Security by design

Come minimizzare la superficie di rischio delle applicazioni business-critical

Massimiliano D'Amore

Manager Technology Infrastructure, Enterprise SPA

La portata degli attacchi informatici: alcuni esempi eclatanti

EQUIFAX

143 milioni di dati dei clienti sottratti sfruttando una falla nel software

I dati personali di quasi tutti gli americani sopra i 18 anni sono esposti

Crollo degl introiti del

27%

in un solo trimestre

YAHOO!

3 miliardi i profili cliente colpiti

I dati personali di tutti gli utenti Yahoo sono stati esposti

Calo di valore Yahoo: $350M

UBER

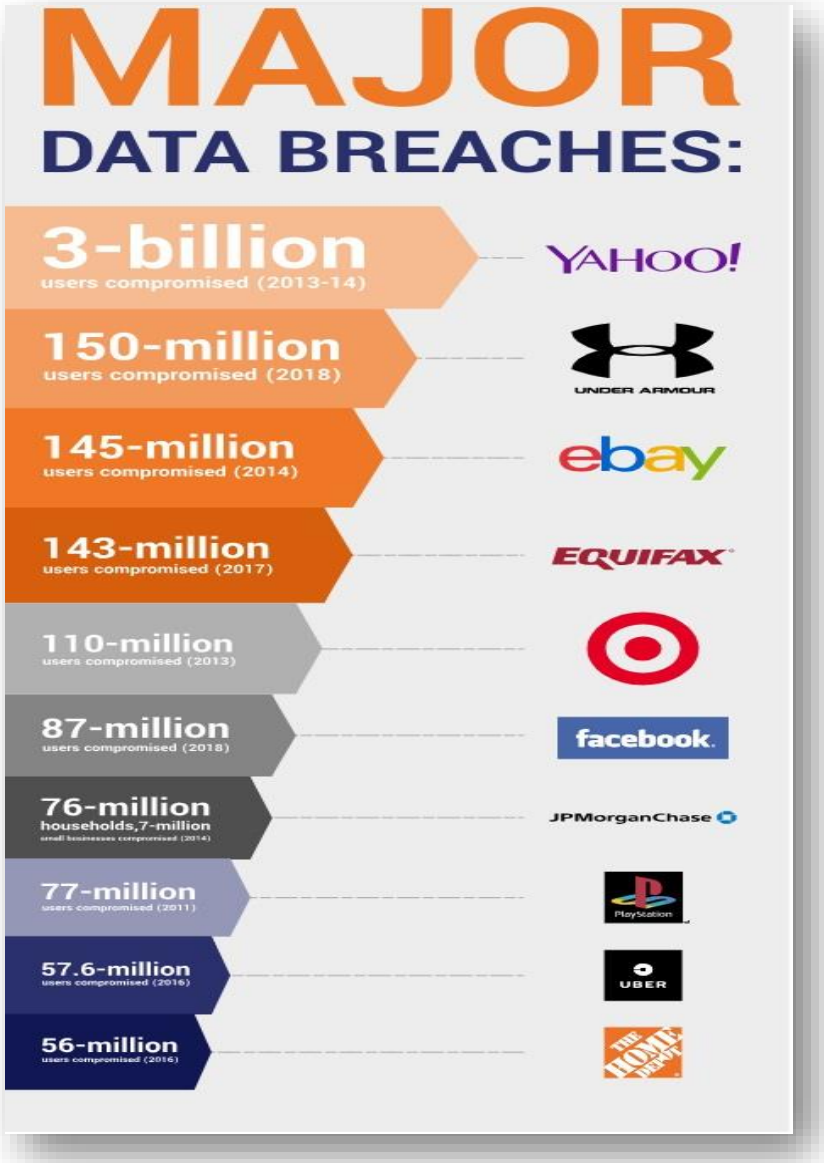
57 million clienti e autisti impattati dalla violazione

I dati degli utenti Uber sono stati esposti per un anno

-$20B capitalizzazione

E danno indiretto per le cause legali

Il Cybercrime colpisce ogni settore industriale e punta più alla sottrazione dei dati che alla monetizzazione diretta



Ogni organizzazione che subisce un attacco informatico rilevante subisce danni diretti ed indiretti:

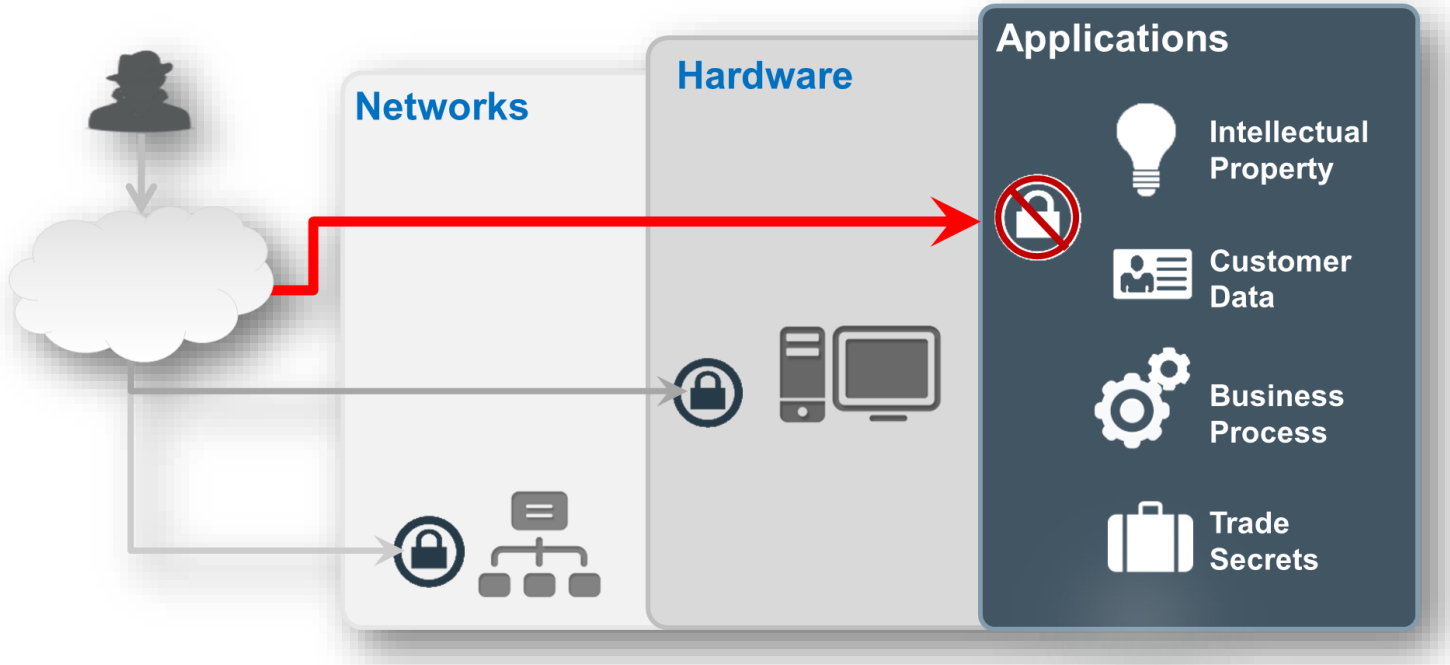
- Perdita di *business* per indisponibilità dei servizi
- Costi di ripristino e di ulteriore sicurizzazione *post-mortem*
- Ricadute di reputazione, immagine, valore in borsa, competitività
- Violazione di normative: sanzioni e cause da parte degli utenti impattati (es. Facebook – Cambridge Analytica)

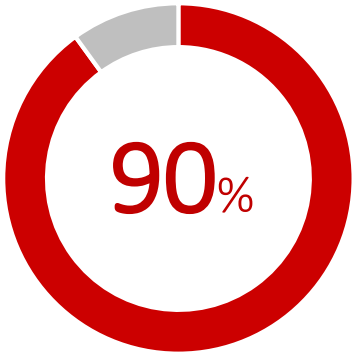
IL SALONE DEI PAGAMENTI
PAYVOLUTION

La App-economy ha spostato la superficie di rischio Cyber sulle applicazioni

All'inizio dell'era Internet (fino ai primi anni 2000) il perimetro della rete aziendale era il punto d'ingresso degli attacchi informatici.

Il Mobile, la multicanalità e l'avvento della App-economy hanno spostato l'attenzione del Cybercrime sulle applicazioni che hanno accesso diretto ai dati aziendali e personali.





è la percentuale di attacchi informatici che sfrutta vulnerabilità applicative

Homeland Security

Source: [1]U.S. Department of Homeland Security's U.S. Computer Emergency Response Team (US-CERT) 2017

IL SALONE DEI PAGAMENTI PAYVOLUTION

OWASP Top 10, lo standard di riferimento per la sicurezza delle applicazioni web e la *Security by Design* nelle normative

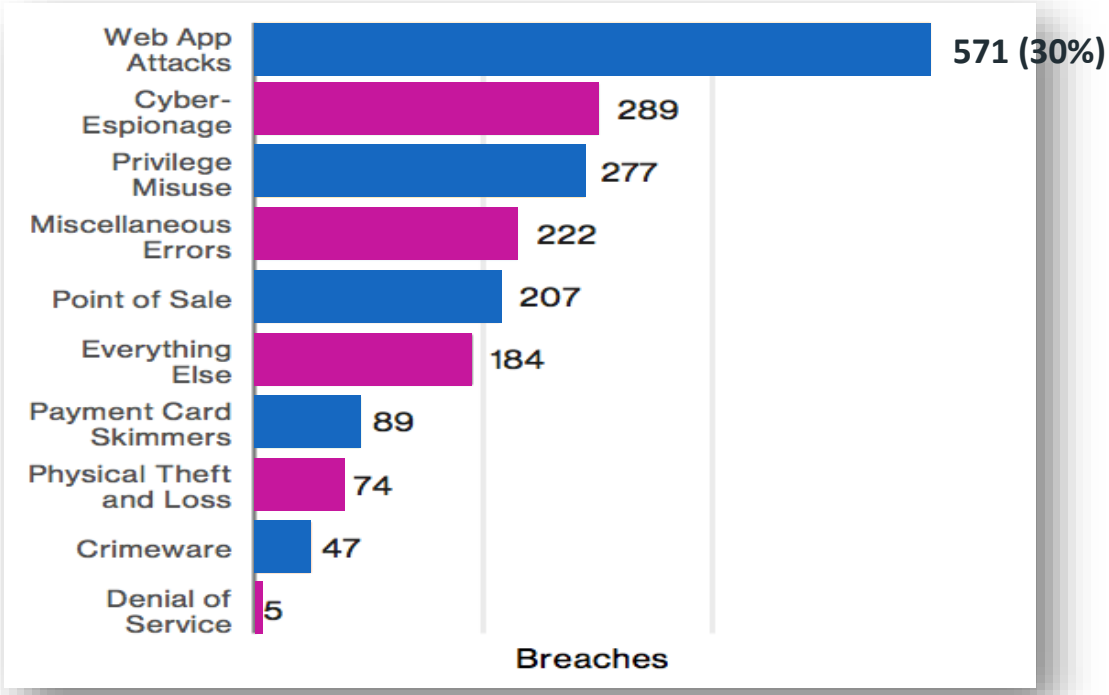
Nel 2001 nasce il progetto OWASP - Open Web Application Security Project. È una no-profit che sviluppa standard e strumenti per analizzare le vulnerabilità delle applicazioni web e in generale diffondere la cultura della sicurezza applicative nelle aziende. Ogni anno OWASP pubblica una relazione sull'andamento degli attacchi applicativi e una lista dei 10 tipi di vulnerabilità più diffuse, l'OWASP top 10.
OWASP Top 10 rappresenta uno standard *de facto* per misurare il livello di sicurezza intrinseca di un'applicazione web a seguito di un'analisi strumentale (Penetration test).

Lo standard PCI-DSS prevede nell'ambito dei Requisiti 6 e 11 dei controlli periodici delle applicazioni tramite strumenti di analisi statica e dinamica del software, per rilevare ed eliminare tutte le vulnerabilità gravi.

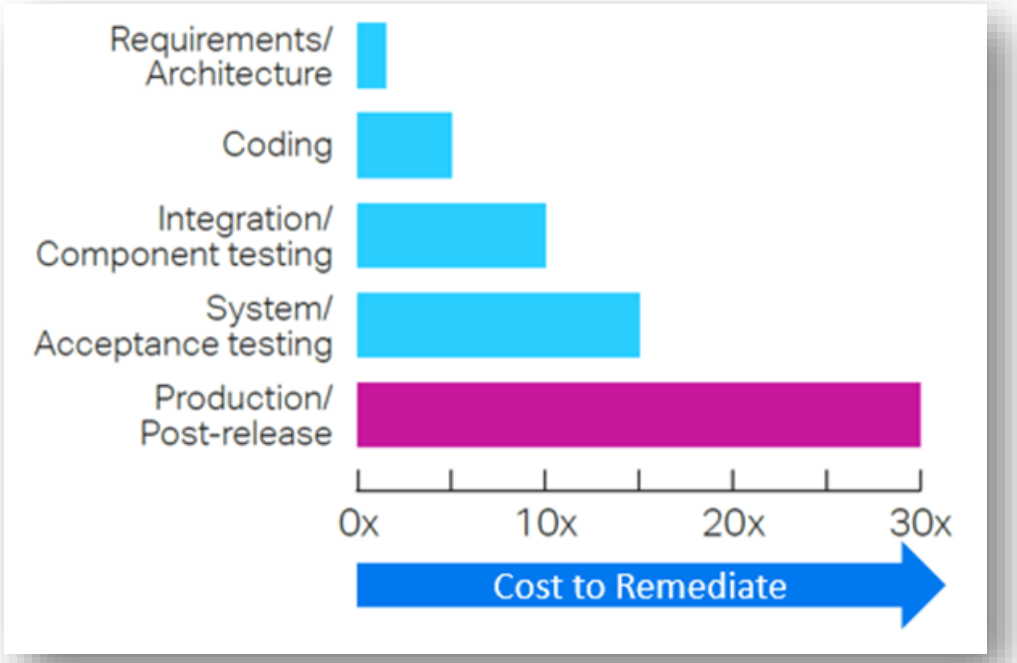
Il recente regolamento europeo sulla protezione dei dati personali (GDPR) prevede esplicitamente l'adozione del concetto di *Privacy by design* già a partire dalla fase di progettazione delle applicazioni.

Un approccio radicale: mettere in sicurezza il codice sorgente

Le web applications tradizionali e mobile sono ancora il bersaglio preferito del Cybercrime, sia sviluppate in casa che da terze parti. Più delle truffe sui POS e della clonazione delle carte di pagamento.



Source: Verizon DBIR 2017



Adottare una tecnologia di analisi delle vulnerabilità in fase di sviluppo del Sw invece che in collaudo o produzione comporta una significativa riduzione del danno potenziale a seguito di un incidente informatico (fino a 30x)

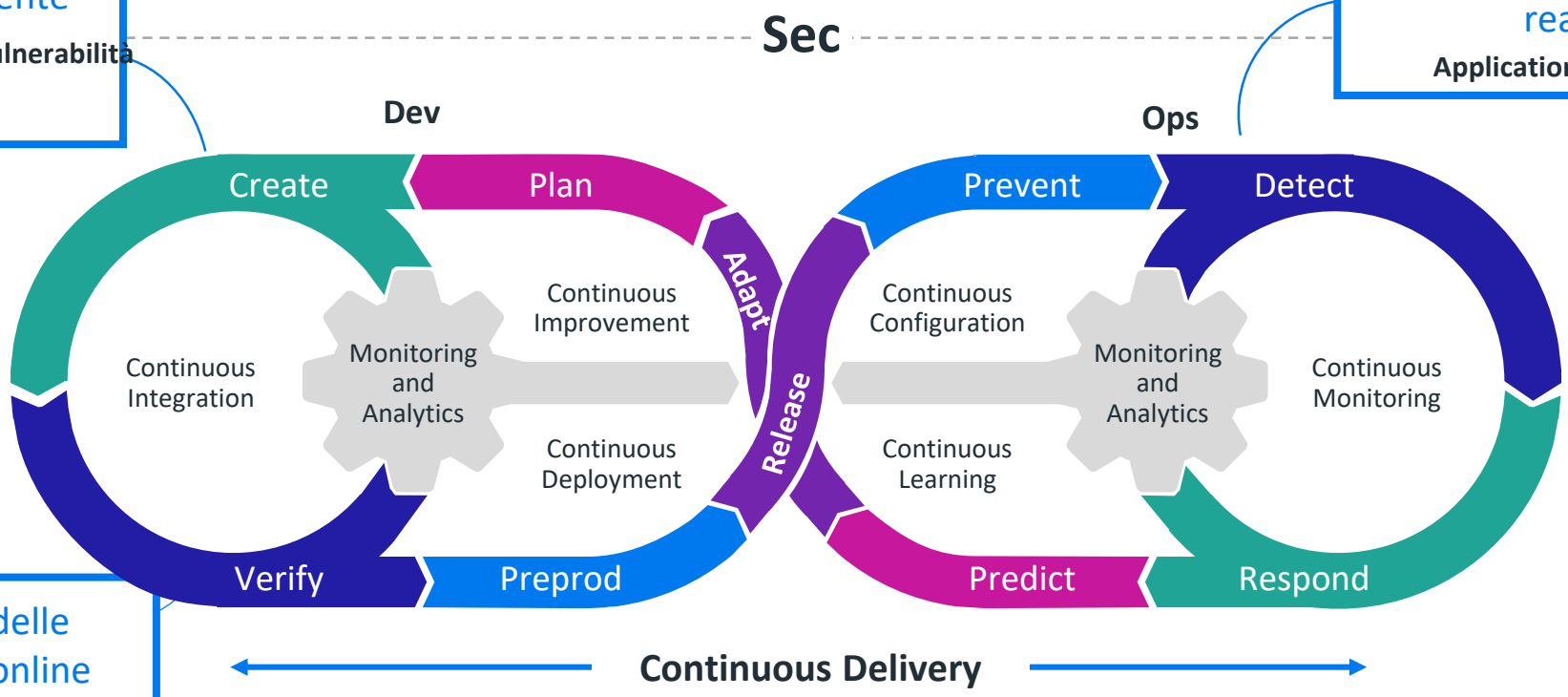
L’inserimento dei test di sicurezza nella metodologia DevOps

Analisi del codice sorgente

Rilevazione e mitigazione delle vulnerabilità in fase di sviluppo)

Protezione delle applicazioni in tempo reale

Application Defender



Audit periodico delle applicazioni web online

Simulazione automatizzata di un potenziale attacco hacker

Il *Security by Design* implementato nel processo DevOps di Enterprise: garanzia di eccellenza nella minimizzazione del rischio cyber per le applicazioni aziendali

Source: “10 Things to Get Right for Successful DevSecOps,” Gartner, Inc., 2017

Enterprise SpA e la certificazione OWASP Top 10 delle applicazioni Core

Enterprise SpA ha investito proattivamente in tecnologie e processi di sicurezza applicativa per certificare le soluzioni per il banking Piattaforma Pr.E.M.I.A. HUB UniPay Portal4Bank App4Bank 4CoreBanking etc

- Adozione della tecnologia leader di mercato Micro Focus Fortify
- Metodologia di Security by Design e by Default
- Rilevazione ed eliminazione delle vulnerabilità applicative classificate in OWASP Top 10 2017
- Le applicazioni web vengono sottoposte ad audit di sicurezza periodico (analisi dinamica o penetration test) per mantenere il più elevato livello di sicurezza possibile rispetto all'evoluzione delle minacce Cyber
- I clienti Enterprise vengono aggiornati periodicamente tramite assesment report sulle vulnerabilità eventualmente in atto
- Tutti i clienti hanno una garanzia rispetto alla sicurezza intrinseca dei prodotti

Un valore aggiunto di grande qualità considerando alcuni dati significativi:

- L'80% delle applicazioni bancarie web risulta vulnerabile ad una diffusa tipologia di attacco (XSS)
- Solo il 30% delle applicazioni ha superato lo scan OWASP Top 10 2017: circa il 40% di quelle sviluppate in azienda e solo il 25% di quelle fornite da terze parti

Fortify Application Security Research Update 2017 Report

IL FUTURO PASSA DA QUI

#SalonePagamenti2018 #payvolution