LA SICUREZZA DEI SERVIZI WEB 2.0: MATRIX E VIRGILIO.IT

Matrix S.p.A., società del Gruppo Telecom Italia dedicata alla creazione di servizi web 2.0 e al marketing su canali web e mobile, con la collaborazione di Spike Reply ha definito e implementato un innovativo processo di gestione degli aspetti di sicurezza funzionali e tecnologici dei propri prodotti. Parte importante dell'attività consiste nella costante sensibilizzazione dei dipendenti e collaboratori con funzioni aziendali legate alla generazione di business al fine di far percepire la sicurezza come una opportunità e non come ostacolo al Time To Market.

CONTESTO

Matrix S.p.A. è una società storica del panorama di Internet italiano. Propone agli utenti innovativi servizi propri del Web 2.0

All'interno del Gruppo Telecom Italia, Matrix S.p.A.:

- Gestisce la creazione di servizi Web 2.0 su canali internet e mobile
- Gestisce, tramite la concessionaria di pubblicità Niumidia Advertising le iniziative web e mobile marketing
- Progetta, sviluppa ed eroga i servizi di VIRGILIO.IT per milioni di utenti tra i quali posta elettronica, social networking e servizi informativi di portale

L'ESIGENZA DI SICUREZZA DEI SERVIZI WEB 2.0. In Matrix, come all'interno dei cicli produttivi di ciascuna IT company, i requisiti normativi, la qualità del business erogato, l'affidabilità e la robustezza nei confronti dei competitors sono importanti punti chiave per il successo di un prodotto o di un servizio. Per le applicazioni web, la cura di questi aspetti produttivi non può prescindere dalla cura degli aspetti di sicurezza, tema importante e reso complesso da affrontare con l'avvento dei nuovi *Business Model* propri del Web 2.0. A fronte di questi cambiamenti sono mutate le minacce di sicurezza alle quali sono esposti i servizi offerti dalle applicazioni web e i nostri clienti. Per far fronte a tali nuove minacce nasce l'esigenza di una definizione di un processo integrato di sicurezza e l'identificazione di metodologie e tecnologie a supporto della sicurezza di un prodotto o servizio web.

LA SENSIBILITA' AI TEMI DI SICUREZZA. Le aziende il cui business è legato in maniera non sempre evidente alla sicurezza, hanno la necessità di essere sensibilizzate alle tematiche di sicurezza per poter comprendere al meglio quali sono gli aspetti che rappresentano dei vincoli, quali degli utili aspetti e quali delle opportunità.

GLI ABUSI SUL WEB. Virgilio, come tutti i provider di social network, è soggetto ad abusi di vario genere, dal Cyberbullismo alla pubblicazione di materiale illecito (e.g. pedopornografia, copyright, etc). Tali abusi vanno ad aggiungersi a quelli che già colpiscono normalmente gli utenti della rete, come violazione di password, furto d'identità o negazione di servizio.

SOLUZIONE

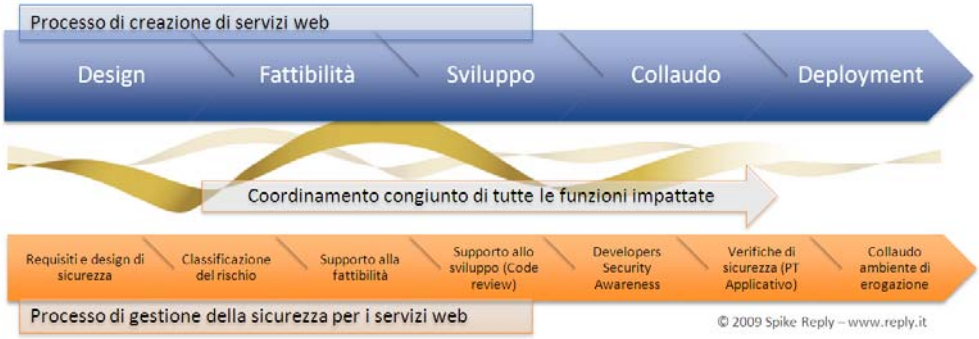
La gestione della sicurezza dei servizi web in Matrix S.p.A. richiede le competenze di tutte le funzioni aziendali: le persone responsabili della gestione della sicurezza forniscono la competenza specifica, i responsabili dello sviluppo forniscono la conoscenza dei processi, le funzioni marketing forniscono la conoscenza degli impatti sui clienti e sul business. Tutti cooperano con le competenze specifiche per la comune finalità di coordinare la creazione di prodotti che possano essere considerati sicuri.

DEFINIZIONE DI UN MODELLO DI GESTIONE DELLA SICUREZZA PER IL WEB 2.0. Il risultato delle numerose attività condotte presso il cliente è stato quello di innovare la gestione della sicurezza creando in stretta collaborazione con il Cliente un nuovo modello di governo della sicurezza che tiene in considerazione tutte le reali e peculiari esigenze di sicurezza proprie delle Aziende che operano nel mondo del Web 2.0.

IL PROGRAMMA DI SECURITY AWARENESS. La formazione e la sensibilizzazione delle funzioni di Business riveste una importanza strategica, fornendo gli strumenti culturali per comprendere le opportunità di Business che possono derivare dall'affrontare in modo strutturato la sicurezza dei prodotti Web 2.0. Le modalità di erogazione del programma di sensibilizzazione consistono in: corsi mirati con argomenti specifici legati al business di Matrix, produzione e diffusione di materiale informativo e l'erogazione di una rassegna stampa degli eventi di sicurezza di

maggiore spicco trovati nei siti web più autorevoli, corredata da una contestualizzazione commentata per l'azienda a cura della funzione Security.

IL PROCESSO INTEGRATO PER LA SICUREZZA DEI PRODOTTI WEB. L'Azienda deve poter garantire i livelli di sicurezza dei servizi Web 2.0 offerti, come richiesto dai vincoli normativi, dalle politiche di sicurezza Aziendali e dagli utenti stessi dei servizi.



La funzione sicurezza si configura dunque come centro di competenza e servizio nei confronti delle funzioni responsabili della creazione delle applicazioni web, governando un processo non intrusivo verso l'Azienda finalizzato alla misurazione del reale rischio residuo di un servizio erogato.

In parallelo alla fase di **design** del progetto, il processo di sicurezza affianca le attività di evidenziazione dei requisiti e vincoli e l'analisi delle funzionalità di sicurezza che il prodotto o servizio vuole offrire. L'integrazione tra la funzione sicurezza e le persone preposte al design del prodotto è strategica in quanto queste ultime potrebbero non essere dotate delle competenze necessarie per tenere in considerazione tutti i requisiti di legge o i problemi noti relativi alla sicurezza del prodotto o servizio che viene sviluppato.

La fase iniziale di definizione dei requisiti è inoltre un'opportunità per sviluppare prodotti e servizi che abbiano un elemento in più rispetto ai tutti i competitors che non considerano gli aspetti di sicurezza come reali opportunità di Business. La collaborazione con la funzione di security in fase iniziale consente di effettuare una pianificazione attenta e accurata del lavoro da svolgere e crea i presupposti per la creazione di un prodotto o di un servizio robusto e duraturo.

La "classificazione del rischio" dei prodotti è effettuata congiuntamente alla **fattibilità** del servizio, e permette di commisurare le risorse da dedicare al prodotto o servizio specifico in relazione alla criticità dello stesso. Tramite l'utilizzo di metodologie orientate all'analisi delle minacce e vulnerabilità proprie del web, la funzione sicurezza calcola, documenta e comunica ai responsabili di business la reale esposizione aziendale al rischio.

La funzione Sicurezza adotta specifiche metodologie, best practices e strumenti dedicati alla sicurezza nello **sviluppo** in quanto rappresentano l'unico modo per ovviare alle vulnerabilità applicative che consentono a un attaccante di commettere illeciti mettendo a repentaglio il business. Per questa fase la funzione sicurezza si configura come centro di servizio a disposizione dei Team di Sviluppo. Particolare attenzione viene riservata anche alla fase di **test** che è particolarmente "mirata" e non coinvolge solo le caratteristiche funzionali dell'applicazione. In questa fase viene infatti verificata l'effettiva aderenza delle applicazioni web alle linee guida della programmazione sicura. Le attività di Penetration Testing applicativo sono uno strumento fondamentale per questo tipo di attività che vanno a completare l'attività di analisi del codice affrontata in fase di sviluppo.

VALORE REPLY

Spike Reply è stata in grado di percepire le reali esigenze del cliente, analizzare il contesto culturale e organizzativo e di impostare una strategia per la creazione di una funzione Sicurezza riconosciuta come competente ed efficace.
La proposta metodologica di Reply è stata riconosciuta come innovativa, grazie alle leve di Business utilizzate per creare la cultura della sicurezza in Azienda.