Ministero
dell'Economia
e delle Finanze

L’approccio di Consip alla sicurezza applicativa

Matteo Cavallini

consip

ULS
Unità Locale di Sicurezza

Chi sono

Dal 2007 Responsabile della Struttura Operativa della Unità Locale della Sicurezza MEF/Consip che raggruppa nella propria constituency:

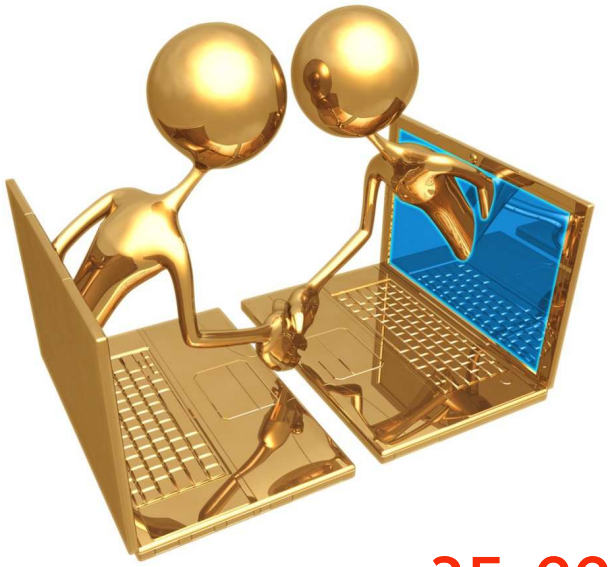
- Dipartimento del Tesoro;
- Ragioneria Generale dello Stato;
- Dipartimento Amministrazione Generale;
- Consip

Precedentemente ho partecipato al progetto di creazione del Gov-CERT.it (ora CERT-SPC) con il ruolo di esperto senior di sicurezza e nel passato ho ricopero vari ruoli di responsabilità nella progettazione, realizzazione e gestione delle infrastrutture di sicurezza informatica per il Ministero del Tesoro.

Ho inziato la mia carriera in Securteam come consulente

Lo scenario e l'esigenza

Consip attua le esigenze di sviluppo del MEF
principalmente attraverso contratti di outsourcing



100 sistemi applicativi

550.000 Function Point totali

50.000 Function Point annui

35.000 utenti esterni e 17.000 interni

I rischi tipici

The wire protocol guys don't worry about security because that's really a network protocol problem. The network protocol guys don't worry about it because, really, it's an application problem. The application guys don't worry about it because, after all, they can just use the IP address and trust the network

I ragazzi dei cavi non si preoccupano della sicurezza perchè è un problema di protocolli. I colleghi della rete non se ne preoccupano perchè è un problema delle applicazioni. Gli applicativi non se ne interessano perchè in fondo usano solo un indirizzo IP e si fidano della rete

Marcus J. Ranum

I rischi tipici

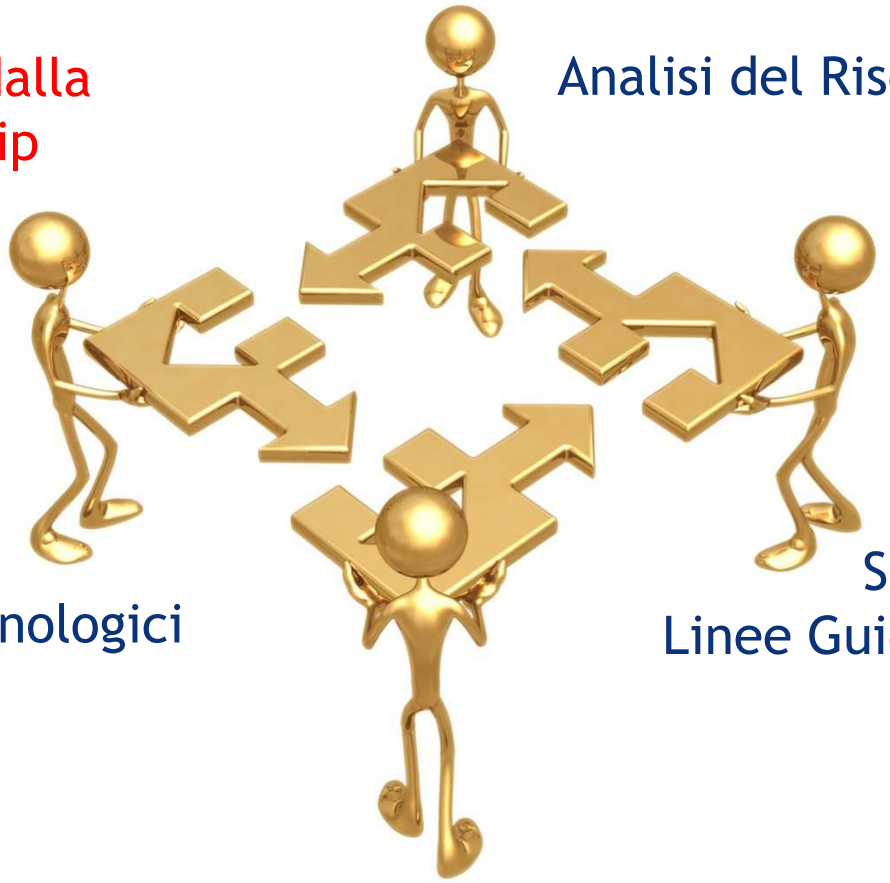
I've got an intelligence briefing, a security briefing, and a 90-minute budget meeting all scheduled for the same 45 minutes

Devo partecipare ad una riunione con l'intelligence, ad un incontro con la sicurezza e a un meeting di 90 minuti sul budget, tutto negli stessi 45 minuti

Martin Sheen in "The West Wing"

L'approccio complessivo per la sicurezza

Servizi svolti dalla
ULS MEF/Consip



Analisi del Rischio

Standard e
Linee Guida per lo sviluppo

Strumenti tecnologici

Contrattualistica e collaudi

L’analisi del rischio

Per i progetti applicativi è previsto che venga utilizzata una metodologia per l’analisi del rischio (Defender) e uno strumento automatizzato per l’esecuzione dell’analisi.
I risultati dell’analisi sono utilizzati per individuare le opportune contromisure di sicurezza da adottare.
I livelli di rischio sono quindi nuovamente ricalcolati alla luce delle misure adottate
E’ stata messa a punto una procedura che fissa i principali passi operativi da svolgere e le figure, interne ed esterne, da coinvolgere

consip

Ministero dell'Economia e delle Finanze

Le linee guida per lo sviluppo

Linee guida per l'utilizzo di strumenti crittografici nelle applicazione del MEF

Linee guida per il piano di test relativo alla sicurezza delle applicazioni web

Indicazioni per l'uso di prodotti programma

Linee Guida di programmazione Sviluppo e applicazioni "NET"

Linee guida di programmazione Sicurezza delle applicazioni Web

Standard programmazione Applicazioni Web Java J2EE (Java 2 Enterprise Edition)

I contratti di outsourcing

Nei contratti di outsourcing sono state inserite specifiche clausole legate alla sicurezza del software sviluppato
Per alcuni contratti, è stato previsto che il fornitore presenti, preventivamente al collaudo, una propria documentazione che attesta lo svolgimento di verifiche sulla sicurezza dell'applicazione e certifichi la conseguente assenza di vulnerabilità
(ad esempio Top Ten OWASP) nell'applicazione prodotta

In molti contratti sono state inserite clausole che legano il fornitore a seguire, oltre alle linee guida Consip, anche specifici standard sulla sicurezza delle applicazioni tra cui OWASP
Infine, sono previste specifiche penali che scattano qualora, nel corso del collaudo o dell'esercizio, emergano vulnerabilità applicative. Le penali sono maggiorate nel caso in cui derivi un danno dalla presenza delle vulnerabilità

Il collaudo delle applicazioni

Consip ha adottato un proprio Piano di test relativo alla sicurezza delle applicazioni web che si affianca al "normale" piano di test, teso alle verifiche funzionali dell'applicazione e allo stress test

Per alcune applicazioni sono state svolte caratteristiche attività di valutazione della sicurezza.

In particolare sono stati svolti:

- progetti di Secure Code Review sul software fornito
- sessioni di Penetration Test Applicativo

Infine, nella fase di profiling applicativo, Consip verifica approfonditamente i risultati delle analisi prestazionali delle applicazioni in collaudo, evidenziandone le possibilità di fine-tuning e prevenendone, nel contempo, reali o potenziali problematiche di esercizio

Gli strumenti tecnologici

Per le attività di collaudo e di gestione applicativa corrente, Consip si è dotata di un'apposito scanner per le vulnerabilità applicative

Stiamo valutando l'adozione di un Web Application Firewall che possa essere utilizzato per la prevenzione degli incidenti e, in caso di necessità, come patch virtuale per i sistemi vulnerabili

I servizi svolti dalla ULS MEF/Consip

L'Unità Locale di Sicurezza MEF/Consip è il
CERT interno per il MEF e Consip e svolge i servizi di:

GESTIONE INCIDENTI

- Analisi incidente
- Elaborazione strategia di risposta
- Gestione task force
- Report finale

I servizi svolti dalla ULS MEF/Consip

L'Unità Locale di Sicurezza MEF/Consip è il
CERT interno per il MEF e Consip e svolge i servizi di:

PREVENZIONE INCIDENTI

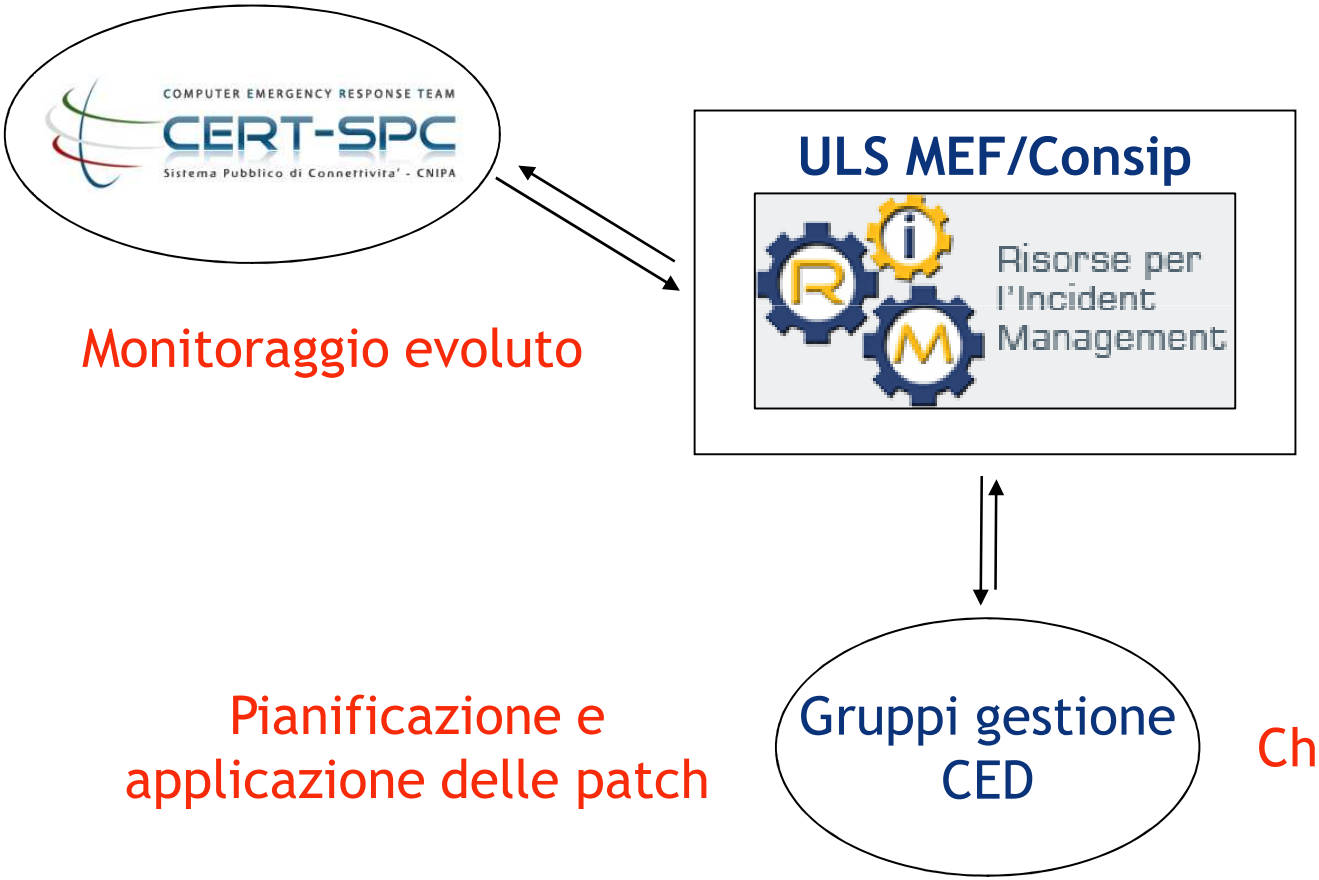
Servizi proattivi

- Sicurezza applicativa
- Collaborazioni
- Il Notiziario della ULS
- Seminari di approfondimento

Servizi reattivi

- Monitoraggio
- Gestione segnalazioni
- Supporto alle attività

L'aggiornamento degli ambienti



Monitoraggio evoluto

Monitoraggio interno svolto dai Reperibili ULS

Filtro e Triage delle segnalazioni

Dispatching interno delle segnalazioni

Pianificazione e applicazione delle patch

Chiusura della segnalazione

Conclusioni

Consolidamento ed attuazione del

Piano 2010 per la sicurezza delle applicazioni web

che prevede:

- aggiornamento e adeguamento linee guida sicurezza
- redazione linee guida per clausole contrattuali
- adozione modalità standard per penetration test
- acquisizione Web Application Firewall

Redazione di un documento di visione complessivo che valorizzi…

la forza del team!!!

consip

Ministero dell'Economia e delle Finanze

Grazie per l'attenzione

matteo.cavallini@tesoro.it
uls@tesoro.it