solo in termini qualitativi (es. impatto alto/medio/basso)**
  - perdita di credibilità
  - danni agli interessi di un'organizzazione
  - violazioni di segretezza
  - ...

29

Analisi quantitativa vs qualitativa

- **analisi qualitativa:**
  - pro: prioritizza i rischi e identifica le aree di immediato miglioramento
  - con: rende difficile un'analisi costi-benefici sui controlli suggeriti
- **analisi quantitativa:**
  - pro: fornisce una misura della magnitudine degli impatti usabile in un'analisi costi-benefici sui controlli
  - con: in base ai range numerici usati, il significato dei risultati può non essere chiaro e richiedere un'interprezione qualitativa a posteriori

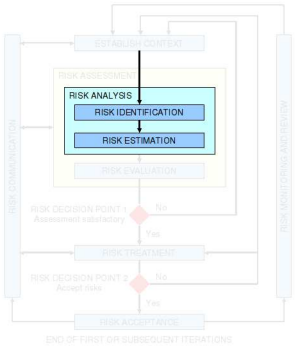
30

Criteri di accettazione dei rischi

- **in base a cosa un rischio è accettabile o meno?**
- **può dipendere da diverse considerazioni:**
  - modello di business
  - vincoli normativi
  - risorse economiche
  - risorse tecnologiche
  - risorse operative

31

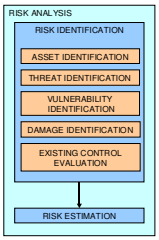
2. Analisi dei rischi (risk analysis)



32

Analisi dei rischi

- **è la parte più importante e delicata**
- **richiede un approccio sistematico e molte informazioni**
- **non può mai essere ritenuta definitiva**
- **svolge la funzione di guida per tutti i provvedimenti da adottare**
- **è propedeutica all'attuazione delle contromisure**



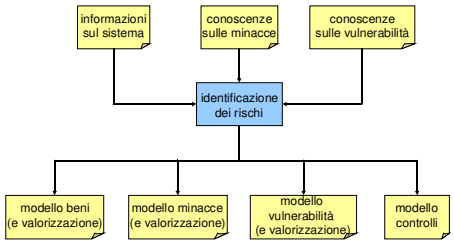
33

Analisi dei rischi

- **in genere è un processo iterativo:**
  - per approfondimento crescente
    - specie in sistemi complessi è opportuno iniziare con un'analisi macrosocopica che viene dettagliata progressivamente
  - dovute a cambiamenti nel sistema sotto analisi
    - già effettuati o pianificati
  - periodiche
    - per tener conto di nuove minacce, incidenti inattesi, effetti inattesi di incidenti previsti

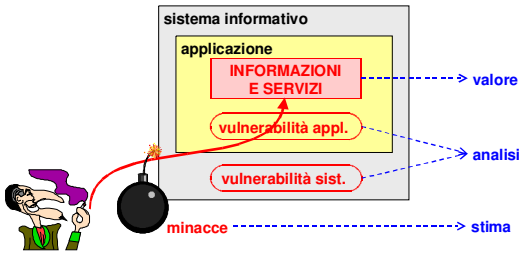
34

2.1. Identificazione dei rischi



35

Modello dei rischi (beni - minacce - vulnerabilità)



36

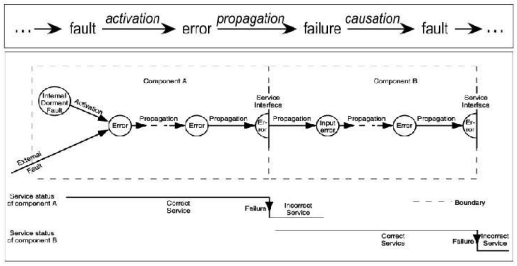
Modello dei rischi

- **un incidente è un evento o una serie di eventi relativi sicurezza dell'informazione**
- **un attacco complesso prevede in genere lo sfruttamento di un insieme di vulnerabilità in cascata**
  - es. malware
- **dobbiamo anche considerare l'eventuale occorrenza comcomitante di eventi indipendenti**
  - es. attacco in presenza di rottura accidentale

37

Propagazione di eventi naturali (fault)

- **buoni modelli predittivi**

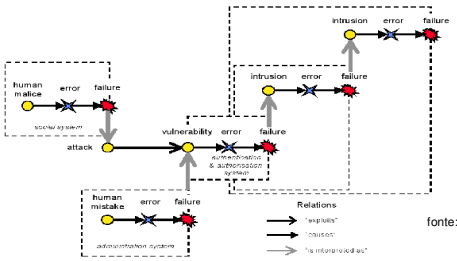


fonte: Avizienis, Laprie, Randell, Landwher,
"Basic Concepts and Taxonomy of Dependable and Secure Computing", IEEE TDSC, 2004

38

Propagazione di eventi di sicurezza

- **più complessa e meno definita**
  - tuttora argomento di ricerca



fonte: progetto MAFTIA

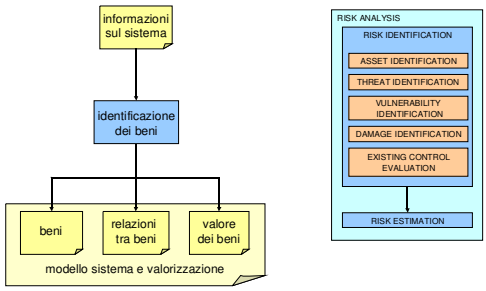
39

2.1.1. Identificazione dei beni (asset identification)

- **un bene è qualsiasi cosa che ha valore per l'organizzazione e quindi deve essere protetto**
- **un sistema IT non è solo hardware e software**
- **il livello di dettaglio dipende dallo scopo e livello dell'analisi**
  - bisogna comunque tener traccia degli asset che vengono tralasciati per l'attuale iterazione di analisi
- **è un passo fondamentale dove si concentra la conoscenza del sistema sotto analisi**

40

2.1.1. Identificazione dei beni



41

Identificazione dei beni

- **in effetti si tratta di un processo con tre passi distinti:**
  - identificazione (identification)
    - beni e relazioni, categorie
  - aggregazione (aggregation)
    - utile per dipendenze
  - valorizzazione (estimation)
    - assegnazione di un valore

42

Componenti del sistema informativo

- **analisi per categorie:**
  - informazioni
  - servizi business
  - persone (utenti, personale)
  - dati
  - software
  - hardware
  - parti di ricambio (es. backup)
  - documentazione

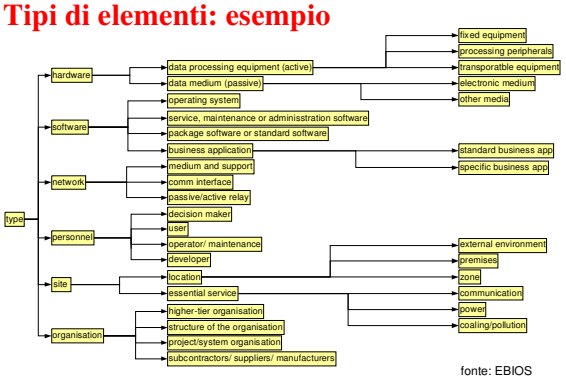
43

Componenti del sistema informativo

- **l'insieme di categorie rilevanti dipende dal tipo di sistema sotto analisi**
  - specifica applicazione
  - sito di commercio elettronico
  - sistema IT aziendale
  - sistema di automazione industriale
  - ...
- **le tassonomie indicate dalle varie metodologie sono pertanto da ritenersi dei punti di partenza**
  - da personalizzare e adattare al caso specifico

44

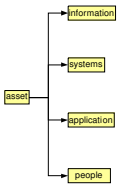
Tipi di elementi: esempio



fonte: EBIOS

45

Tipi di elementi: esempio



fonte: OCTAVE-S

46

Relazioni tra le componenti

- **requisiti funzionali**
- **flusso delle informazioni**
- **ruoli e autorizzazioni**
- **topologia di rete**
- **aggregazioni**
- **dipendenze**

47

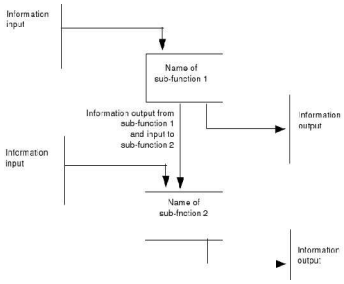
Requisiti funzionali

- **qualsiasi sistema informativo può essere diviso in:**
  - servizi business (business services, operational functions)
  - servizi tecnici (technical services, support functions)
  - servizi di verifica (checking and monitoring functions)
- **un cambiamento in un servizio business può avere conseguenze importanti sugli altri servizi**
- **un cambiamento in un servizio di supporto o verifica non dovrebbe avere un impatto diretto sui servizi business**

48

Flusso delle informazioni

- **diagramma di flusso input-output**

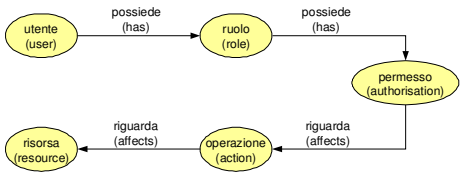


fonte: EBIOS

49

Ruoli e autorizzazioni

- **a ogni utente e personale vengono assegnati uno o più ruoli (categorie di utenza)**
- **un ruolo è autorizzato a compiere una o più operazioni su una o più risorse**



50

Ruoli e autorizzazioni

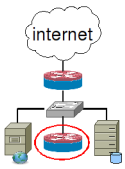
- **tre modalità principali di gestione della sicurezza:**
  - esclusiva (exclusive) = tutti gli utenti che accedono al sistema sono autorizzati a tutte le informazioni/ operazioni e hanno identiche necessità di accesso
  - dominante (dominant) = tutti sono autorizzati a tutte le informazioni/operazioni, ma non hanno identiche necessità di accesso
  - multilivello (multilevel) = non tutti sono autorizzati a tutte le informazioni/operazioni, e non tutti hanno identiche necessità di accesso

fonte: EBIOS

51

Tipologia di rete

- **canali dedicati vs condivisi**
- **connettività verso l'esterno**
- **topologia fisica vs logica**
  - varie tecnologie di rete, alta disponibilità, e sicurezza alterano la topologia fisica
    - WLAN
    - indirizzamento IP
    - P2P
    - VLAN, VPN, ...



52

Aggregazione dei beni

- **corrisponde ad una scomposizione del sistema in sottosistemi**
- **utile a semplificare l'applicazione dell'analisi**
  - in genere è più facile studiare un insieme di sottositemi separati che un unico sistema multifunzione
    - ma il numero di sottosistemi interagenti deve rimanere basso
  - essenziale in sistemi di grandi dimensioni
  - facilita l'identificazione di bordi e barriere

53

Criteri di aggregazione

- **non esistono metodi di aggregazione/scomposizione fissi, ma alcuni criteri:**
  1. architettura hardware
  2. funzioni o informazioni essenziali
  3. ruoli e responsabilità
  4. sotto-zone distinte
  5. isolamento di sottositemi 'comuni'

54

Criterio 1: architettura hardware

- **gli aggregati sono singole macchine o insiemi di macchine**
- **il livello di aggregazione dipende dal livello di interazione tra le varie parti (macchine o insiemi di macchine)**
- **esempio di livelli crescenti di interazione:**
  - macchine fisicamente separate e trasferimento via supporto magneto/ottico
  - macchine connesse da cavo di rete dedicato
  - macchine connesse via rete locale
  - macchine connesse via rete locale, con stesso sistema operativo, e amministrate centralmente

55

Criterio 2: funzioni/informazioni

- **aggregazione/decomposizione basata:**
  - sulle funzioni supportate da un componente o insieme di componenti
  - oppure su come le informazioni più sensibili sono processate
- **esempio di aggregazione per funzioni:**
  - il servizio 'portale' dipende dal server web, il software Apache, e il gruppo di continuità
- **esempio di aggregazione per informazioni:**
  - i profili utente sono mantenuti presso il database server e processati dall'applicazione java 'myProfile'

56

Criterio 3: responsabilità

- **aggrega componenti gestiti da una singola entità:**
  - gruppo di sviluppo
  - gruppo di amministrazione
  - gruppo di utenti
- **utile anche quando esistomo diversi sistemi di documentazione separata**

57

Criterio 4: sotto-zone

- **aggrega componenti (dispositivi, informazioni, personale) in base alla zona in cui sono localizzati:**
  - edifici
  - zone riservate
  - ...
- **efficace quando il livello di interoperabilità di una zona con l'esterno è sufficientemente basso**

58

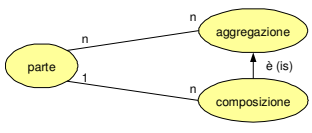
Criterio 5: sistemi comuni

- **dopo aver applicato i primi 4 criteri, alcuni (insiemi di) elementi possono trovarsi nell'intersezione tra più sottosistemi**
  - es. server condivisi, reti condivise, personale condiviso, ...
- **è possibile aggregare questi elementi in sottosistemi separati:**
  - sono studiati separatamente
  - i risultati sono poi trasferiti a tutti i sottosistemi in cui sono inclusi

59

Nota: aggregazione vs composizione

- **la relazione di composizione è una relazione di aggregazione in cui le parti non possono essere condivise tra diverse composizioni**



- **per descrivere sistemi informativi di sufficiente complessità è necessaria l'aggregazione**

60

Dipendenze (dependencies)

- **a cosa serve identificare le relazioni tra i beni?**
- **fondamentalmente a identificare le 'dipendenze'**
  - nessuna definizione precisa da parte delle metodologie => possiamo definirle come relazioni tra beni che influenzano l'impatto di un incidente
- **la relazione di dipendenza è ricorsiva**
  - A dipende da B che dipende da C ...
- **sono essenziali in varie fasi:**
  - valorizzare gli asset
  - valutare gli impatti
  - identificare minacce e vulnerabilità

61

Esempi di dipendenze

- **più rilevanti e numerosi i servizi business supportati da un server, più alto il valore di quel server**
- **i requisiti di sicurezza di un servizio di data storage dipende direttamente dalla confidenzialità dei dati processati**
- **se un processo dipende dall'integrità di certi dati prodotti da un'altro processo, allora i dati in input al secondo servizio devono avere un'affidabilità adeguata**
- **l'integrità di un'informazione dipende dall'hardware e software usati per il suo storage e processamento**
- **il corretto funzionamento di un dispositivo hardware dipende dalla fornitura di corrente e possibilmente dal condizionamento**

62

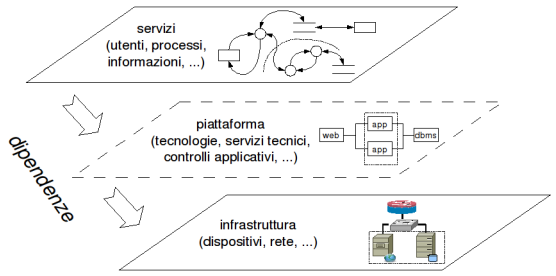
Modello strutturato del sistema

- **in quale formato organizzare tutte le informazioni sul sistema?**
- **dipende dalle varie metodologie di analisi e in generale non esistono metodi fissi**
- **per un sistema in fase di progetto è utile riusare la metodologia di progettazione selezionata**
  - es. UML
- **quando non esiste già una modellazione si possono usare alcune rappresentazioni 'universali'**

63

Modello strutturato del sistema

- **esempio di rappresentazione universale multi-livello:**



64

Modello strutturato del sistema

- **tre livelli principali:**
  - business (o servizi): informazioni, attori e processi, scambio di informazioni
  - logico (o piattaforma): basi dati, programmi, librerie, protocolli
  - fisico (o infrastruttura): storage, computer, siti, canali di comunicazione
- **dipendenze intra e inter livello**
- **questa divisione rispecchia le tre dimensioni di un sistema informativo moderno:**
  - informazioni, programmi, e comunicazioni

65

Modello servizi

- **il modello servizi descrive:**
  - informazioni
  - processi essenziali
  - flusso delle informazioni
  - aggregazione in macroprocessi
  - perimetri di gestione e fiducia

66

Importanza del modello servizi

- **il reale valore di un sistema IT risiede nelle informazioni e nei processi business che supporta**
  - (cfr. fase di valorizzazione degli asset)
- **qui risiede anche il reale obiettivo di un attacco organizzato**

67

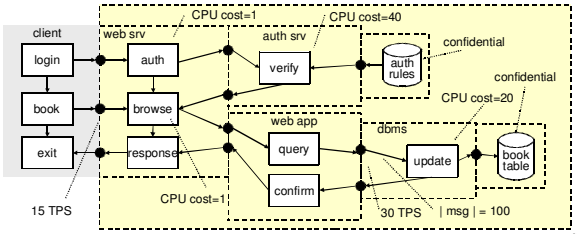
Descrizione del modello servizi

- **Data Flow Diagrams (DFD)**
  - formalismo semplice e intuitivo
  - può essere esteso con informazioni sulla sequenzialità tra flussi
- **Unified Modelling Language (UML)**
  - si possono usare sequence o activity diagram
- **Service Oriented Architecture (SOA)**
  - linguaggi XML per la descrizione di processi
  - es. BPEL

68

Modello servizi: esempio

- **grafo direzionato**
  - nodi = utenti/processi/informazioni
  - archi = scambio informazioni/interazioni/azioni



69

Descrizione del modello servizi

- **qualsiasi sia il formato scelto, per produrre una buona rappresentazione è necessaria l'interazione con un gruppo misto di:**
  - manager
  - esperti dei sistemi informativi
  - utenti

70

Modello piattaforma

- **il modello piattaforma descrive:**
  - applicazioni
  - interazioni tra applicazioni
  - dipendenze software
  - protocolli
  - aggregazione in sistemi applicativi
  - ridondanza logica
  - mediazione logica

71

Importanza del modello piattaforma

- **la maggior parte delle vulnerabilità sono legate a:**
  - mancanze in specifiche tecnologie
  - carenze in specifici protocolli
  - errori in specifiche implementazioni software
- **alcune architetture applicative prevengono o mascherano specifici incidenti**
- **anche la propagazione di eventi di sicurezza è dunque influenzata da qyuesto livello**

72

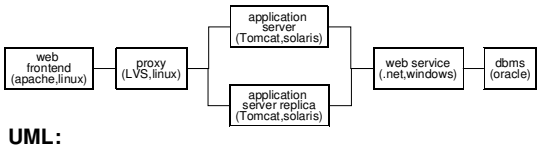
Descrizione del modello piattaforma

- **varie soluzioni legate a specifiche piattaforme tecnologiche**
  - es. metodologie e strumenti Microsoft per lo sviluppo di applicazioni in ambiente Windows/.Net
- **può ridursi a una lista di specifici software**
  - es. RedHat versione X con Apache versione Y
- **oppure può essere incluso nel modello servizi**
  - specie per processi sufficientemente semplici e basati su tecnologie standard (es. sito di commercio elettronico)

73

Modello piattaforma: esempio

- **grafo (non) direzionato:**
  - nodi = processi software
  - archi = comunicazioni di rete tra i processi (protocolli)



- **UML:**
  - corrisponde sostanzialmente al deployment diagram

74

Descrizione del modello piattaforma

- **per produrre una buona rappresentazione è necessaria l'interazione con:**
  - esperti dei sistemi informativi
  - sviluppatori applicazioni
  - consulenti esterni (es. assistenza e supporto)

75

Modello infrastruttura

- **il modello infrastruttura descrive:**
  - dispositivi (archiviazione, server, rete, sicurezza)
  - terminali utente
  - interfacce di rete, cavi
  - locali, edifici, siti
  - istanze software (in esecuzione e non)
  - istanze dati (attivi e non)
  - servizi di supporto (energia, condizionamento)
  - informazioni di configurazione (es. indirizzamento IP)

76

Importanza del modello infrastruttura

- **molte informazioni e funzioni sono replicate**
- **molte vulnerabilità sono legate a specifici dispositivi**
  - come complesso hardware / software
- **il guasto di alcuni dispotivi e sistemi è funzione dell'età**
  - es. dischi
- **molti eventi sono localizzati**
  - eventi naturali presso specifici siti
  - incendio / allagamento di specifici locali
  - mancanza energia elettrica
- **...**

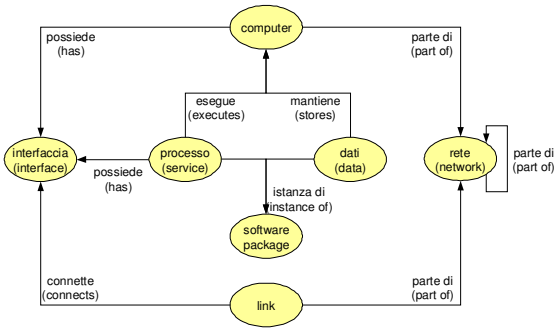
77

Descrizione del modello infrastruttura

- **grafo non direzionato:**
  - nodi = dispositivi hardware
  - archi = collegamenti di rete
- **molti strumenti e librerie di disegno:**
  - Microsoft Visio, Dia, ...
- **informazioni aggiuntive spesso disponibili in forma tabellare**
  - es. software installato, indirizzi IP, ...

78

Componenti IT



79

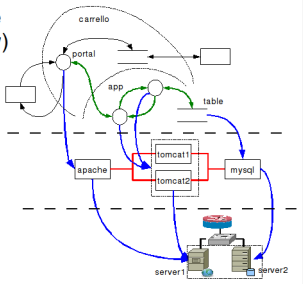
Descrizione del modello infrastruttura

- **per produrre una buona rappresentazione è necessaria l'interazione con:**
  - esperti dei sistemi informativi
  - amministratori dei sistemi informativi

80

Relazioni tra livelli

- **allocazione dei beni**
  - funzione e suo abiente di esecuzione (hw / sw)
  - informazioni e dati (permanenti e temporanei)
  - interazioni e elementi intermedi (rete)
  - ...



81

Replicazione

- **possiamo avere istanze multiple di alcuni beni**
  - es. copie software, dati ridondati, server identici, processi in load balancing, ...
- **tutte le repliche devono essere identificate**
- **note:**
  - in genere la replicazione è un vantaggio contro minacce alla disponibilità/integrità ma uno svantaggio contro minacce alla confidenzialità
    - es. chiave di riserva sotto lo zerbino
  - in effetti la replicazione è un controllo
    - (crf. identificazione dei controlli)

82

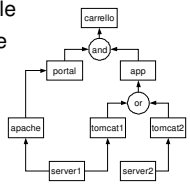
Modello delle dipendenze

- **in genere un bene può avere dipendenze multiple**
- **le possiamo combinare attraverso operatori logici:**
  - AND = tutti
    - es. il servizio 'carrello' dipende dal portale web, dall'applicazione Java 'carrello', e dal database 'magazzino'
  - OR = uno o più
    - es. la funzione 'lista prodotti' dipende dal dbms1 o dalla replica dbms2
  - N = almeno N
  - ...

83

Modello dipendenze: esempio

- **grafo diretto**
  - nodi = beni + operatori di combinazione per dipendenze multiple
  - archi = dipendenze



- **nota:**
  - gli operatori di combinazione tra dipendenze mutliple corrispondono ad aggregazioni tra asset

84

Semantica di un modello strutturato

- **riassumendo, un modello strutturato del sistema fornisce:**
  - la lista dei beni
  - parametri caratteristici di ogni bene
    - es. indirizzo IP di un'interfaccia di rete
  - relazioni riguardanti i beni, tra cui:
    - categorizzazione di ogni bene
    - varie aggregazioni tra beni
    - dipendenze tra beni

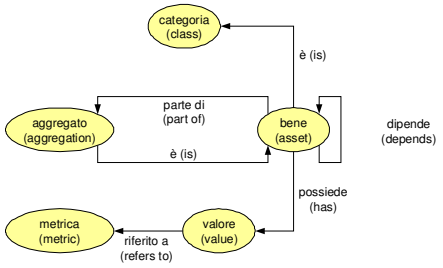
85

Valorizzazione dei beni (asset estimation)

- **assegnare ad ogni bene il valore in termini di:**
  - importanza (criticality)
    - = livello di importanza dell'asset
  - sensibilità (sensitivity)
    - = livello di protezione richiesto per l'asset
- **le metodologie forniscono linee guida da personalizzare per il caso specifico**
  - l'effettivo modello da usare è stabilito nella fase di definizione del contesto come parte dei criteri di rischio e impatto

86

Modello dei beni (beni - relazioni - valore)



87

Modello generale per valorizzazione

- **importanza via scala di valori:**
  - assoluta (analisi quantitativa)
    - es. 10K euro
  - ordinata (analisi qualitativa)
    - es. low/medium/high, range [0,10]
  - ...
- **sensibilità via multidimensionalità:**
  - es. proprietà di sicurezza
    - es. “disponibilità 10Ke, confidenzialità 0Ke” vs “disponibilità 0Ke, confidenzialità 10Ke”

88

Valutazione monetaria (quantitativa)

- **possibili criteri di assegnazione:**
  - costo originale/sostituzione/riparazione/rigenerazione
  - costo penali
  - costo personale (operativo/tattico/strategico) per il recupero
  - valore per un concorrente
  - ...
- **un bene può avere più valori:**
  - come valore complessivo si può usare il più alto o la somma di tutti o parte dei valori

89

Valutazione monetaria (quantitativa)

- **monetizzare i risultati è sempre utile per facilitare comprensione e supporto a tutti i livelli di una organizzazione**
- **si possono fattorizzare aspetti molto diversi tra loro**
- **se un certo valore è da ritenersi alto o basso dipende dall'organizzazione**
  - es. piccola vs grande azienda
- **in pratica si opera su ordini di grandezza, risultando simile ad un'analisi qualitativa con un range sufficientemente ampio**

90

Dimensioni

- **non esiste un vero e proprio insieme fisso**
  - dipendono dalla metodologia
  - in genere è possibile aggiungere ulteriori dimensioni ad un insieme predefinito
- **chiamate anche:**
  - aree di impatto (attenzione sul tipo di impatto)
  - proprietà (attenzione sulle caratteristiche del bene)
  - requisiti (attenzione sulla sensibilità)
  - metriche (attenzione sulla struttura dei valori)
- **alcune metodologie distinguono tra alcuni di questi aspetti altre no**

91

Esempio di dimensioni

- **CIA usate da tutti:**
  - confidenzialità (confidentiality)
  - integrità (integrity)
  - disponibilità (availability)
- **altre proprietà di uso comune:**
  - tracciabilità (accountability)
  - autenticità (authenticity)
  - affidabilità (reliability / dependability / assurance / resiliency / trust)

92

Esempio di dimensioni

Impact Area	Low	Moderate	High
Reputation	Reputation is minimally affected; little or no effort or expense is required to recover.	Reputation is damaged, and some effort and expense is required to recover.	Reputation is severely destroyed or damaged.
Customer Loss	Less than ____% reduction in customers due to loss of confidence	____% to ____% reduction in customers due to loss of confidence	More than ____% reduction in customers due to loss of confidence
Other.			

Impact Area	Low	Moderate	High
Operating Costs	Increase of less than ____% in yearly operating costs	Yearly operating costs increase by ____% to ____%	Yearly operating costs increase by more than ____%
Revenue Loss	Less than ____% yearly revenue loss	____% to ____% yearly revenue loss	Greater than ____% yearly revenue loss
One-Time Financial Loss	One-time financial cost of less than $ ____	One-time financial cost of $ ____ to $ ____	One-time financial cost greater than $ ____

fonte: OCTAVE Allegro

93

Esempi di valorizzazione dei beni

- **qualitativo in range [1,10], proprietà CIA:**

asset	C	I	A
table	10	5	10
app	0	10	5
...	...	...	...

- **quantitativo in euro, singola dimensione:**

asset	euro
table	100K
app	20K
...	...

- **quantitativo in euro, proprietà CIA:**

asset	C	I	A
table	100K	50K	100K
app	0	50K	10K
...	...	...	...

94

Dimensioni: note

- **spesso le dimensioni usate non sono indipendenti tra loro**

Esempio di selezione e interpretazione proprietà di sicurezza:
disponibilità: bene non più presente o permanentemente e completamente danneggiato
integrità: bene presente ma in forma degradata
confidenzialità: bene disponibile ad entità non autorizzate
autenticità: bene disponibile, integro, ma contraffatto
tracciabilità: bene di cui non si può determinare la provenienza

- **è possibile passare da un un sistema di dimensioni ad un'altro**

asset	C	I	A
table	10	5	10
app	0	10	5
...	...	...	...

asset	euro
table	100K
app	20K
...	...

95

Dipendenze e propagazione dei valori

- **in genere si valorizzano solo i beni essenziali (informazioni, servizi business)**
- **poi si propagano i valori in base alle dipendenze derivate dal modello del sistema**
  - es. se A vale 10 e dipende da B, allora anche B varrà 10
- **i modelli di propagazione non sono specificati dalle metodologie**
  - è l'analista a definirlo più o meno esplicitamente usando gli strumenti della metodologia

96

Dipendenze e propagazione dei valori

- **in genere la propagazione può aumentare il valore ma non abbassarlo:**
  - se il valore del bene dipendente (es. dati) è più basso del valore del bene considerato (es. servizio), il valore non viene cambiato
  - se il valore è più alto, il valore viene incrementato
- **le regole di aggiornamento dipendono dalla metodologia, ma in genere si usano regole semplici:**
  - il valore più alto
  - somma per dimensione
  - somma pesata sul grado di dipendenza

97

Grado di dipendenza

- **possiamo valorizzare anche il grado di dipendenza in base alle dimensioni selezionate**
  - valore booleano:
    - es. A dipende da B per confidenzialità e per disponibilità
  - scala proporzionale:
    - es. A dipende da B per il 100% in confidenzialità e per il 50% in disponibilità

98

Dipendenze multiple

- **raramente si considerano gli operatori logici**
  - AND ha una semantica chiara:
    - se A vale 10 e dipende da B e C, allora sia B sia C valgono almeno 10
  - OR ha una semantica più complessa:
    - se A dipende da B o C, quale valore ha B?
    - es. l'applicazione Java 'carrello' è replicata su 10 server, quale è il valore intrinseco di ogni singola replica?
- **il valore è spesso una proprietà emergente dell'aggregato e non delle sue singole parti**

99

Esempio di propagazione valori

dipendenze

asset	dipendente	C	I	A
app	tomcat1	100%	0%	50%
tomcat1	server1	100%	100%	100%

asset	C	I	A
table	0	10	5
app	1	5	10
...	...	...	...

beni

asset	C	I	A
table	0	10	5
app	1	5	10
tomcat1	1	0	5
...	...	...	...

100

Semantica del modello di valorizzazione

- **volendo identificare delle linee guida generali:**
  - l'uso di dimensioni con semantica a livello di organizzazione (es. reputazione, perdite finanziarie) è molto utile per la raccolta di informazioni sull'effettivo valore dei beni
    - es. per questionari e interviste
  - l'uso di dimensioni con semantica legata agli aspetti di sicurezza delle informazioni è utile per valutare l'impatto in base alle relazioni tra i beni e la propagazione degli eventi di sicurezza
    - es. per uno strumento automatico di analisi
  - la combinazione può avvenire via trasformazioni

101