Studio Fiorenzi
Security & Forensics

GDPR: Gestire i Cyber Risk e Il Data Breach dei sistemi informatici

Proteggere i dati per proteggere il business

Presentazioni

- Dottore in Scienze dell'Informazione (informatica) mi occupo di Sicurezza Informatica e Digital Forensics dal 1997
- Iscritto Albo CTU Tribunale di Firenze n. 7519 dal 2003 ,Albo Periti Tribunale di Firenze n. 422 dal 2011
- Iscritto a ruolo Albo Periti ed Esperti CCIAA Firenze n. 1130 dal 2004
- Organizzatore e relatore di convegni sul tema della sicurezza informatica e della computer forensics
- Co Autore per gli aspetti di computer forensics al libro "Internet e il danno alla persona" edito da Giappichelli nel 2012
- Certificato ECCE European Certificate on the fight against Cybercrime and Electronic Evidence (ECCE) 2009
- Lead Auditor ISO27001
- Board of Directors ONIF – Osservatorio Nazionale Informatica Forense www.onif.it
- CTS CLUSIT – Comitato Tecnico Scientifico CLUSIT www.clusit.it
- Membro IISFA - International Information System Forensics Association

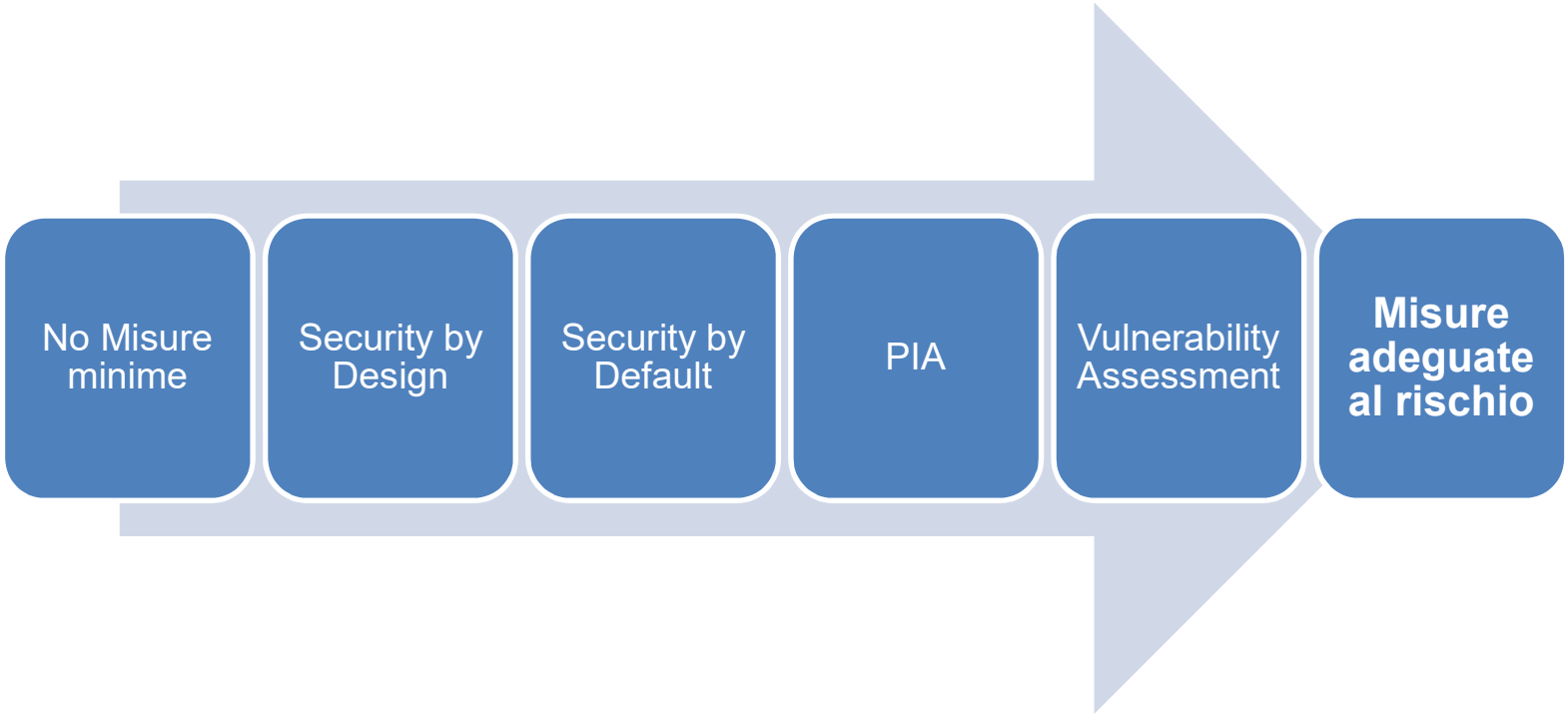
Dlgs 196/2003

E’ percepita da tutti come				
Un ostacolo al business	Riguarda la privacy	Obbligo da rispettare	Checklist di adempimenti	Oneshot : una volta per sempre

Dlgs196/2003: Misure minime…

- Sistema di Autenticazione informatica
- Sistema di Autorizzazione informatica (verifica annuale)
- Antivirus con aggiornamento almeno semestrale
- Patching dei sistemi annuale
- Backup settimanali
- Aggiornamento annuale lista incaricati
- Regolamento aziendale uso email e accesso Internet (2007->

GDPR: Cyber Security Approach



Quale è il rischio per i vostri dati: Questo?

Ce ne sono molti altri…

- Furto di dati
  - Furto di Identità
  - Ricatto dati sensibili
  - Uso di dati riservati e non conosciuti alla controparte per vantaggio, ostacolo o azioni denigratorie
- Dipendente/socio infedele
- Blocco della rete
- Alterazione e/o cancellazione dati
- Data breach
- Web reputation

Ce ne sono molti altri…

- Acceso e/o controllo remoto computer e server
  - Impersonare la vittima e agire per suo conto
  - Spiare l'attività della vittima
  - Accesso completo alle piattaforme «giuridiche» ad esempio PCT
  - Accesso completo agli strumenti di firma digitale (firma e accesso alla PA)
  - Diventare testa di ponte per attacchi e azioni criminose
  - Usare i dati conservati nei sistemi per fare privilege escalation ed accedere ad
    - Altri dispositivi
    - Conti correnti
    - Caselle di posta
    - Servizi cloud
    - Social
    - Blog
    - Sito studio
    - Sistemi informatici dei clienti

Lo Studio Legale e i dati

Lo studio Legale per sua natura, gestisce una grande quantità di dati: personali, sensibili, giudiziari.

Il GDPR impone agli studi l'implementazione di tecniche di *risk-management*.

Sistema di Gestione della Sicurezza e Protezione dei Dati correlata all'analisi dei rischi

Cosa fare per proteggersi

Le misure di sicurezza devono essere adeguate al rischio
riguardano tutti gli elementi in cui l'informazione viene
processata

Strumenti di Cyber Security GDPR View

Policy regolamenti

- Relativamente agli strumenti informatici e alle credenziali di accesso che sono forniti a dipendenti e collaboratori definire :
  - Finalità
  - Regole
  - Modalità di controllo
  - Sistema sanzionatorio chiare regole uso degli strumenti aziendali e delle credenziali

Formazione continua

- Awaress rispetto ai rischi informatici
- Educare ai coretti comportamenti
  - Clear Desk
  - Password non banali
  - Strumenti di protezione password keepass

Strumenti di Cyber Security GDPR View

Antivirus

- aggiornamenti ogni volta che sono disponibili
- Web Risk reputation
- APT Advanced Persistent Threat

Patching

- Computer: Sistema operativo 1 volta al mese
- Smartphone, tablet etc.. S.O e App appena disponibili
- Sofware legacy ed embedded: problema aperto
- Software applicativo: CRM, ERP, etc… fornitori spesso assenti

Strumenti di Cyber Security GDPR View

Sicurezza della rete

- Sistemi Firewall
- Sistemi IPS/IDS
- VPN per le connessioni remote
- Segmentazione della rete
- Monitoraggio rete
- Network Analysis
- Connessioni Cifrate SSL

Protezione Patrimonio Aziendale

- DLP Data loss prevention
- Sistemi di URL e Content Filtering

Strumenti di Cyber Security GDPR View

Security Management

- Asset invenntory
- **Security Assessment**
- Vulnerablity Management
- CDN (Content, Web Application Firewall)
- Anti DDOS
- Sistemi antifrode (siti ecommerce ERP/CRM)

Business Continuity & Disaster Recovery

- Backup
- Ambienti Virtuali: VM Snapshot
- Replica su sito secondario
- Processi, procedure e Test di BC e DR

Data breach e Incidente informatico

Data breach:un incidente di sicurezza in cui dati sensibili, protetti o riservati vengono acceduti, consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato.

Incidente informatico: qualsiasi evento che non fa parte dell'operativita' standard di un servizio e che causa, o puo' causare, un'interruzione e una riduzione della qualita' di tale servizio

GDPR & Notifica Breach:

72 Ore

- Chi ci ha bucato
- Come ci ha bucato
- Quando ci ha bucato
- Da dove è entrato

Poche ore

- Sanitizzare i sistemi
- Ripristinare i dati
- Mettere in sicurezzza dati e applicazioni

Pochissimo tempo

- Individuare le fonti di prova
- Raccogliere le evidenze in modalità forense
- Analizzare live il breach
- Analizzare offline le evidenze raccolte
- Individuare una soluzione di sicurezza

E la gestione del brech?

- Analisi Forense sistemi compromessi
  - Indagine informatica post incidente sui sistemi compromessi per comprendere come, quando e chi ha avuto accesso ai dati o compromesso i sistemi
- Forensics readiness
  - Preparare a priori lo studio o l'azienda alla gestione di un incidente raccogliendo tutte i dati necessari a rendere più rapida, efficace e meno costosa l'analisi di un breach nel momento in cui si verifica

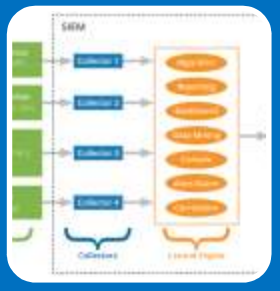
Forensics Readiness e ADS

- Il provvedimento sugli Amministratori di sistema definiva il concetto di raccolta log
- Predisporre un sistema per la raccolta di computer e dispositivi in tempo reale. (SIEM)
- In caso di breach dei sistemi il soggetto tende a trattenersi al suo interno per non meno di 6 mesi, cancellando le sue tracce
- La remotizzazione dei log permette di scoprire, anche distanza di tempo chi, come, quando si è introdotto nei nostri sistemi.

SIEM: Correlazione, analisi, allarmi

Utilizzare i log e l'informazione in essa contenuta per comprende se

- Siamo nel mirino di qualcuno
- C'è un'attività anomala
- C'è una compromissione
- Abbiamo dipendenti e collaboratori infedeli



Tuning SIEM correlation roules & allarm

- Sviluppare
- Testare
- Eliminare falsi positivi
- Mantenere aggiornate

SIEM: Correlazione, analisi, allarmi

IoA
Indicator of Attack

- Track connessioni «legittime» incoming da Bad IP sui log source
- Drop/Reject connessioni incoming da bad IP su FW
- Network scan
- Off Hours internal activity

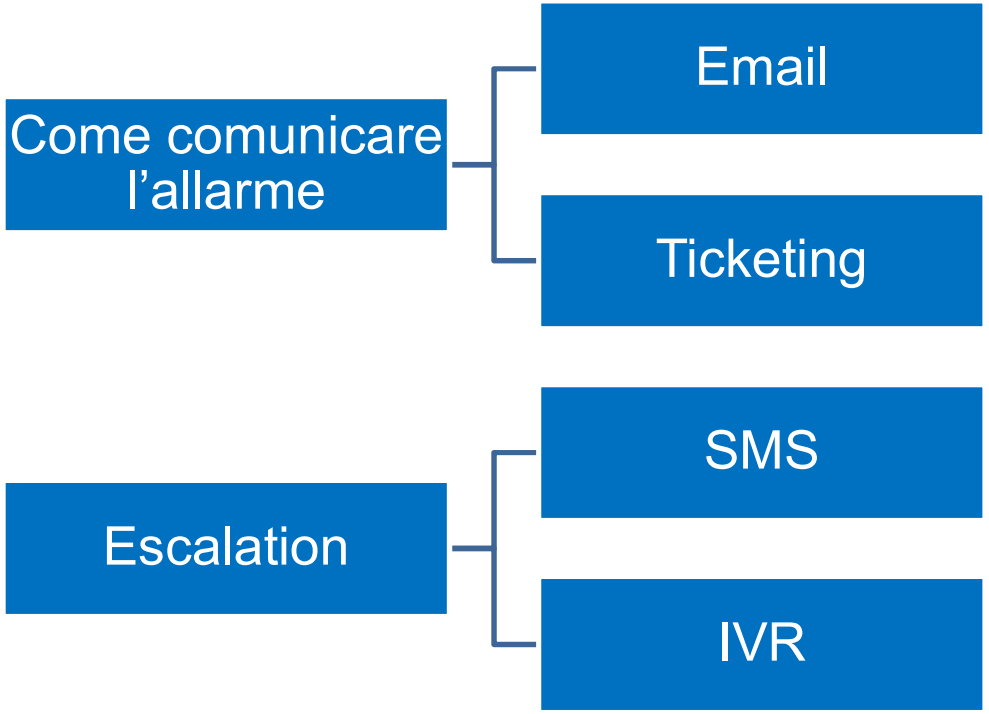
IoC
Indicator of Compromission

- Connessioni outgoing «legittimo» verso Bad IP
- Drop/reject connessioni verso Bad IP
- Multiple failed login from single host
- Multiple login with single username from differente region
- Traffico DNS in uscita
- Errori nei log
- Errori log applicativi

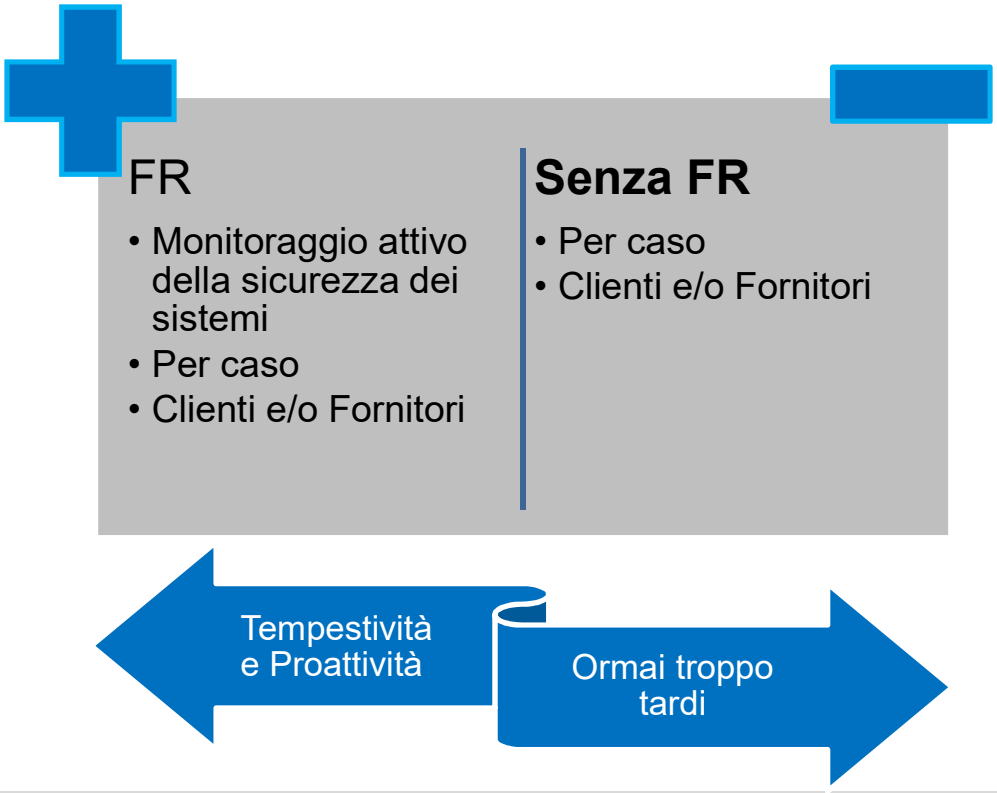
Antifrode

- Profiling utente
- Uso di account e carte «segnalate»
- Bad IP
- Behaviour analysis traffico IP/utenza

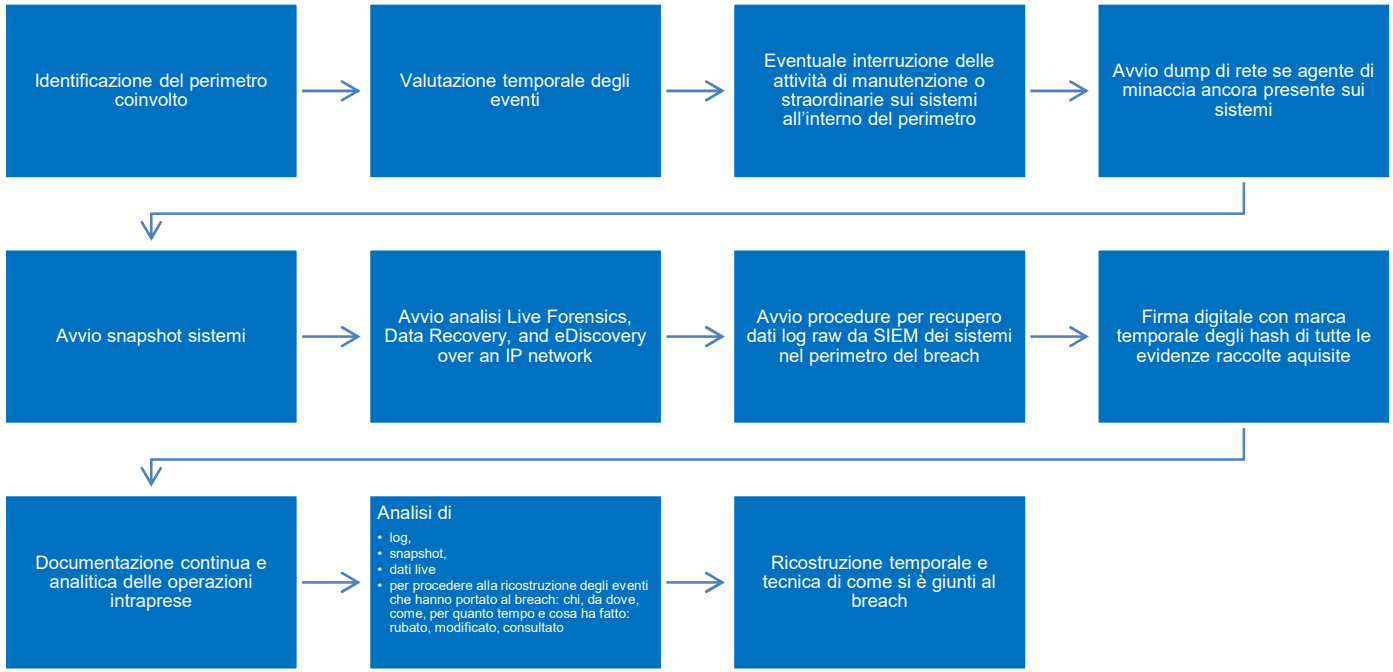
SIEM: Correlazione, analisi, allarmi



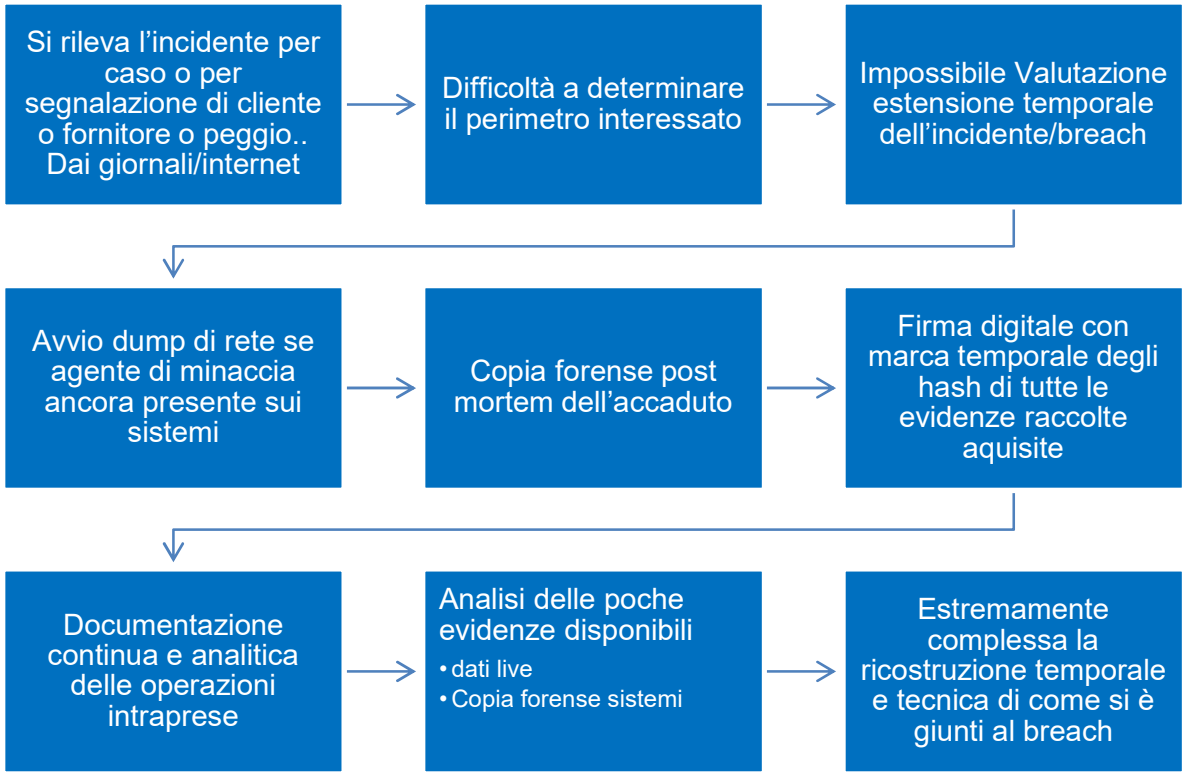
Come scopriamo incident o breach



FR :Team Forense all'opera



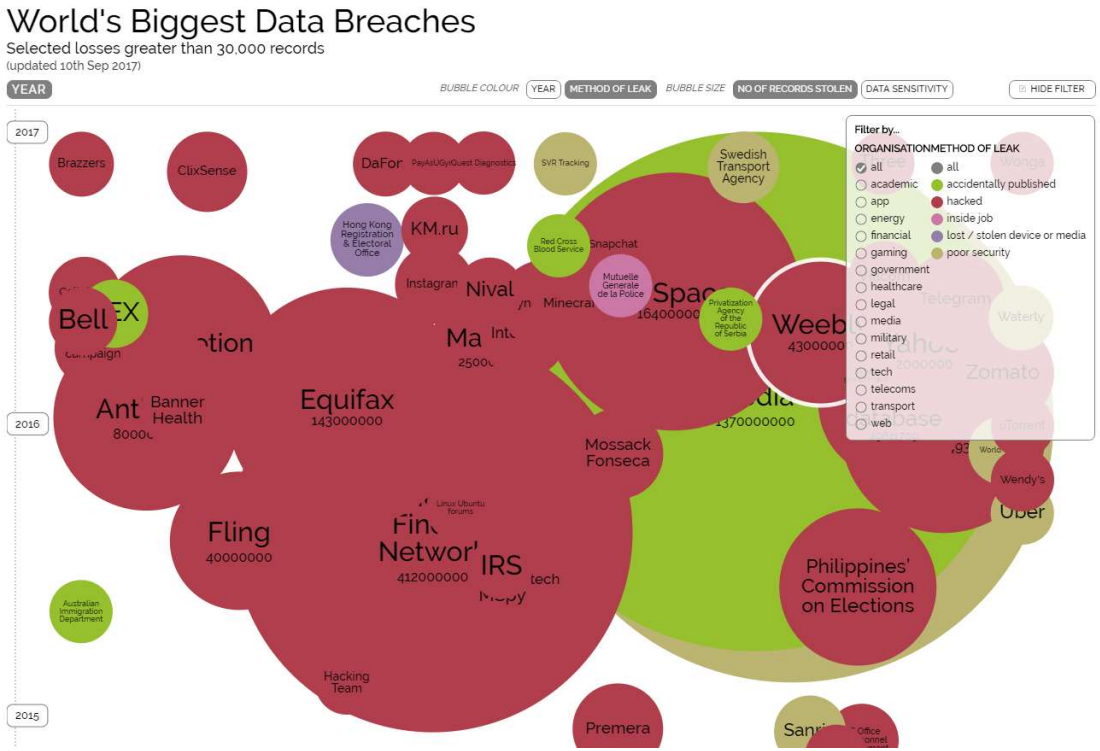
In assenza di Forensics Readintess



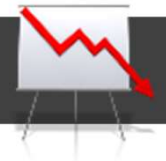
Forensics Readiness: perchè

- Forensics Readiness è incident prevention non Incident response
- Oggi è necessario assumere che un incident accadrà anche se il risk assessment dice ha probabilità bassa, e Forensics Readiness ci permette di gestirlo anticipatamente
- Perché Forensics Readiness raccoglie sistematicamente le informazioni nel tempo, e permette di rilevare situazioni in cui chi vi minaccia, interno o esterno cercherà di
  - Cancellare le prove della sua attività
  - Rimanere silente per sfruttare i sistemi
  - Permanere per mesi prima di «bruciare» le sue vittime

Data breach: un fenomeno in crescita



Forensiscs Readiness ROI



La mancata adozione di forensic readiness può determinare:

- Perdita di business - danni reputazionali
- Perdita di incassi - perdita di clienti
- Azioni legali - incapacità di soddisfare SLA, azioni inappropriate, ecc ...
- Furto di dati, modifica o distruzione
- Incapacità di ripristinare efficacemente l'accesso / controllo amministrativo
- Fermo dei sistemi di erogazione del business

Forensics Readiness ROI

Forensic readiness garantisce le aziende di :

- Determinare rapidamente il vettore di attacco
- Comprendere e isolare le informazioni pertinenti, minimizzando le risorse necessarie
- Interrompere tempestivamente gli accessi abusivi
- Contenere i danni e ridurre il tempo di inattività
- Rileva le tendenze nel tempo
- Ottenere sconti sui premi assicurativi

Infine…

«Il futuro dipende da quello che facciamo nel presente»

Mahatma Gandhi

Studio Fiorenzi
Security & Forensics

Dott. Alessandro Fiorenzi
Email af@studiofiorenzi.it
Mobile: +393487920172
https://www.studiofiorenzi.it