

Modelli sicuri di cooperazione



Il progetto di sicurezza di
un sistema di servizi



Modelli sicuri di cooperazione

- Contesto nazionale ed internazionale
- Struttura e requisiti di un sistema di servizi: il modello
- Vulnerabilità dei servizi
 - processi
 - natura del sistema



Scopo di un sistema di servizi

- È ormai noto che devono essere le informazioni a viaggiare e non le persone. Da ciò ne deriva che offrire all'utente un certo tipo di servizio significa svincolarlo completamente dall'onere di conoscere:
 - le tecniche di interazione tra l'utente e l'ente (front-office),
 - il modello organizzativo soggiacente (back-office),
 - la documentazione necessaria al servizio richiesto,
 - la coerenza e l'integrità dell'informazione nelle diverse basi dati coinvolte,
 - i passi procedurali previsti (workflow) dal servizio.



Processi del modello

■ Il modello di sicurezza che andiamo a proporre prevede i seguenti processi (o fasi logiche):

- Autorizzazione: che consiste nell'identificazione del richiedente e nell'autorizzazione all'erogazione del servizio,
- Attivazione: che permette di percorrere tutti i passi procedurali previsti dal servizio,
- Esecuzione: che consente di eseguire i procedimenti presso gli uffici/enti di competenza, previsti dal servizio richiesto,
- Erogazione: che fornisce l'output del servizio all'utente,
- Logging: che consente la tracciatura degli eventi.

F
A
L
L
B
A
C
K

C
A
L
L
C
E
N
T
E
R



Contesto internazionale

■ Analizzare il contesto internazionale (e successivamente quello nazionale) ci aiuta a meglio delimitare i confini dello studio e di conseguenza meglio individuare le caratteristiche di sicurezza da implementare ai fini dell'erogazione di un sistema di servizi.

Negli USA, paese leader nel campo dell'interoperabilità e della cooperazione applicativa, c'è grande fermento attorno alla definizione di standard tecnologici come XML, SOAP, ... che implementano in modalità nativa la sicurezza.

Il processo però è agli inizi, prova ne è che la Rand Corporation afferma che nessuna amministrazione pubblica americana espone i propri dati sensibili sotto Internet (sanità, tesoro, finanza, ...) e che il programma di e-Government è di recente costituzione (1999).



Contesto nazionale

Pochi concetti basilari:

- Il rispetto dell'autonomia decisionale è alla base di un qualsiasi sistema di servizi che prevede un rapporto di tipo inter-amministrativo: ad ognuno le proprie competenze e responsabilità.
- L'impatto sui modelli organizzativi e tecnici deve essere il **MINIMO**
- **MASSIMO** equilibrio tra i costi della sicurezza e l'abbattimento del rischio ottenuto
- Il servizio deve essere erogato dall'ente responsabile dello stesso o da un ente **DELEGATO**

Esempio: lo sportello unico alle imprese

- Servizio erogato dal Comune di carattere inter-amministrativo.
 - **PRIMA**: 43 autorizzazioni di tipo diverso rilasciate da enti a livello centrale, regionale e locale.
 - **DOPO**: un'unica richiesta presso il Comune.
- Basato sul processo di sincronizzazione dei procedimenti amministrativi e su un processo di delega al Comune definito da apposito regolamento
- Responsabilità del Comune: processo di autorizzazione, di attivazione e di erogazione.
- Responsabilità dell'Ente: processo di esecuzione e di logging



Modello dei processi e responsabilità

Front-office=

fornitore del servizio

■ Caratteristiche:

- Portale: Interfaccia unica x l'utente
- Possiede la delega degli enti

■ Responsabilità processo:

- **Autorizzazione:** identificazione del richiedente, e autorizzazione all'erogazione del servizio
- **Attivazione:** attivazione dei diversi procedimenti presso le sedi competenti e sincronizzazione degli stessi
- **Erogazione:** fornitura dell'output

Back-office=

responsabile del servizio

■ Caratteristiche:

- Detiene la base informativa del servizio (o di un suo passo procedurale)

■ Responsabilità processo:

- **Esecuzione:** svolgimento del passo procedurale che compone il servizio.



Modello dei processi e responsabilità

- Diverso è il caso del processo di fall back necessario a garantire l'univocità del dato e la coerenza dell'informazioni nelle basi dati dei diversi enti che concorrono all'erogazione del servizio (si pensi al caso di una variazione anagrafica, rilevata dal comune e che deve essere propagata al Ministero dell'Interno, a quello delle Finanze, all'ASL, all'INPS, ecc...). Infatti non esiste una regola ben specifica che consente di attribuirne la competenza. Si deve quindi pensare ad un processo che di caso in caso deve essere valutato ed imputato.
- Il processo di logging o tracciabilità degli eventi si deve pensare generalmente come un processo di tipo trasversale.
- Il processo di call center, volto ad assistere gli utenti si deve considerare anch'esso come un processo di tipo trasversale.



Vulnerabilità di un sistema di servizi

Quando si eroga un servizio in rete, il sistema informativo soggiacente è per definizione vulnerabile agli attacchi derivanti da utenti che, intenzionalmente o inavvertitamente, sfruttano buchi di sicurezza che possono derivare da:

- i sistemi di supporto,
- le applicazioni,
- dalla natura intrinseca dell'architettura di sistema,
- delle risorse utilizzate.



Processo/attacchi

030-N990-R030-N500M
030-N500M030-N500M

Abuso di privilegi.

Va evitato, attraverso un controllo degli accessi, che un processo autorizzato ad accedere ad un certo insieme di dati possa anche accedere ad altre informazioni per il cui accesso non ha ottenuto autorizzazioni.

Intercettazione delle informazioni.

Vanno implementate tecniche di crittografia o comunque tecniche atte a garantire la riservatezza delle informazioni nel riguardi di soggetti non autorizzati a conoscerne il contenuto.



Processo/attacchi

F
-
a
b
c
d
e
f
g
h
i
j
k
l
m
n
o
p
q
r
s
t
u
v
w
x
y
z

Affidabilità (autenticità) della fonte e integrità dell'informazione trasmessa.

È necessario premunirsi affinché le sorgenti da cui provengono le informazioni siano state preventivamente autenticate e che l'informazione trasmessa non sia stata in qualche modo manipolata ma corrisponda esattamente a quella trasmessa dalla fonte originale.

Distruzione del logging.

è necessario premunirsi affinché i file dove sono contenuti i dati della tracciabilità dell'evento (chi, come e quando) non siano modificati, rimossi o compromessi.



Il progetto di
sicurezza di
sistema di ser

Natura sistema/attacchi

National Defense Institute & Rand – Securing the U.S. Defense Information Infrastructure: a proposal approach

ar
t
t
e
t
t
e
-
s
c
r
a
e
o
n
g
e
n
i
t
à

Unicità

È necessario premunirsi da un attacco fisico basato sulla criticità di avere un sistema unico, come per esempio un sistema legacy adottando misure di ridondanza del sistema, di backup/recovery ed adottando specifiche politiche di accesso fisico al sistema.

Singularità

Caratteristica dovuta alla criticità di avere un sistema molto specifico come per esempio quello basato su comunicazioni satellitari. Valutare significativamente strumenti e mezzi alternativi.

Centralizzazione

Il fatto di avere un nodo unico o un unico processo rende critico e dannoso un eventuale fermo della risorsa. Valutare attentamente risorse di backup distribuite

Separabilità

Maggiore è la distribuzione delle risorse, maggiore l'esposizione agli attacchi. Valutare l'inserimento di nodi centralizzati per il controllo degli accessi.

Omogeneità

Un attacco prodotto su una risorsa può essere facilmente condotto su risorse omogenee. Diversificare ed integrare soluzioni alternative.



Il progetto di sicurezza di sistema di ser

Natura sistema/attacchi

National Defense Institute & Rand – Securing the U.S. Defense Information Infrastructure: a proposal approach

C
O
M
P
I
S
S
I
T
À
S
T
R
U
T
T
U
R
A
L
E

Ricettività

Poca efficienza di componenti strutturali del sistema: la robustezza di un sistema è assimilabile a quella del componente meno sicuro. Innalzare la sicurezza proteggendo la componente più critica.

Conoscenza

In caso di malafede o di riconducibilità a modelli e strutture note, è relativamente semplice sferrare un attacco sia fisico, sia logico. Aggiornare sempre i modelli architetturali.



Il progetto di
sicurezza di
sistema di ser

Natura sistema/attacchi

National Defense Institute & Rand – Securing the U.S. Defense Information Infrastructure: a proposal approach

A
d
a
t
t
a
b
i
l
i
t
à

Rigidità

In presenza di una configurazione poco flessibile, si è in difficoltà ad intervenire in maniera tempestiva.

Flessibilità

in presenza di una configurazione molto flessibile, si è in difficoltà ad intercettare in maniera tempestiva il tipo di attacco.

Ingenuità

Difficoltà a riconoscere un attacco dal normale funzionamento.



Il progetto di
sicurezza di un
sistema di servizi

Natura sistema/attacchi

National Defense Institute & Rand – Securing the U.S. Defense Information Infrastructure: a proposal approach

C
O
N
T
R
O
L
L
O
R
I
A
S
I
S
T
E
M
A

Limiti di capacità

Un sistema che lavora vicino alle sue capacità limiti è vulnerabile e collassabile più facilmente ad esempio con attacchi di tipo denial of service.

Difficoltà di recovery

Criticità dovuta ad una inibizione del recovery di sistema.

Assenza tracciabilità

L'assenza di monitoraggio dell'uso del sistema favorisce intrusioni sia di tipo autenticazione, sia di tipo autorizzazione.

Difficoltà di gestione

Numerosi aggiornamenti del sistema possono nascondere o facilitare potenziali attacchi.

Usabilità

La facilità dell'interfaccia di gestione è un pericolo per l'uso indiscriminato da parte di persone non competenti.



Il progetto
sicurezza di
sistema di ser

Natura sistema/attacchi

National Defense Institute & Rand – Securing the U.S. Defense Information Infrastructure: a proposal approach

RETOUR-23-030-N-0000M

Remotizzazione

Porre particolare attenzione al processi di autenticazione e di autorizzazione.

Apertura

Caratteristica dovuta all'utilizzo delle funzioni di sistema da parte di molteplici attori.



Il progetto di
sicurezza di
sistema di ser

Natura sistema/attacchi

National Defense Institute & Rand – Securing the U.S. Defense Information Infrastructure: a proposal approach

**M
E
S
O
N
I
S
P
E
R
I
C
O
L
I
D
E
A
T
T
A
C
C
I
A
M
E
T
T
E
R
I
A
L
I**

Accessibilità

Attacco fisico al sistema

Debolezza strutturale

Attacco fisico alle componenti "alimentazione" del sistema.

Dipendenza

Caratteristica dovuta ad un possibile attacco fisico alle risorse infrastrutturali (locali, impianti di condizionamento, ecc ...).