



La sicurezza delle Web Application

Giacomo Segalli – CEO

Paolo Perego – Senior Consultant

eSecurity Lab

25 Gennaio 2007



- Spike Reply è l'azienda del Gruppo Reply specializzata nella Sicurezza delle Informazioni e nella Tutela dei Dati.
- La missione di Spike Reply e' quella di consentire alle aziende Clienti di stabilire relazioni di Fiducia con i loro interlocutori (Clienti, Partner, Azionisti, Cittadini, ...) e di abilitare lo svolgimento dei loro processi di business in condizioni di Sicurezza, supportandoli nello sviluppo delle idonee strategie e nella implementazione delle appropriate soluzioni per una gestione efficace della Sicurezza delle Informazioni.

Aspetti Economici

- Analisi Costi / Benefici
- Valutazione Impatti
- Analisi dei Rischi

Aspetti Strategici

- Obiettivi Aziendali
- Budget Aziendali
- Piano integrato della sicurezza

Aspetti Legali

- Leggi
- Normative
- Standard di Sicurezza

Aspetti Organizzativi

- Risk Analysis & Management
- Definizione Ruoli e Responsabilita'
- Formazione Risorse Umane
- Documentazione e Procedure

Aspetti Tecnologici

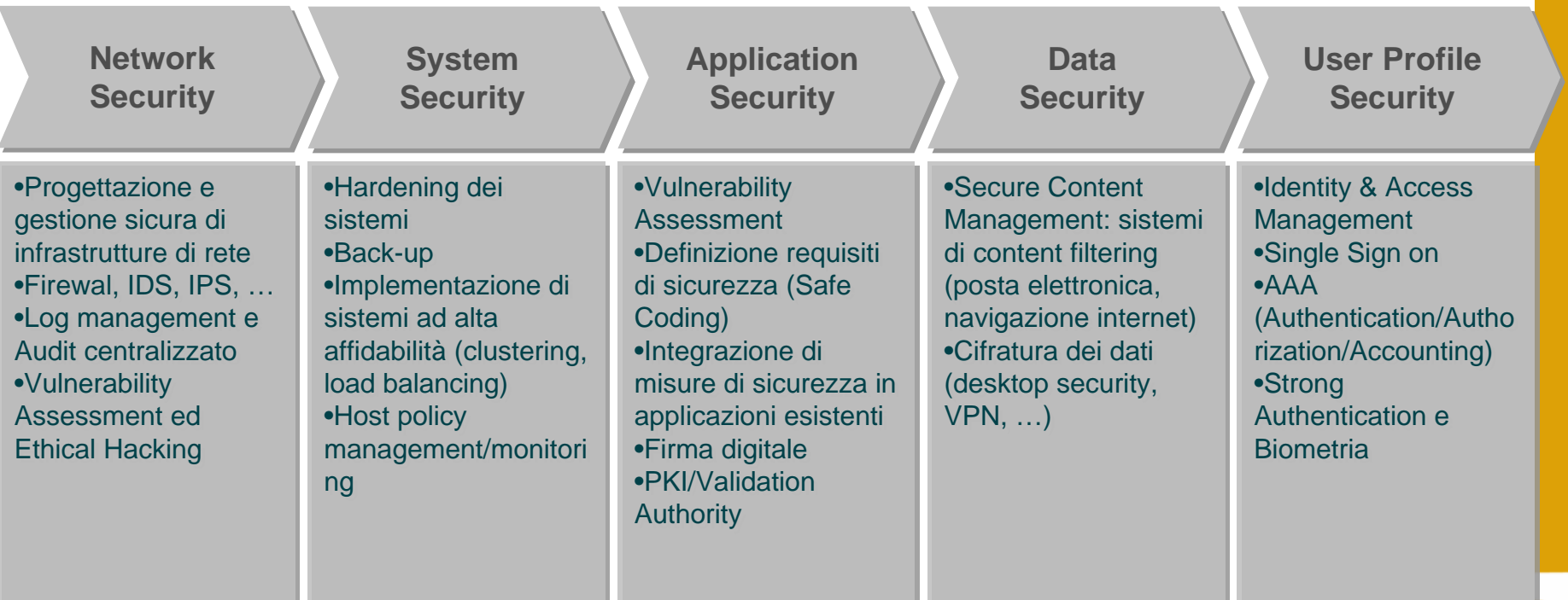
- Verifica livelli di Sicurezza
- Implementazione delle contromisure
- Gestione delle contromisure
 - Sicurezza fisica
 - Sicurezza logica

Spike Reply ha composto una proposizione d'offerta Integrata, Coerente e Completa:

- Analisi e Pianificazione
(Risk Analysis & Management)
- Implementazione Processi e Strumenti
(System Integration)
- Gestione e Controllo
(Governance)



Competenze nella catena del valore della sicurezza ICT *(Fonte SIRMI)*



Servizi professionali e di consulenza trasversali a tutta la catena del valore:

Security Strategy & Compliance	<ul style="list-style-type: none"> • Piani e sistemi di Business Continuity & Disaster Recovery • Definizione e gestione dell'impianto documentale (Politiche Generali e Procedure Operative di Sicurezza) • Consulenza per l'analisi e la gestione del rischio • Sistemi di Gestione della Sicurezza delle Informazioni (ISMS) a norma BS7799 • Adeguamento Privacy (D.Lgs 196/03); definizione del DPSS; impianto normativo • Impatti delle leggi, normative, best practice sul Sistema di Sicurezza (SOX, L.231, Basilea II, ITIL ...)
Security Check & Control	<ul style="list-style-type: none"> • ICT Security Assessment (verifica generale degli aspetti di sicurezza (LOFTA)) • Vulnerability Assessment (identificazione delle vulnerabilità di sicurezza informatica) • Ethical Hacking / Penetration Test (identificazione e verifica pratica delle brecce informatiche: internet, extranet, intranet, applicativo, ...)
Security Governance	<ul style="list-style-type: none"> • Security Event Management / Log Correlation / ... • Vulnerability & Patch Management • Consolidamento, Gestione, Presidio di soluzioni di ICT Security • Secure Application Building (supporto ai team di sviluppo SW e all' intero "Apps Lifecycle Mgmt" per la realizzazione di applicazioni sicure)

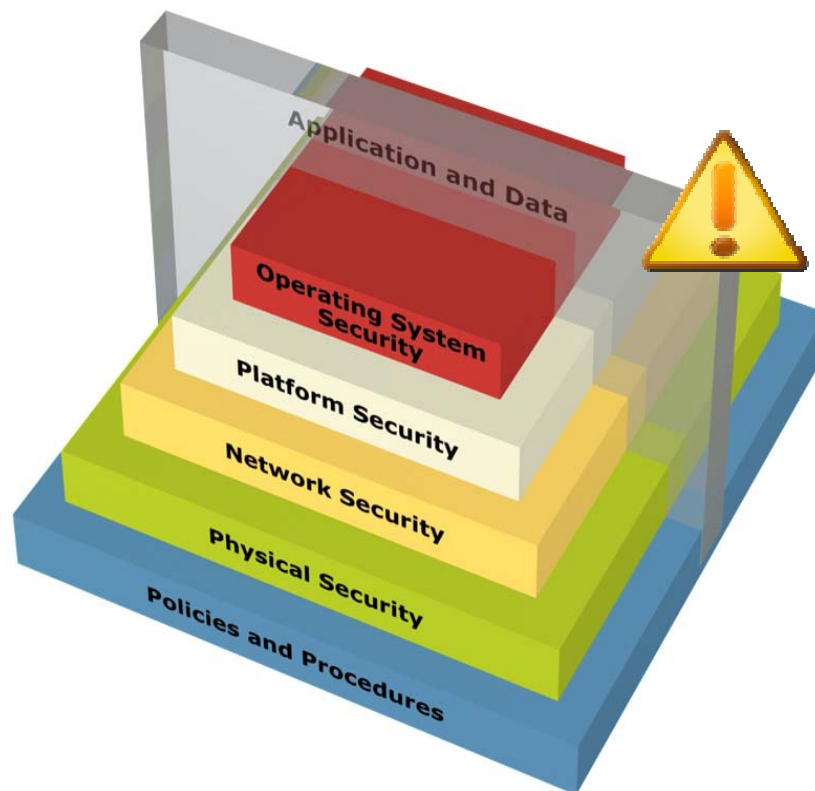


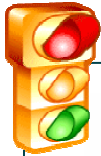
La sicurezza delle Web Application: Secure Application Building

Come integrare la sicurezza nel Software Development Life Cycle

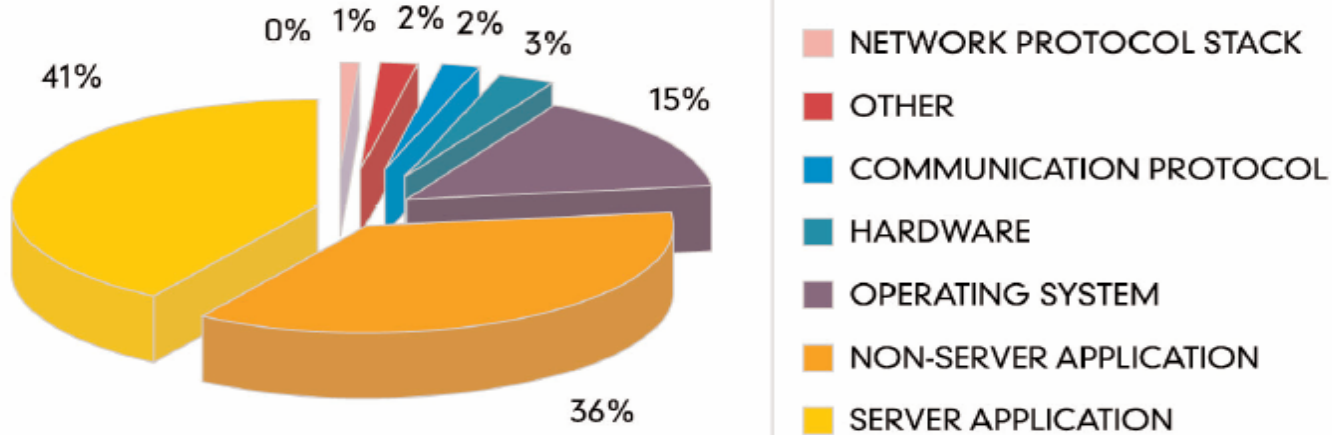


Gli **attacchi applicativi** consistono in tutte le azioni mirate direttamente al livello 7 della pila OSI che possono compromettere la **confidenzialità, integrità e disponibilità dei dati.**





92% of reported vulnerabilities are in applications, not networks



SOURCE: NIST

*“Today over **70% of attacks** against a company’s network come at the **Application Layer**, not the Network or System layer.”*

Fonte - Gartner Group

Tipologia	Possibile obiettivo
<ul style="list-style-type: none">• SQL Injection• Forceful browsing• Cross Site Scripting• Cross Site Tracing• SessionID Tampering	<ul style="list-style-type: none">• Compromissione DB• Bypass autorizzazione• Attacco credenziali utente• Attacco credenziali utente• Privilege Escalation



La problematica coinvolge **ogni elemento legato all'applicazione**, dall'utente finale fino al database server di back-end

CAUSE DELLE VULNERABILITÀ

La problematica della sicurezza non è stata efficacemente affrontata durante la fase di progettazione e sviluppo dell'architettura

Mancata adozione delle best practices di sicurezza per lo sviluppo di codice sicuro

Misconfiguration dei sistemi




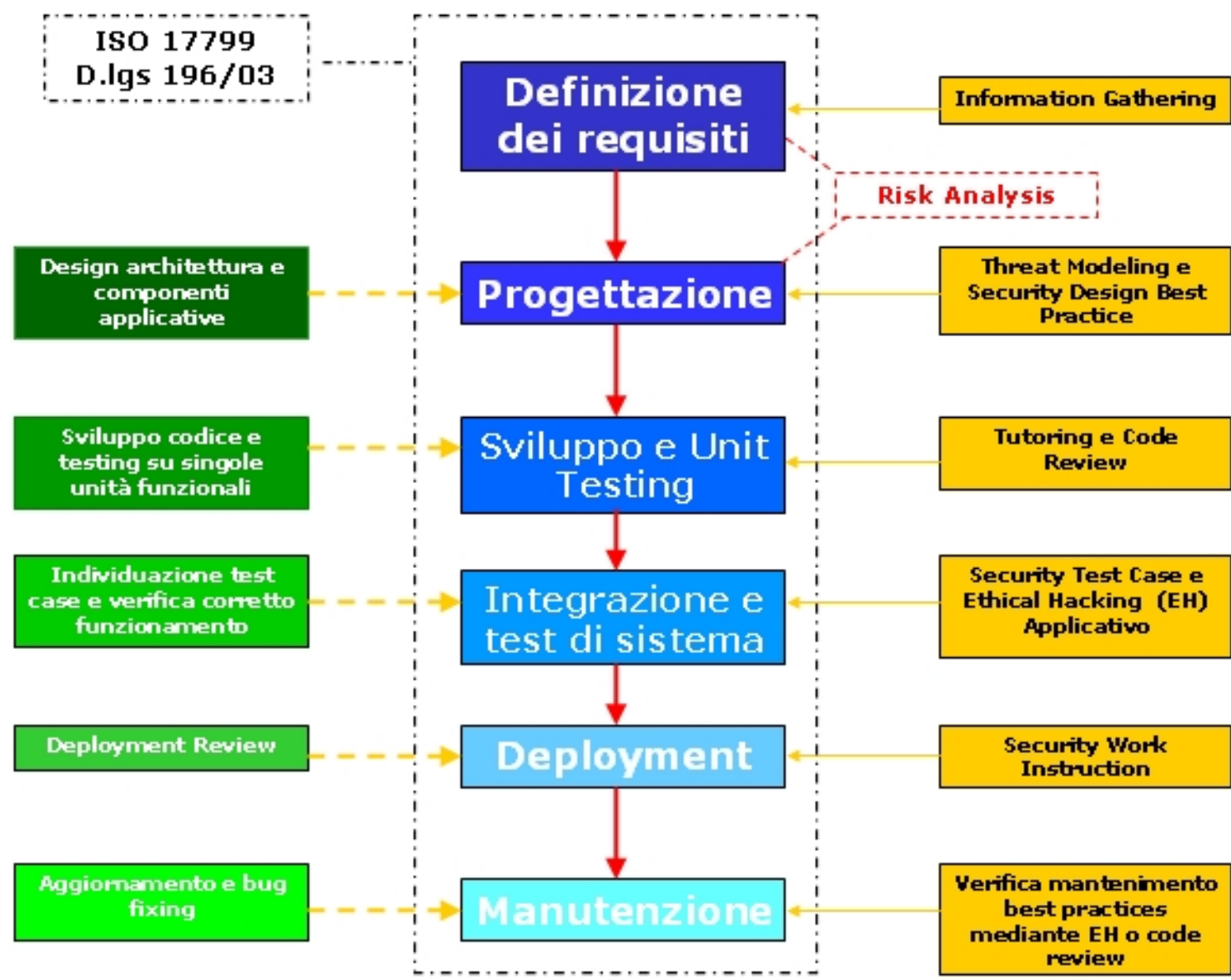
Applicazioni Web “Business Critical”

Deployment di applicazioni web sempre più complesse

Integrazione di servizi web tra soggetti diversi

Ricorso ai Web Services


L'importanza della **sicurezza** dei servizi basati su web è destinata ad **aumentare**:



Definizione dei requisiti

Ambito: Definizione dei requisiti funzionali dall'applicativo.

Obiettivo: Raccogliere le informazioni necessarie al fine di definire un modello completo dell'applicativo analizzato

Area Intervento Spike: Information Gathering

Progettazione

Ambito: Design dell'infrastruttura applicativa

Obiettivo: Definire le linee guide di sicurezza che gli sviluppatori dovranno seguire al fine di scrivere una Web Application secondo i criteri di sviluppo di codice sicuro.

Area Intervento Spike: Threat Modeling, Security Design Best Practice

Sviluppo e Unit Testing

Ambito: Sviluppo del codice applicativo

Obiettivo: Ottenere una Web Application scritta secondo le Best Practice di sviluppo di codice sicuro.

Area intervento Spike: Tutoring Team di Sviluppo, Code Review

Integrazione e Test di Sistema

Ambito: Fase di test funzionale dell'applicazione

Obiettivo: Verificare che gli obiettivi di Sicurezza individuati nella fase di Definizione siano stati rispettati.

Area Intervento Spike: Ethical Hacking Applicativo

Deployment

Ambito: Messa in produzione dell'applicazione

Obiettivo: verificare la corretta configurazione dei sistemi che ospiteranno l'applicativo per eliminare tutte le possibili vulnerabilità architetturali legate ad una non corretta configurazione sistemistica.

Area Intervento Spike: "Work Instructions" di Sicurezza

Manutenzione

Ambito: Aggiunta di nuovi moduli o modifica di quelli già esistenti

Obiettivo: Verificare che le successive modifiche del codice applicativo o aggiunte di nuovi moduli, rispettino i requisiti di sicurezza definiti.

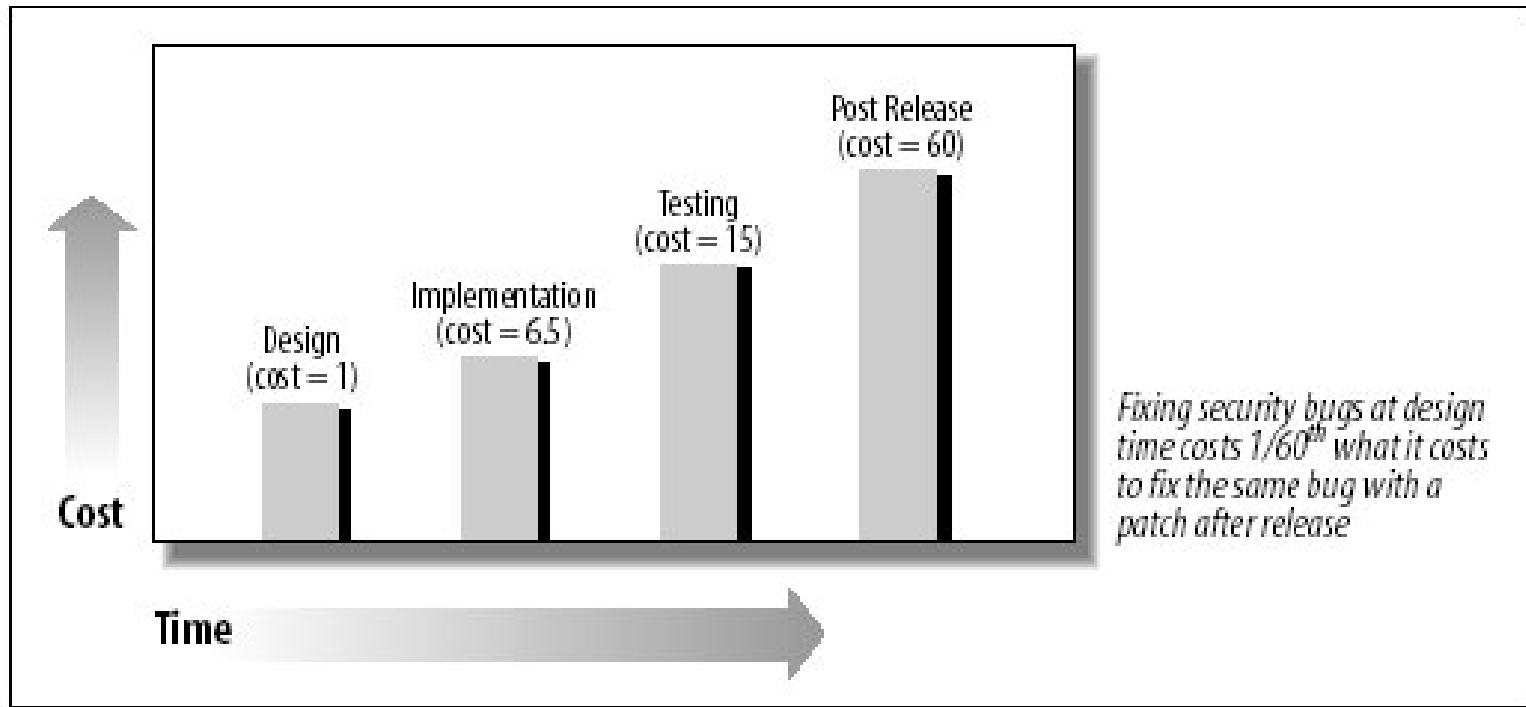
Area intervento Spike: Ethical Hacking Applicativo, Code Review

Il ROI legato alla metodologia di S.A.B.

La metodologia di S.A.B. riduce notevolmente il numero di “Security Bug” che possono presentarsi nelle ultime fasi del ciclo di sviluppo



Abbattimento dei costi e incremento del R.O.I.



IBM Systems Sciences Institute statistics

- sviluppare codice sicuro introduce una metodologia rigorosa che porta alla generazione di software
 - ben documentato
 - ampiamente testato
 - facilmente manutenibile
- sviluppare codice sicuro permette di poter condurre il proprio business attraverso una rete come Internet con un buon margine di confidenza sul grado di affidabilità, riservatezza e protezione dei dati da parte dell'applicazione
- sviluppare codice sicuro permette di avere un ritorno di immagine presso i propri clienti grazie all'affidabilità e alla continuità di servizio che possono essere garantite sul campo
- il codice sviluppato è conforme agli standard ISO 17799 e in adempimento della legge sulla privacy (D.lgs 196/03).

Domande ?

Giacomo Segalli

email: g.segalli@reply.it

Paolo Perego

email: p.perego@reply.it

