FORENSICS READINESS E INCIDENT RESPONSE

MATTIA EPIFANI E FRANCESCO PICASSO

SECURITY SUMMIT

MILANO, 19 MARZO 2015

INTRODUZIONE

Di cosa **parleremo**

- Introduzione informale alla gestione degli **incidenti informatici**
- Introduzione formale alla ***Forensics Readiness***

Di cosa **non** parleremo

- normative, obblighi di notifica dei *data breach*, responsabilità civili e penali, etc.

Obiettivo: un approccio *soft* alla «materia»

http://31hm9m1i8pbpjlzhw3p1uric.wpengine.netdna-cdn.com/wp-content/uploads/2013/08/order-chaos-keys.jpg

INCIDENTE

- «*Avvenimento inatteso che interrompe il corso regolare di un'azione*»
- quanto inatteso?

- «.. *per lo più, avvenimento non lieto* ..»
- quanto non lieto?

http://funnyimagecollect.blogspot.it/2012/01/funny-animal-car-accident-pictures-car.html

http://http://www.treccani.it/vocabolario/incidente2/

INCIDENTE INFORMATICO

- Tutto ciò che impatta il *digitale*
- Tipicamente inteso come Incidente Informatico di Sicurezza
  - incide su CID

- Virtuale… ma **reale**!
- Non solo virtuale..

http://www.maxlolz.com/funny-accident/

INCIDENTI INFORMATICI

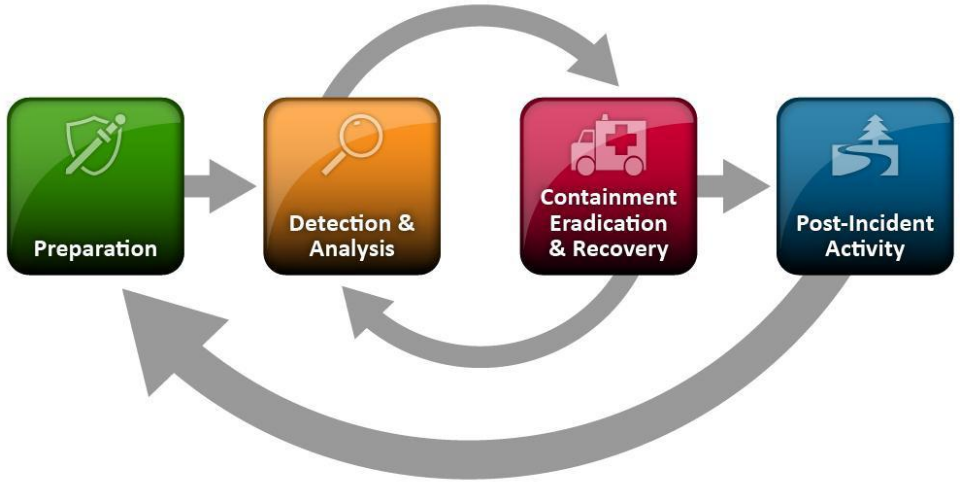
- Business continuity
- Disaster Recovery
- Tipicamente non orientati a rispondere ad indicidenti informatici di sicurezza
  - ad ogni modo utilissimi anche in questi casi

https://www.pinterest.com/pin/161145111394723 41/

- Interruzione (DOS, Worm, …)
- Interferenza (port scans, mapping, probes, …)
- Accesso non autorizzato
  - furto d'identità, rilascio, furto o modifica di dati ed informazioni
- Uso non autorizzato
  - minacce, molestie, abuso degli strumenti
- Furto
  - hardware, software, documenti, password
- (malware)?
- … chi più ne ha più ne metta …

INCIDENT HANDLING

- piano d'azione per gestire gli incidenti informatici
- ossia **eventi** che causano o possono causare danni
- contempla politiche, procedure, competenze
- ciak .. **azione**!



NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide, August 2012.

IDENTIFICATION

- caratterizzare l'evento
  - primo: rilevare
  - secondo: identificare

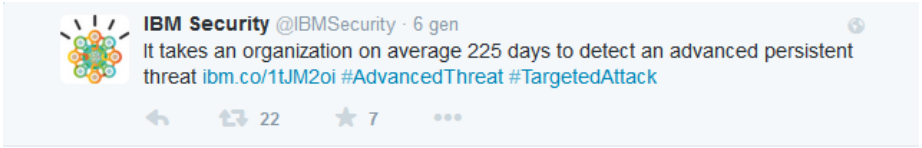
- "*se non trovi l'incidente lui (o quello che ne consegue) troverà te (prima o poi)*"

http://funnyimagecollect.blogspot.it/2012/01/funny-animal-car-accident-pictures-car.html

- L' opportunita' dei falsi positivi

IDENTIFICATION

- fattore **tempo**
- Tipicamente maggiore il tempo di identificazione maggiore il danno
- Potrebbe essere impossibile o inefficace un'azione legale
- Azione **post**-incidente, non **postuma**



REALITY NET
SYSTEM SOLUTIONS

LA BATTAGLIA

- **Contenere** l'attacco
  - Limitare i (possibili) danni
  - Cristallizzare

- **Analizzare** l'incidente
  - 5W (who, what, when, where, why)
  - Per tacer dell'*how* … quali vulnerabilita'
  - Ripulire

- **Ripristinare**
  - *back in production*

FAST RECOVERY

Too Fast Recovery		
Cristallizzazione	No	
Analisi	No	
Vulnerabilità	Ignote	
Rimozione artefatti	Ignota	
Intelligence	No	
Preparazione	No	

Fast Recovery		
Cristallizzazione	Sì	
Analisi	No	*
Vulnerabilità	Ignote	*
Rimozione artefatti	Ignota	
Intelligence	No	*
Preparazione	No	*

Nota: cristallizzare anche le informazioni **correlate**.

OPPORTUNITÀ

- Stimare il danno
- Valutare eventuali azioni disciplinari/legali
- Evitare attriti, essere costruttivi

- Opportunità di **prepararsi**
- Opportunitá di allocare risorse (**budget**)

http://advisoranalyst.com/glablog/wp-content/uploads/2013/12/2012-02-13-BlogPostLessonsLearned2-OppPhoto.jpg

PREPARAZIONE

- **Preventiva**
  - Tesa ad evitare l'incidente o ad identificarlo
- **Proattiva**
  - Tesa a riconsiderare rischi, strumenti e competenze prima che un incidente avvenga
- **Reattiva**
  - Tesa a minimizzare il possibile danno

CASI(STICA) REALI(TY)

- Thin-client scenario

http://www.coolfunpics.com/slides/Tank_Accident.html

POST THIN-CLIENT SCENARIO

- Riconsiderare alcuni macro scenari
  - es: insider
- Analisi dei rischi (o di almeno di parte di essi)
- Migliorare fase di identificazione
  - Tempi!
- Open source threat intelligence
  - Più semplicemente… mantenersi informati
- Formare gli utenti

CONSIDERAZIONI FINALI (PRIMA PARTE)

- Incidenti informatici non sono inusuali
- Possono essere molto complessi e causare danni rilevanti

- La sicurezza è un processo…
- Che dovrebbe contemplare anche il processo di gestione degli incidenti
  - L'elogio dell'ignoranza del dotto
  - Valorizza gli investimenti in sicurezza preventiva
  - Valorizza la conoscenza e le competenze

- Essere pronti… è un requisito necessario.

DIGITAL FORENSICS READINESS

- "**Forensic Readiness** is the achievement of an appropriate level of capability by an organisation in order for it to be able to collect, preserve, protect and analyze Digital Evidence so that this evidence can be effectively used in any legal matters, in disciplinary matters, in an employment tribunal or in a court of law"

  CESG, Good Practice Guide 18, 2009

- "**Forensic Readiness** is having an appropriate level of capability in order to be able to preserve, collect, protect and analyze digital evidence so that this evidence can be used effectively: in any legal matters; in security investigations; in disciplinary proceeding; in an employment tribunal; or in a court of law"

  NICS, Forensics Readiness Guidelines, 2011

UN CASO EMBLEMATICO: APPLE VS. SAMSUNG

- Nel 2010 Apple ha accusato Samsung di **violazione di segreto industriale** di brevetti relativi ad iPhone
- A seguito dell'accusa Samsung non è stata in grado di garantire la **possibilità di accedere** ai messaggi di posta elettronica potenzialmente rilevanti per il caso
- Il giudice ha stabilito che **Samsung ha agito volontariamente nel cancellare i messaggi poiché questi sarebbero stati potenzialmente utili in tribunale a favore di Apple**
- La causa principale dietro la mancata conservazione delle evidenze informatiche è il fatto che **il sistema di gestione della posta elettronica interna procedeva automaticamente alla eliminazione definitiva di tutti i messaggi (compresi quelli cancellati dagli utenti) dopo un periodo di due settimane**.
- Al termine del procedimento Samsung è stata condannata a pagare $1.05 bn di dollari
- **La mancanza di un piano di conservazione proattiva e la perdita di evidenze digitali ha contribuito ad incrementare la multa**

DIGITAL FORENSICS READINESS

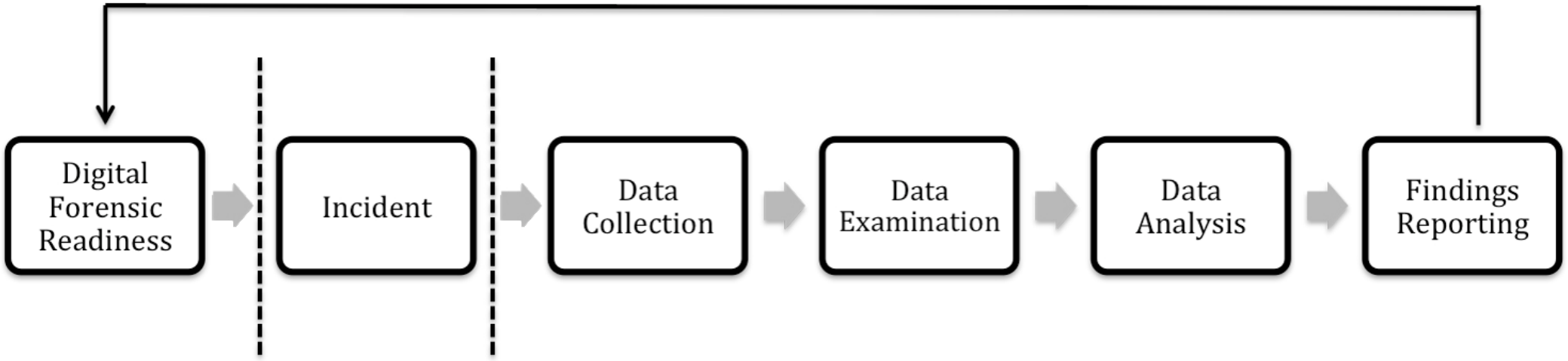
- Il caso illustrato è un buon esempio del perché la digital forensics non deve essere pensata **unicamente come uno strumento post-incidente** ma deve essere attentamente **pianificata in anticipo**
- Una corretta attività di pianificazione permette infatti di **incrementare la possibilità di avere una buona investigazione digitale** in termini di **risultati, tempi e costi**
- Il problema più comune in una investigazione digitale risiede nel fatto che l'investigatore può formulare ipotesi e cercare di ricostruire fatti utili alle indagini **unicamente attraverso una osservazione e valutazione a posteriori di un sistema e dei suoi artefatti**

DIGITAL FORENSICS READINESS

- La maggior parte delle aziende dovrebbe essere già preparata per una qualche forma di **gestione dell'incidente**, ma questa è spesso **orientata alla business continuity** ovvero a minimizzare l'impatto di un incidente sui processi quotidiani di business dell'azienda
- Spesso questo obiettivo prevede delle **azioni che vanno in contrato con la possibilità di arrivare ad una completa investigazione informatica**
- Per impedire tale conflitto un azienda dovrebbe essere capace di preparare un piano per una gestione effettiva di entrambi gli interessi: business continuity e incident response

DIGITAL FORENSICS READINESS

- La DFR corrisponde quindi con la fase di **pianificazione pre-incidente** all'interno del processo tipicamente utilizzato durante una investigazione digitale



DIGITAL FORENSICS READINESS
PASSI OPERATIVI

- Definire gli **scenari del business aziendale** che possono richiedere evidenze digitali
- Identificare **le possibili fonti e i diversi tipi** di evidenze digitali
- Determinare **i requisiti tecnici e legali per la raccolta** delle evidenze digitali
- Raggiungere una capacità per **la raccolta sicura di evidenze digitali** in modo tale da renderle legally-compliant
- Stabilire una **policy per la gestione e la conservazione sicura delle potenziali sorgenti di informazioni**
- Implementare e mantenere **un sistema di monitoraggio** per il rilevamento dei principali incidenti
- Specificare **in quali circostanze** si rende necessaria una **investigazione informatica completa**
- **Addestrare i dipendenti** per la gestione di base degli incidenti
- **Documentare i casi reali** descrivendo l'incidente e il suo impatto
- Garantire una **review legale** per agevolare le azioni di risposta all'incidente

DIGITAL FORENSICS READINESS CHECKLIST

- Policies and Procedures
- Legal
- Public Relations
- Asset inventory and Profiling
- Information gathering plan
- Data preservation
- Tools testing
- Training
- Logistics

DIGITAL FORENSICS READINESS POLICIES AND PROCEDURES

- Sono definite le **procedure e le autorizzazioni necessarie** per la raccolta di evidenze digitali di un dipendente?
- Sono state istituite procedure per la raccolta di evidenze digitali quando un **dipendente viene licenziato o abbandona la società**?
- Sono in essere procedure standard per la **cancellazione sicura dei supporti** prima che questi siano riutilizzati?
- E' stata definita una **politica di conservazione delle evidenze digitali** in termini di tempo (quanto) e luogo (dove, misure di sicurezza, ecc.)?
- Si utilizzano **banner di avvertimento** per gli utenti che indichino che l'uso non autorizzato delle risorse informatiche può essere monitorato?

DIGITAL FORENSICS READINESS
LEGAL AND PUBLIC RELATIONS

- L'ufficio legale (o lo studio esterno di fiducia) hanno **esperienza in materia di normative sui crimini informatici** e regolamenti sulla sicurezza dei sistemi e dei dati?
- E' stato definito, nel piano di gestione degli incidenti, idonea **procedura per la comunicazione interna e esterna**?
- E' stato definito chi deve essere **avvisato in caso di incidente**? (es. management, partner, clienti, dipendenti, forze dell'ordine, ecc.)
- E' definito chi deve **approvare comunicazioni pubbliche** da inviare ai soggetti di cui sopra a seguito di un incidente?

DIGITAL FORENSICS READINESS
ASSETS INVENTORY AND PROFILING

- E' presente in azienda un **inventario delle risorse hardware e software**, con precise identificazione degli utilizzatori? (es. notebook, mobile device, ecc.)
- Sono conservati **known good hash database** per i sistemi operativi e i software utilizzati all'interno dell'azienda?
- Sono definite con precisione le **configurazioni base per sistemi e dispositivi di rete**?
- Sono conservate **immagini di ripristino per tali configurazioni**?

DIGITAL FORENSICS READINESS
INFORMATION GATHERING AND PRESERVATION

- L'**allocazione degli indirizzi IP** alle risorse di rete è correntemente documentata e preservata (es. DHCP logs)?
- Sono conservati i **log di NAT translation**? Per quanto tempo?
- Se sono in uso **server proxy**, quali dati, come e per quanto tempo sono conservati?
- E' possibile attivare in tempi rapidi uno o più **network sniffer** in punti di aggregazione di traffico?
- Sono stata identificate possibili **SPAN port** nei punti nevralgici della rete?
- Il **traffico di rete verso Internet** viene monitorato (Network dump, NetFlow, ecc.)?
- Sono presenti **punti di monitoraggio dove si possa visualizzare il traffico decifrato**?
- E' possibile **acquisire da remoto il contenuto di un computer aziendale** (es. agent per il dump della RAM o per la copia del device di memorizzazione)?

DIGITAL FORENSICS READINESS
DATA PRESERVATION

- **Dove** sono memorizzati **i dati sensibili** dell'azienda?
- E' previsto e documentato **un piano delle autorizzazioni per l'accesso ai dati**?
- Sono conservati file di log dettagliati (es. username, IP address, Port, ecc.) **in relazione agli accessi ai dati** (lettura, scrittura, cancellazione, ecc.)?
- **Per quanto tempo** sono conservati?
- Se sono in uso politiche di **full disk encryption** l'azienda conserva copia delle recovery key?

DIGITAL FORENSICS READINESS
AUDITING AND LOGGING REVIEW

- E' stato verificato che **le comunicazione mail** siano recuperabili in caso di cancellazione da parte dell'utente? Per quanto tempo?
- E' stato verificato che **gli eventi sulla sicurezza del sistema** siano memorizzate sui sitemi critici e che le relative notifiche siano inviate a chi di dovere? (es. login errate, tentativi di bruteforce, ecc.)
- I sistemi critici **sono sincronizzati temporalmente con la stessa sorgente** (trusted)?
- E' stato implementato un **sistema centrale di log** per i sistemi critici?
- Per quanto tempo **sono conservati i file di log**?
- I file sono memorizzati su **dispositivi protetti da scrittura**? Viene calcolato **hash**?

DIGITAL FORENSICS READINESS TOOLS TESTING

- Il team di Incident Response/Forensics ha avuto la possibilità di testare l'efficienza degli strumenti in uso rispetto alle risorse aziendali?
- In particolare sono stati effettuati test relativi alla **possibilità tecnica di analizzare:**
  - Dispositivi mobile aziendali
  - Dispositivi con sistemi operativi particolari
  - Dispositivi industriali
- E' stato definito **un ambiente virtuale e propriamente separato dalla rete per l'analisi di malware?**

DIGITAL FORENSICS READINESS
LOGISTICS

- E' noto il **contatto di emergenza** per incidenti che si verificano su dati conservati **presso fornitori terzi**? (es. ISP, gestore dominio di posta, cloud storage/services, ecc.)
- Sono attivi contatti per la collaborazione e il supporto all'azienda da parte delle forze dell'ordine?
- Nel caso di aziende prive di un servizio di investigazione interno, è noto il servizio esterno al quale rivolgersi in caso di incidenti informatici?

DIGITAL FORENSICS READINESS
TRAINING AND AWARNESS

- Il personale aziendale è stato formato sulle **modalità di reporting di un incidente informatico**?
- Sono state fornite **le linee guida base comportamentali** per i primi interventi da parte dell'utente inesperto?
- Il proprio team investigativo (interno o esterno) è **adeguatamente formato** e **certificato** per svolgere quel ruolo?
- Esiste **un piano formativo** per garantire un livello di conoscenze elevato e **costantemente aggiornato** per i membri del team investigativo?

FIRST RESPONDERS ACTIONS

- Contattare immediatamente il team incaricato alla gestione dell'incidente
- **Non**
  - Effettuare login sul dispositivo
  - Effettuare logout dal dispositivo (se l'utente è in quel momento connesso)
  - Inserire alcun comando
  - Eseguire applicazioni
  - Interrompere applicazioni o processi
  - Riavviare il sistema
  - Spegnere il dispositivo
  - Fare rebuild del sistema
- Se strettamente necessario, e previo accordo con il team, disconnettere l'host dalla rete e registrare il momento esatto in cui questo avviene

IN CONCLUSIONE….

- Fare una valutazione degli aspetti che abbiamo introdotto (e anche altri) è fondamentale per poter gestire in modo efficace un incidente
- Nella maggior parte dei casi non è necessario introdurre nuovi dispositivi o strumenti di rilevamento, ma ottimizzare quanto già c'è
- Il miglior modo per valutare se siamo pronti a fare una investigazione forense? **Simulare l'incidente**
- Es. simulare un furto di dati, simulare un'infezione tramite malware, verificare quali file di log abbiamo a disposizione, verificare cosa può succedere in caso di smarrimento di un dispositivo, ecc.

REALITY NET
System Solutions

Security & Digital Investigations

www.realitynet.it

Genova
via Assarotti 4/1
tel. 010.837.62.57

Milano
via Giuseppe Luosi 14
tel. 02.871.972.30

REALITY NET
System Solutions