



L'analisi di sicurezza delle applicazioni web: come realizzare un processo nella PA

Stefano Di Paola

CTO
Minded Security





OWASP Day per la PA
Roma
5, Novembre 2009

Chi Sono

- ➊ Ricercatore in ambito sicurezza informatica, consulente e Penetration Tester
- ➋ Progettista software
- ➌ Ricercatore di Vulnerabilità (Adobe Reader, Flash, Microsoft, Google)
- ➍ Membro e direttore Ricerca e sviluppo di OWASP Italia
- ➎ Publication/Talks of Research Papers
- ➏ CTO @ Minded Security Application Security Consulting
- ➐ Responsabile delle attività di WAPT
- ➑ Lead Auditor ISO 27001:2005



Agenda

-  **Introduzione**
-  **Analisi di sicurezza delle App Web**
-  **Il punto di vista nella PA**
-  **Realizzare un processo nella PA**



Cos'e' una applicazione Web

- Applicazione accessibile via web per mezzo di una rete informatica
- Diffuse dagli anni 90 e impostesi negli anni 2000
- Facili da sviluppare
- Relativamente facili da usare
- Hanno sostituito molte applicazioni “desktop” (Email, operazioni bancarie...)
- Hanno il pregio di essere pubblicamente accessibili



La sicurezza delle applicazioni web

- Hanno lo svantaggio di essere pubblicamente accessibili
- Sono altamente diffuse
- Permettono di fare accedere a dati centralizzati esponendoli ad accessi non autorizzati
- Offrono utilizzo di risorse esponendo servizi e macchine



La Sicurezza delle Informazioni

- Si applica a:
 - Sicurezza dei processi industriali
 - Sicurezza del software
- Si basa sul valore dell'informazione:
 - Asset inventory
 - Risk Analysis
- La Triade CIA
 - Confidentiality
 - Integrity
 - Availability



Il valore dell'informazione

🌐 E' stimabile sulla base dei:

- ▶ Requisiti di Business
- ▶ Requisiti di Cogente
- ▶ Requisiti di Benchmark e Contrattuali

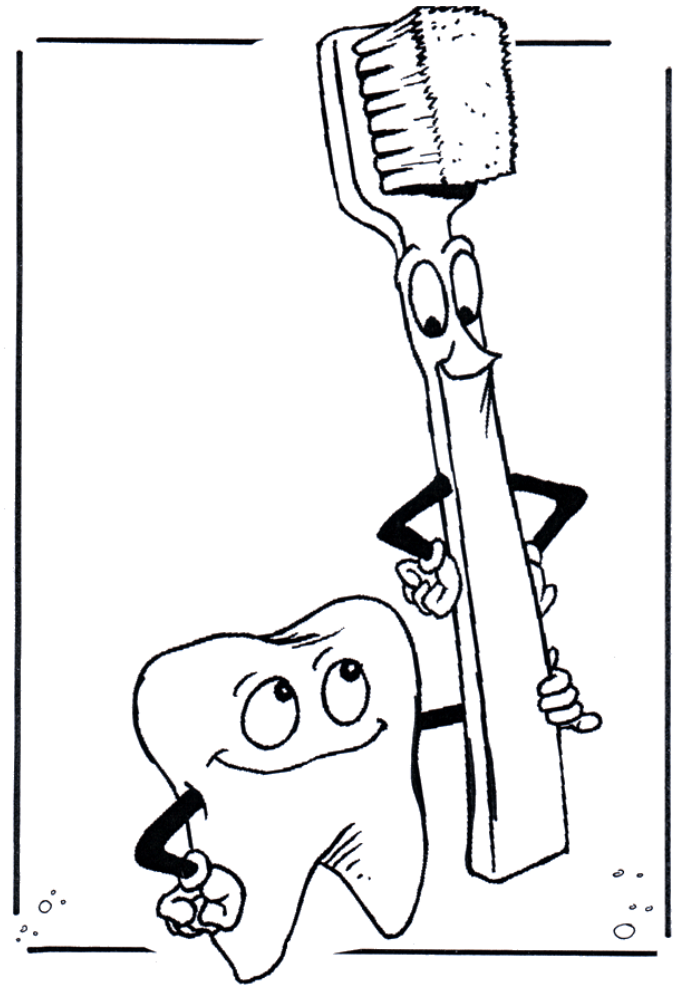
🌐 Come si stima il valore dell'informazione?

- ▶ Ci sono due fasi fondamentali:
 - **Asset inventory:** una volta determinate le informazioni da proteggere si segue il flusso di tale informazione nel processo (industriale o Software) e si stabiliscono i beni (asset) di valore effettuando un inventario.
 - **Risk Analysis:** sulla base dell'inventario si definiscono le esposizioni degli asset a minacce e l'impatto sulla attuazione delle minacce, stabilendo successivamente una valutazione del rischio (Qualitativa o Quantitativa).



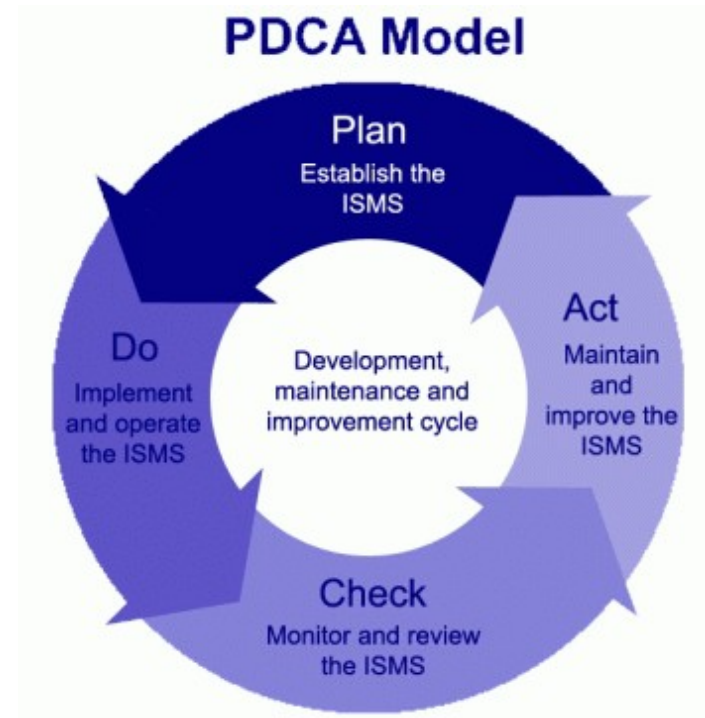
Le misure Preventive

- Sulla base delle stime di impatto si costruiscono le misure preventive.
 - ▶ Autenticazione (Authentication)
 - ▶ Autorizzazione (Authorization)
 - ▶ Identificazione (Identification)
 - ▶ Responsabilità (Accountability)
 - ▶ Gestione degli Incidenti (Incident Handling)
 - ▶ Monitoraggio (Logging & Monitoring)



Il Ciclo PDCA - Il processo generico

- **Plan:** Stabilisce una politica di sicurezza in relazione agli obiettivi, i goal, i processi e le procedure per controllare il rischio e migliorare la sicurezza delle informazioni.
- **Do:** Implementa e mette in atto le politiche di sicurezza, i controlli, i processi e le procedure .
- **Check :** Verifica e dove possibile misura, le performance delle politiche di sicurezza e gli obiettivi nella loro applicazione. Riporta i risultati alla dirigenza per la revisione.
- **Act:** Risolve le problematiche riportate in fase Check attraverso azioni correttive e preventive per apportare un continuo miglioramento del sistema.



Gli standard per la Sicurezza delle Informazioni

- ➊ Sono sempre più richiesti sul mercato
- ➋ Si basano su common practice
- ➌ Si applicano ai processi
- ➍ Nascono per esigenza di uniformità
- ➎ Hanno punti in comune
- ➏ Sono descrizioni di processo valutabili attraverso l'applicazione di controlli
- ➐ Esistono decine di Standard perchè ognuno si applica a realtà o troppo specifiche o troppo generiche



L'Esempio ISO27001 - I Domini

- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communication and operational management
- Access control
- Systems development and maintenance
- Information security and incident management
- Business Continuity Plan
- Compliance



Applicazione degli Standard al SDLC

ISO 17799 Reference	
9.6.1 – Information Access Restriction	Authentication and Authorisation
9.7.1 – Event Logging	Logging
10.2 – Security in Application Security 10.2.1 – Input Data Validation 10.2.2 – Control of Internal Processing 10.2.3 – Message Authentication 10.2.4 – Output Data Validation	Data Validation
10.3 – Cryptographic Controls 10.3.2 – Encryption 10.3.3 – Digital Signatures 10.3.4 – Non-repudiation Services 10.3.5 – Key Management	Cryptography
12.1.4 – Data Protection and Privacy of Personal Information	Privacy



Il processo - Buone Prassi

1. Istituire un programma di sensibilizzazione
2. Effettuare verifiche applicative
3. Comprendere i requisiti di sicurezza
4. Implementare pratiche di programmazione sicura
5. Costruire procedure di risoluzione di vulnerabilità
6. Definire delle metriche e monitorarle
7. Definire linee guida di sicurezza operativa



Le attività di verifica della sicurezza del Software

- 🔍 Sono le attività di verifica del processo applicato
- 🔍 Analisi sicurezza dell'architettura
 - ▶ Considera e analizza le soluzioni di sicurezza nei punti critici della applicazione
- 🔍 Web Application Penetration Test
 - ▶ Simula un attacco effettuato da utenze malevoli senza avere accesso alle informazioni interne della applicazione
- 🔍 Secure Code Review
 - ▶ Analizza e individua le problematiche di sicurezza avendo a disposizione il codice sorgente della applicazione.



Perchè è importante

- ➊ Qualità del codice (corretto funzionamento)
- ➋ Protezione dei dati:
 - ▶ Privacy
 - ▶ Identity Theft
 - ▶ Accesso a informazioni interne riservate
- ➌ ... e delle risorse
 - ▶ Accesso a risorse non autorizzato

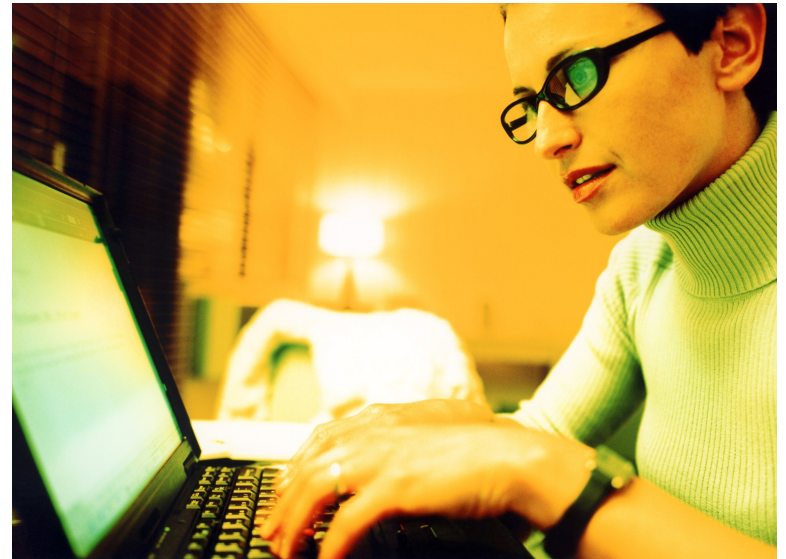


Il Punto di Vista nella PA



Applicazioni Web nella PA

- ➊ Per il cittadino
 - ▶ E-government
 - ▶ E-procurement
 - ▶ E-democracy
- ➋ Per la gestione i dati interni
 - ▶ Applicazioni di gestione
 - ▶ Email interne
 - ▶ Accesso a informazioni riservate (comunicazione inter-istituto)



L'importanza dei dati e non solo...

🕒 Privacy

- ▶ Acquisizione di dati sensibili

🕒 Privilege escalation

- ▶ Identity Theft

🕒 Utilizzo di risorse

- ▶ Accesso non autorizzato
- ▶ Attacchi ad altre strutture



Dlgs. 196/03

- Nasce come summa di più standard ponendo l'accento sulla gestione del dato sensibile
- Si basa sul:
 - ▶ riconoscimento del diritto del singolo sui propri dati personali
 - ▶ fatto che "Chiunque ha diritto alla protezione dei dati personali che lo riguardano"



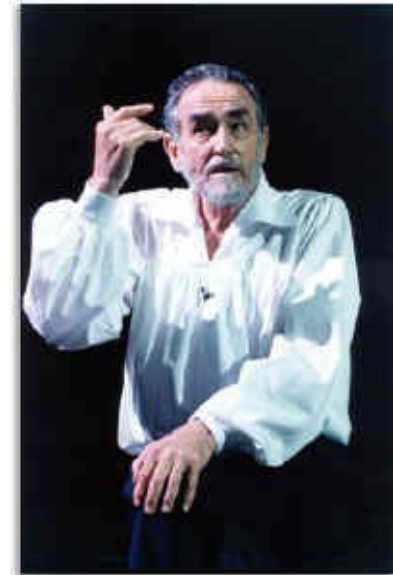
Dlgs. 196/03 - Inoltre...

- ➊ L'Analisi economica del diritto (EAL=Economic Analysis of Law) riconosce il suo valore in quanto si è nella situazione in cui:
 - ▶ Il danneggiato non ha vantaggi dall'attività del danneggiante
 - ▶ Il danneggiato non può far nulla per ridurre il rischio di essere danneggiato
 - ▶ Il danneggiato non ha le informazioni necessarie per dimostrare il comportamento colposo del danneggiante
 - ▶ Il danneggiante è l'unico a ricavare dei vantaggi nello svolgere l'attività pericolosa
 - ▶ **Il danneggiante è l'unico che può ridurre il rischio**
 - ▶ **Il danneggiante è l'unico a sapere cosa ha fatto**
- ➋ Dove danneggiante è inteso come
 - ▶ “Colui che crea le condizioni perchè si verifichi il fatto”



Definire un processo nella PA - Gli attori

- L'organizzazione
 - ▶ Dirigente
 - ▶ Responsabile
 - ▶ Operatore
- Il team di sviluppo interno delle applicazioni
- L'outsourcing



La dirigenza

- ➊ Sensibilizzazione sulle tematiche
- ➋ Definizione delle responsabilità
- ➌ Formazione di alto livello
- ➍ Identificazione del valore del dato
- ➎ Richiesta di commitment
- ➏ Organizzazione del budget
- ➐ Inserimento tra i requisiti del software nei capitolati tecnici di gare.



Il team di sviluppo interno

Formazione

- ▶ Portare consapevolezza nell'operato durante lo sviluppo
- ▶ Parlare un linguaggio comune
- ▶ Comprensione del processo PDCA
- ▶ Qualità del software come qualità dei servizi

Analisi delle criticità

- ▶ Identificare le criticità per definire le soluzioni

Definizione delle soluzioni

- ▶ Identificazione delle soluzioni alle criticità
- ▶ Corretta implementazione



Outsourcing - Dare impulso all'economia

- Richiedere che sia effettuato un processo di qualità.
- Richiedere che sia effettuato un processo di testing della sicurezza.
- Definire, insieme ai fornitori, una politica di gestione nella eventualità di individuazione di problematiche di security nella fase di produzione.



Conclusioni

La sicurezza del software

- ▶ è un processo
- ▶ è un super insieme degli aspetti di networking e data retention
- ▶ si interseca con il processo di qualità del software

La sicurezza del software nella PA

- ▶ è strettamente legata al dlgs 196/03
- ▶ è fortemente legata alla sensibilizzazione degli attori
- ▶ deve essere richiesta anche ai fornitori di software



Grazie!

Grazie!

:)

Domande?



Minded
— security —

Stefano Di Paola

stefano.dipaola@mindedsecurity.com

