Ministero
dell'Economia
e delle Finanze

Le Unità Locali di Sicurezza: l'esperienza della ULS MEF/Consip

Matteo Cavallini

consip

Agenda

Lo scenario normativo: ruoli e compiti delle ULS

La ULS MEF/Consip

L'approccio operativo

I risultati ottenuti

Il Progetto di Collaborazione Consip/CNIPA

Lo scenario normativo: le regole tecniche

SPC - Componente Centrale di Sicurezza

CERT-SPC-C
CERT-SPC-R

Centro di Gestione SPC

Le "Regole tecniche SPC" sono state approvate dalla Commissione di Coordinameno SPC nel Novembre 2006 e quindi in seguito trasformate in DPCM. Sono state firmate dal Presidente Prodi il 1 aprile 2008, attualmente sono in attesa di pubblicazione sulla GURI

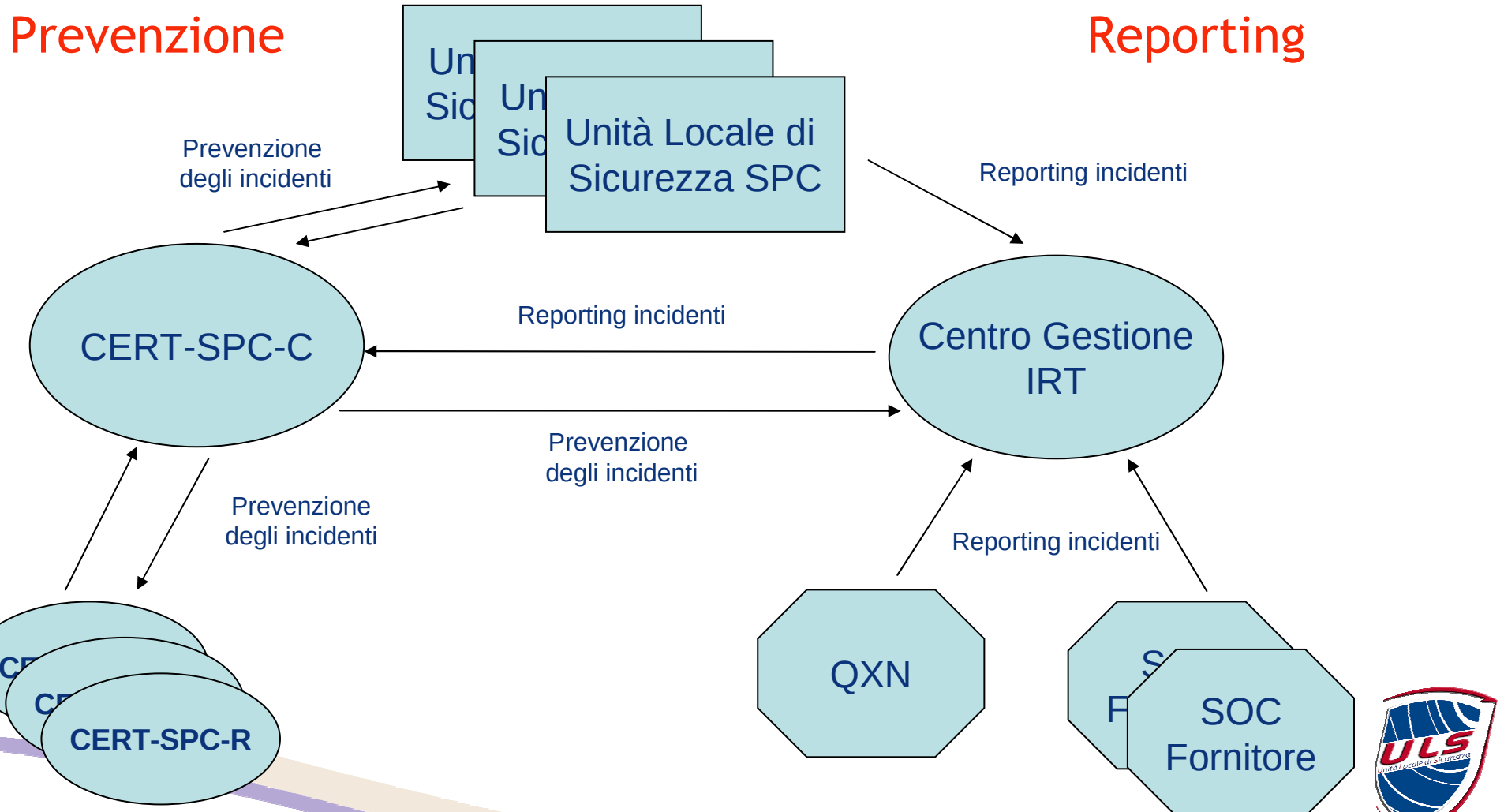
Lo scenario normativo: le regole tecniche

SPC - Componente Distribuita di Sicurezza

Unità Locale di Sicurezza SPC

Le **ULS sono responsabili** di gestire gli aspetti relativi alla **sicurezza delle infrastrutture** connesse al SPC situate **nell'ambito del dominio** di competenza e di **costituire l'interfaccia verso le altre strutture** organizzative che compongono il sistema di sicurezza del SPC.
Per dominio si intende l'insieme delle risorse e delle politiche che ricadono sotto la responsabilità di una specifica organizzazione. Un dominio può eventualmente essere scomposto in più "sottodomini".

Flussi informativi sulla sicurezza in SPC



Compiti dell'Unità Locale di Sicurezza

1. ***garantire*** la realizzazione ed il mantenimento almeno del ***livello minimo di sicurezza sul dominio di competenza***;
2. ***garantire*** che la ***politica di sicurezza*** presso la propria organizzazione sia ***conforme*** agli indirizzi e alle politiche di sicurezza emesse dalla Commissione;
3. ***interagire con la componente centrale*** per raccogliere, aggregare e predisporre nel formato richiesto le informazioni necessarie per verificare il livello di sicurezza del SPC;
4. ***notificare alla componente centrale ed al CERT-SPC-C***, secondo le modalità stabilite, eventuali ***incidenti informatici o situazioni di attenzione o vulnerabilità***;
5. ***adottare*** tutte quelle ***contromisure volte a limitare il rischio di attacchi*** informatici vecchi o nuovi;
6. ***eliminare*** eventuali ***vulnerabilità all'interno della rete***, individuate ***a seguito di segnalazioni di abuso*** causate da sistemi o infrastrutture della pubblica amministrazione violati dall'esterno e successivamente utilizzati per condurre illeciti.

Struttura dell'Unità Locale di Sicurezza

Presso ogni Unità Locale di Sicurezza sono attive le funzioni di ***IRT*** e ***Abuse Desk*** che sono coordinate dalle corrispondenti funzioni presenti nel CG-SIC.

IRT (Incident Response Team)

1. prevenzione degli incidenti informatici;
2. gestione degli incidenti informatici;
3. collaborare con le analoghe strutture presenti in SPC (CERT-SPC-C, Centro di Gestione della Sicurezza e altre Unità Locali di Sicurezza)

Abuse Desk

1. limitare possibili disservizi verso gli utenti SPC causati da abusi;
2. limitare il rischio che i riferimenti ad application server (es. mail server) della Pubblica Amministrazione siano inseriti in qualche black-list;
3. eliminare eventuali vulnerabilità all'interno della rete, individuate a seguito di segnalazioni di abuso;

L'iniziativa di Consip

A Dicembre 2006, di concerto con il DAG del MEF, Consip ha costituito la struttura operativa della Unità Locale di Sicurezza.

I tempi per l'inizio delle attività operative della ULS sono stati stimati in circa 5 mesi.

Da Maggio 2007 l'iniziativa è uscita dalla fase di start-up ed è entrata nella fase di pre-esercizio.

L'iniziativa del MEF

Da Marzo 2008 è stata costituita presso il DAG la "*Struttura di Governo della ULS*" che svolge compiti di indirizzo e coordinamento della struttura operativa ULS predisposta da Consip.

La Struttura di Governo della ULS stabilisce:

- i compiti, le responsabilità e i livelli di servizio erogati dalla ULS;
- l'utilizzo delle caselle di posta ufficiali in uso alla ULS;
- le modalità di comunicazione degli eventi rilevanti;
- le modalità di escalation in caso di emergenza.

Attuale scenario operativo

Attuale scenario operativo

Gestione degli incidenti

Filtro e Triage delle Segnalazioni
Definizione piano di contenimento

L’approccio operativo - 1

Al fine di creare un framework per l’IRT sono state realizzate 12 di procedure operative volte a regolamentare le attività che il Team avrebbe svolto nel campo della prevenzione e gestione degli incidenti.

Queste procedure sono state successivamente condivise ed approvate internamente all’IRT e, ad oggi, sono estesamente applicate dai componenti del Team.

L’approccio operativo - 2

Per la formazione del team, data la numerosità e la natura delle attività, si è ritenuto conveniente adottare un approccio a matrice con risorse solo parzialmente dedicate all’IRT.

Sono state quindi individuate le unità che svolgono attività collegate alle problematiche di prevenzione e gestione degli incidenti informatici, ne sono stati contattati i responsabili ed è stato chiesto loro di indicare una risorsa di riferimento ed una di back-up per le attività dell’IRT.

I componenti del Team, a seconda delle funzioni svolte, sono stati suddivisi in:

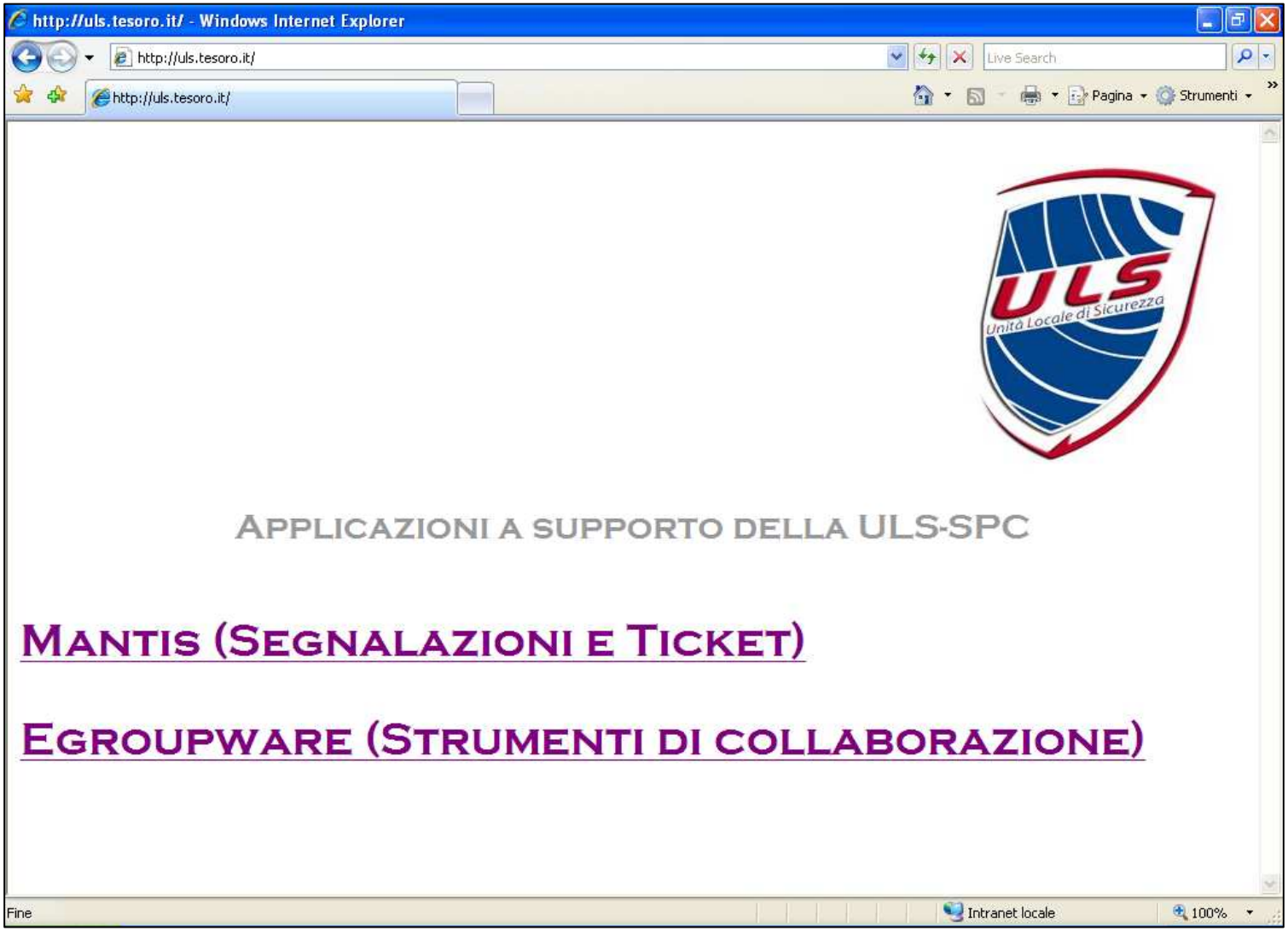
- Reperibili IRT
- Risorse IRT

L’approccio operativo - 3

Ai vari gruppi di Risorse IRT è stato quindi chiesto di elencare le principali tecnologie che sono in uso presso i relativi ambiti di riferimento.

Sulla base delle indicazioni fornite è stata stilata una lista (Technology list) che viene utilizzata per le attività di monitoraggio.

Gli strumenti a disposizione del Team



I risultati ottenuti - 1

La creazione di un gruppo interdirezionale, coeso e motivato assieme al varo di procedure “ad hoc” e allo sviluppo di adeguate applicazioni software ha permesso di gestire da Maggio 2007 :

- 145 segnalazioni di prevenzione incidenti;
- 4 incidenti, chiusi nell’arco della giornata lavorativa;
- 2 emergenze, chiuse in meno di 24 ore.

I risultati ottenuti - 2

Tra le iniziative di maggior rilievo che sono state messe in campo dalla ULS MEF/Consip si segnalano:

- Workshop Consip di lancio dell'iniziativa e di sensibilizzazione sulle tematiche della prevenzione e gestione degli incidenti;
- Predisposizione di un "Notiziario della Unità Locale di Sicurezza" con cui far crescere la sensibilità degli utenti verso le tematiche di sicurezza informatica (ad oggi ne sono stati pubblicati 42);
- Progetto Pilota con il CNIPA sul Monitoraggio Evoluto che pone la ULS MEF/Consip all'avanguardia nella PA.

Il Progetto Pilota con CNIPA

E’ stato avviato un Progetto Pilota con il CNIPA finalizzato a determinare il servizio di “Monitoraggio evoluto” erogato dal CERT-SPC-C alle ULS delle Amministrazioni.

Tale progetto consta di 3 fasi:

Fase 1 - definizione delle modalità operative e tecniche del sistema evoluto di monitoraggio (basato sulle tecnologie individuate dalle Amministrazioni). Erogazione delle informazioni tramite appositi bollettini del CERT-SPC-C.

Fase 2 – modellizzazione dei processi di prevenzione e gestione degli incidenti informatici presso le ULS. Definizione di un set standard di strumenti software (Open Source) in uso alla ULS.

Fase 3 – organizzazione di un evento comune CNIPA/Consip/MEF per la pubblicazione dei risultati e la distribuzione del materiale prodotto.

Il Progetto Pilota con CNIPA

Il GdL che ha seguito le attività di progettazione e redazione del documento di "Monitoraggio Evoluto" e di progettazione e realizzazione delle Risorse per l'Incident Management" (RIM) è costituito interamente da personale della ULS MEF/Consip e del CERT-SPC-C.

Per completare il progetto non sono state utilizzate risorse economiche aggiuntive.

I risultati: il Monitoraggio Evoluto

Nella progettazione del servizio di Monitoraggio Evoluto si è deciso di mantenere un approccio differenziato per le vulnerabilità informatiche e per le minacce. Di conseguenza il servizio di Early Warning erogato dal CERT-SPC è stato diversificato per tipologia di contenuti: Segnalazioni per le vulnerabilità e Avvisi per le minacce. Inoltre, al fine di veicolare tra le ULS delle Amministrazioni aderenti ad SPC informazioni di carattere meno tecnico o analisi di più alto livello è stato predisposto un Notiziario Giornaliero, all'interno del quale vengono anche riprese le informazioni eventualmente reperite dalle ULS.

I risultati: il Monitoraggio Evoluto

Una delle principali innovazioni è rappresentata dalla possibilità di effettuare il **Monitoraggio effettuato dal CERT-SPC in correlazione con le tecnologie di interesse per le amministrazioni.** A tal fine è stato predisposto uno specifico strumento finalizzato al censimento delle tecnologie di interesse.

Le Risorse per l'Incident Management (RIM)

Le RIM sono costituite da 3 applicazioni Open-Source personalizzate nell'ambito del progetto CNIPA/Consip.

Al fine di rendere il più semplice possibile l'integrazione con gli ambienti di produzione degli utenti finali, l'ambiente è fornito sotto forma di "*Virtual Appliance*".

L'installazione quindi risulta particolarmente semplice, consistendo nella configurazione di alcuni parametri relativi al proprio ambiente operativo.

Le Risorse per l'Incident Management (RIM)

VMWare

Aprire il file
Configurare i parametri di rete e di posta

Le Risorse per l'Incident Management (RIM)

Prossimi passi

- Workshop sulla sicurezza delle applicazioni Web;
- Evento di presentazione dei risultati della collaborazione con il CNIPA e distribuzione del DVD contenente le RIM;
- Proposizione di un nuovo progetto di collaborazione finalizzato alla crescita della community delle ULS;
- Partecipazione ad attività di testing e simulazione di incidenti informatici.

Grazie per l'attenzione

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