Risposta agli Incidenti Informatici

Vincenzo Calabrò

Malware

Software creato con lo scopo di causare danni ai dati di un sistema informatico sul quale viene eseguito

- **Malware**: software creato con lo scopo di causare danni ai dati di un sistema informatico sul quale viene eseguito
- **Ramsoware**: malware che chiede riscatto per rimuovere il danno
  - **Cryptolocker**: ramsoware che cifra i dati di un sistema vittima e chiede riscatto per decifrare
- **Virus**: malware in grado di infettare altri computer tramite un eseguibile autoriproducendosi
  - I virus possono essere dannosi per il sistema operativo che li ospita, ma anche nel caso migliore comportano comunque un certo spreco di risorse in termini di RAM, CPU e spazio sul disco fisso
  - Il termine virus viene frequentemente ed impropriamente usato come sinonimo di malware
- **Worm**: di malware in grado di autoreplicarsi senza necessità di eseguibili per diffondersi
- **Trojan**: malware nascosto all'interno di altri programmi che apre una backdoor per controllare il sistema da remoto; il sistema vittima è detto *bot* o *zombie*
  - I sistemi vittima di trojan possono comporre delle **botnet**
- **Dialer**: malware che crea una connessione tramite la linea telefonica in maniera automatica senza consenso dell'utente (esistono comunque dialer legittimi).
- **Spyware**: malware che raccoglie informazioni riguardanti l'attività online di un utente senza il suo consenso, inviando all'esterno via Internet (es. per inviare spam mirato)

DoS e dDoS

- **DoS**
  - **Denial of Service**
  - Attacco informatico con il quale si cerca di rende indisponibile un sistema informatico (ad esempio un sito web) portandolo al limite delle prestazioni
- **dDoS**
  - **Distribuited Denial of Service**
  - funzionamento identico ma realizzato utilizzando numerose macchine attaccanti che insieme costituiscono una *botnet*
    - gli attaccanti si avvalgono di *botnet* di *zombie* infettati da *trojan*
    - quando il numero di *zombie* è ritenuto adeguato o quando viene a verificarsi una data condizione, gli *zombie* si attivano ed eseguono l'operazione richiesta

Phishing

- Mediante tecniche di ingegneria sociale, si induce la vittima a fornire dati personali, codici di accesso a servizi (tipicamente, home banking o numero di carta di credito). L'induzione fraudolenta delle vittime a fornire tali dati può avvenire:
  - mediante l'invio casuale ad un ampio numero di vittime ignare di messaggi di posta elettronica che fanno riferimento per forma e contenuto a siti bancari o postali o istituzionali o normalmente frequentati dalla vittima, o riportano link a siti come quelli di cui si è detto, con richiesta di effettuare operazioni di inserimento dati per il compimento di operazioni di cui la vittima ignora il contenuto fraudolento
  - mediante contatti telefonici
  - mediante l'invio di SMS (SMISHING)

Pharming

- Tecnica fraudolenta di cracking, evolutiva del phishing, utilizzata per ottenere l'accesso ad informazioni personali e riservate, con varie finalità
- Si basa sul fatto che ogni volta che un utente digita nel proprio browser l'indirizzo di una pagina web nella forma alfanumerica (come www.pippo.it) questo viene tradotto automaticamente dal server DNS del proprio provider in un indirizzo IP numerico (ad es. 145.97.39.155) che serve al protocollo IP per reperire nella rete internet il percorso per raggiungere il server web corrispondente a quel dominio
- Il pharming si attua indirizzando la vittima ignara verso un server web "clone" appositamente attrezzato per carpire i dati personali della vittima
- Con questa tecnica l'utente rivela inconsapevolmente a sconosciuti i propri dati personali, sensibili o meno, nonché i codici e/o la password di accesso ai servizi di home banking, di autorizzazione dei pagamenti oppure il numero della carta di credito

Spoofing

- Tecnica fraudolenta consistente in un attacco informatico attuato previa falsificazione dell'identità dell'attaccante (spoof) con la quale l'attaccante può, sotto falsa identità, accedere ai servizi ed alle risorse consentiti al sostituito

Port scanning

- Tecnica informatica utilizzata per raccogliere informazioni su un computer connesso ad una rete stabilendo quali porte siano in ascolto su una macchina
- Tale attività può essere svolta sia per scopi legittimi (ad es. verifica dei servizi disponibili), sia per scopi illegittimi (ad es. quale attività preparatoria di accessi abusivi a sistema informatico o telematico)

Sniffing

- Tecnica di intercettazione passiva dei dati che transitano in una rete
- Tale attività può essere svolta sia per scopi legittimi (ad esempio l'analisi e l'individuazione di problemi di comunicazione o di tentativi di intrusione), ma anche per scopi illeciti (ad es. intercettazione fraudolenta di password o di altri dati, anche personali)
- Gli sniffer intercettano i singoli pacchetti e ricostruiscono il flusso (salvo casi di uso di protocolli cifrati)

Gestione degli incidenti

Approccio tipico

- «*Oh no… un incidente informatico… E ora cosa facciamo?*»
- Ricerca di una soluzione rapida e semplice
- Fallita la soluzione individuate, si convive con l'incidente per lungo tempo
- Se qualcuno a capo se ne accorge, aggiornare il CV e cercare un altro lavoro, altrimenti continuare come se nulla fosse…

Soluzione migliore

- Cominciare prima che l'incidente si verifichi: perchè attendere di subirlo?
  - Avviare il processo decisionale e di gestione in situazioni di tranquillità
- Rendere gli incidenti parte delle attività, del budget, delle policy di sicurezza: cioè **valutare, ridurre e gestire i rischi**
  - Riduzioni dei costi
  - Processi definiti e non attacchi di panico o improvvisazione
  - Gestione (a costi ridotti) con compagnie assicurative
  - Individuazione con calma dei partner esterni

Valutazioni

- Backup
  - Come vengono fatti? Con che frequenza? Dove sono conservati? **Sono fatti dei test di recovery?**
- Quali sono gli asset da proteggere?
  - Quali sono i rischi ai quali vanno incontro gli asset (fisici)?
    - Come si opera in caso di furto o danneggiamento?
  - Quali sono i rischi ai quali vanno incontro I sistemi informative (dati)?
  - Quali sono le vulnerabilità da tenere sotto controllo?
  - Come possono manifestarsi i rischi individuati?
- Viene effettuato un monitoraggio del traffico di rete?
  - Quali sono le comunicazioni fisiologiche?
  - Quali sono i servizi e gli interlocutori inibiti? E quali permessi da controllare?
  - Quanto è veloce la rete?
  - Quali servizi sono esposti all'esterno? E come sono protetti?
- Quale sistema di posta elettronica viene utilizzato?
  - Chi può spedire? Sono implementate misure di sicurezza per spedire?

Valutazione

Livelli da valutare e controllare

- Sicurezza fisica e logica
  - Dati
  - Applicazioni
  - Dispositivi
  - Rete
  - Perimetro e locali
  - Documentazione non digitale
- Persone
  - Know how
- Processi
- Policy

Partire con attività soft

- Definire policy
- Organizzare gli staff
- Mettere a calendario la formazione per il personale
- Valutare periodicamente le vulnerabilità
  - Autonomamente o con consulenti esterni
  - Non dimenticare test di social engineering
  - Eseguire tali valutazioni con tutte le opportune autorizzazioni
- Mantenere aggiornati i sistemi
- Policy rigide sulla gestione delle password
- Definire i comportamenti “fisiologici” di sistemi e rete
  - Quindi monitorare e analizzare il traffico di rete e le performance di rete e sistemi
  - Effettuare analisi (almeno con dati aggregati) dei log
- Verificare i backup
  - È efficiente? I dispositivi funzionano? Provati dei ripristini?

CSIRT

- Gruppo di persone che intervengono in risposta all'incidente
  - Competenza, esperienza, responsabilità, autorità
  - Da costituire in un momento di tranquillità, non mentre è in atto l'incidente
  - Definire chiaramente i ruoli: non deve esserci nessuno che possa dire "non è il mio ruolo"
- Parte attiva nelle riorganizzazioni aziendali e nella gestione dei sistemi informative
- Monitorare vulnerabilità e rischi e ricerca soluzioni e processi per mitigare/eliminare i rischi
- Ruolo di controllo centrale
- Riceve notizie di possibili incidenti, li valuta e li documenta
- Promuove consapevolezza della sicurezza in azienda
- Referente in caso di audit o intervento autorità giuridizia

CSIRT: Computer Security Incident Response Team

- Formazione per l'uso degli strumenti più idonei
  - Conoscenza delle funzionalità vari tool esistenti
  - Acquisto o rapida disponibilità al noleggio
  - Utilizzo dei tool
- Rapporti interpersonali e competenze giuridiche
  - Contatti
  - Legali
    - Coinvolgere I legali non appena si evidenzia risvolto giuridico
  - Polizia Giudiziaria e Autorità Giudiziaria
  - Internet Service Provider
  - Rapporti con media e stampa
- Raccogliere dati urgenti e rilevanti anche in contesti offline
  - Se in formato elettronico, cifrarle
    - Password
    - Configurazioni
    - Informazioni riservate
    - Procedure

CSIRT Team

- Team leader
  - Organizza il lavoro ed è responsabile del team
- Incident leader
  - Responsabile nella gestione di uno specifico incidente e della squadra che lo affronta
  - Nominato dal team leader sulla base delle competenze e del caso specifico
- Incaricati alla gestione
  - Collaborano alla gestione degli incidenti
- Membri associati
  - Collaborano nella gestione dell'incidente pur non essendo parte del CSIRT
    - Referente IT
      - Coordina le comunicazioni tra CSIRT e dipartimento IT
    - Referente legale
      - Coordina le comunicazioni tra CSIRT e ufficio legale
      - Questioni relative alle policy e alle contestazioni
      - Valuta profili di natura penale e civilistica
    - Referente informatica forense
      - Raccoglie prove informatiche
    - Referente Pubbliche Relazioni
      - Gestisce l'incidente verso l'esterno
    - Management aziendale
      - Definisce l'impatto aziendale dell'incidente
      - Valuta l'operato dei vari membri coinvolti

Ruoli e responsabilità nelle varie fasi

	Incident leader	Referente IT	Referente Legale	Referente informatica forense	Referente P.R.	Management
Valutazione iniziale	**Responsabile**	Collabora		Aggiornato		
Risposta iniziale	**Responsabile**	Implementa	Aggiornato	Aggiornato	Aggiornato	Aggiornato
Raccolta evidenze informatiche	Collabora	Collaboratore	Aggiornato	**Responsabile**		
Soluzione temporanea	**Responsabile**	Implements	Aggiornato	Collabora	Aggiornato	Collabora
Comunicazioni con l'esterno	Collabora	Collabora	Collabora		Implementa	**Responsabile**
Rapporti con l'autorità giudiziaira	Aggiornato	Aggiornato	**Responsabile**	Collabora	Aggiornato	Collabora
Soluzione definitiva all'incidente	**Responsabile**	Implementa	Aggiornato		Aggiornato	Aggiornato
Valutazione dell'impatto dell'incidente e dell'operato dei vari membri	Aggiornato	Aggiornato	Collabora		Aggiornato	**Responsabile**

Incident response

- Definiamo incidente ogni situazione di violazione
  - Es. un utente riesce ad avere accesso a un sistema a cui non è autorizzato ad accedere
- Un esempio: accesso a sistema o ai dati non autorizzato
  - Uso di account non assegnato
  - Uso di account altrui
  - Uso di vulnerabilità del sistema
  - Ma anche… uso improprio del proprio account

- L'incident response rappresenta la risposta all'incidente informatico
  - Chi subisce l'incidente deve essere in grado di verificare rapidamente se tale evento vada considerato un incidente informatico o meno ed eventualmente mettere in atto una serie di metodiche al fine di poter reagire efficacemente alla minaccia rilevata
    - Garantire la tempestiva identificazione dell'evento
    - Garantire la sua eventuale classificazione in "incidente informatico"
    - Decidere le conseguenti operazioni da svolgere tempestivamente nel momento in cui l'evento viene segnalato
    - Programmare successive attività di investigazione atte a reperire possibili fonti di prova

Alcuni esempi

- **L'utilizzo non autorizzato di servizi**
- il gioco
- mail relay
- accesso remoto
- l'utilizzo di apparecchiature aziendali per uso personale guadagno
- server personali sulla rete
- **Spionaggio**
- monitoraggio e-mail
- Utilizzo di ISP
- il furto del notebook
- la copia dei dati
- masterizzatori CD, unità zip, memoria flash
- semplici metodi di trojan / tunneling
- **Hoaxes**
- **Sonde aggressive**

Come si opera

- Rilevamento
  - Riconoscimento del potenziale incidente
- Identificazione
  - Identificazione delle potenziali prove relative all'incidente
  - Avviare catena di custodia e acquisizione
- Conservazione
  - Mantenimento delle prove informatiche raccolte (integrità, attendibilità, conservazione a lungo termine)
- Analisi
  - Analisi delle prove informatiche rilevate

- Si rientra nelle attività di informatica forense

Cosa prevede il piano di Incident Response

- Prima valutazione
- Comunicazione dell’incidente
- Contenimento danni e riduzione al minimo del rischio
- Identificazione del tipo e della gravità del sistema compromesso
- Proteggere le evidenze
- Notifica a contatti esterni di supporto all’azienda (se ci sono)
- Ripristino dei sistemi coinvolti
- Documentazione completa dell’incidente
- Valutazione dei danni e dei costi
- Rivedere le politiche di risposta e aggiornamento

Effettuare un assessment iniziale

- È un problema di configurazione?
- Iniziare cercando di determinare tipo e gravità
- Ottenere informazioni per ulteriori studi e successiva comunicazione
- Come pensare di contenere il tutto?
- Registrare tutto quello che si fa

- **Comunicazione dell'incidente:**
  - Comunicare al team del CSIRT
  - Stabilire chi eventualmente contattare fuori dal team

Contenimento del danno

- Rapidità e decisione possono fare la differenza
- Priorità
  - Proteggere i dati classificati e sensibili
  - Proteggere altri dati (proprietario, scientifico, gestionale)
  - Proteggere hardware e software
  - Minimizzare l'interruzione di risorse di calcolo
- Fare un confronto dei costi
- Disabilitare punto di ingresso malevolo
- Ricostruire il sistema violato da zero
- Cambiare le password
- **Obiettivo**: tornare in linea nel più breve tempo possibile, proteggendo le persone, preservare le attività ed evitando che l'incidente si verifichi nuovamente

Determinare la natura dell'attacco

- Questa fase potrebbe essere diversa dall'assessment iniziale
  - Qual è l'origine?
  - Quali sono gli obiettivi finali?
  - Quali sono i sistemi compromessi?
  - A quali files hanno avuto accesso?

Determinare la gravità dell'attacco

- Lavorare con gli altri membri del CSIRT team
  - Sono tutti d'accordo con l'assessment iniziale?
- Si sono verificati degli accessi non autorizzati?
- Nel gruppo di amministrazione sono comparsi dei membri nuovi ed inaspettati?
- Ci sono nuovi programmi in esecuzione automatica?
- Eventuali lacune nei log?
  - Eventuali errori di accesso
    - Orari e tempi da correggere
- Cambi di permessi improvvisi
- Cosa c'è di diverso ora rispetto al precedente controllo?
- Sono presenti dati non rilevanti per l'azienda?
  - Es: porno, musica…
- Tutti i dati dei dipendenti sono in pericolo?
  - Eventi ripercussioni su privacy
- Qualche cambiamento nelle prestazioni?

Raccogliere e proteggere le prove

- Fare sempre un’acquisizione
  - Meglio in doppia copia
  - Meglio su supporti di tipo diverso (es. su hd da conservare e su un NAS)

- Più motivi
  - Da utilizzare per recupero dei dati rilevanti
  - Per analizzare cosa è accaduto
  - Per raccolta prove

- Documentare ogni cosa

Comunicazione all’esterno

- Potenziali contatti
- Forze di polizia locali e nazionali
- Agenzie di sicurezza
- Esperti di malware
- Coordinarsi con il proprio legale
- Quale tipo di dichiarazione pubblica?
  - Dipende dal tipo di azienda
  - Dipende dal tipo di clientela
  - Dipende dall’effetto dell’incidente

Compilare e organizzare la documentazione

- Che tipo di attacco è stato?
- Che risposta è stata data?
  - chi
  - quando
  - perchè
- Organizzare ed esaminare la documentazione con il legale rappresentante
- **Verificare anche la possibilità dell'esistenza di un insider**

Valutazione danni e costi

- Verificare i costi diretti ed indiretti
  - Perdita di competitività (causata dalla perdita di informazioni confidenziali)
  - Perdita da inattività
  - Spese legali
  - Spese per indagine
  - Spese per recovery
  - Sostituzione hw/sw
  - Costi di aggiornamento
  - Danni reputazionali

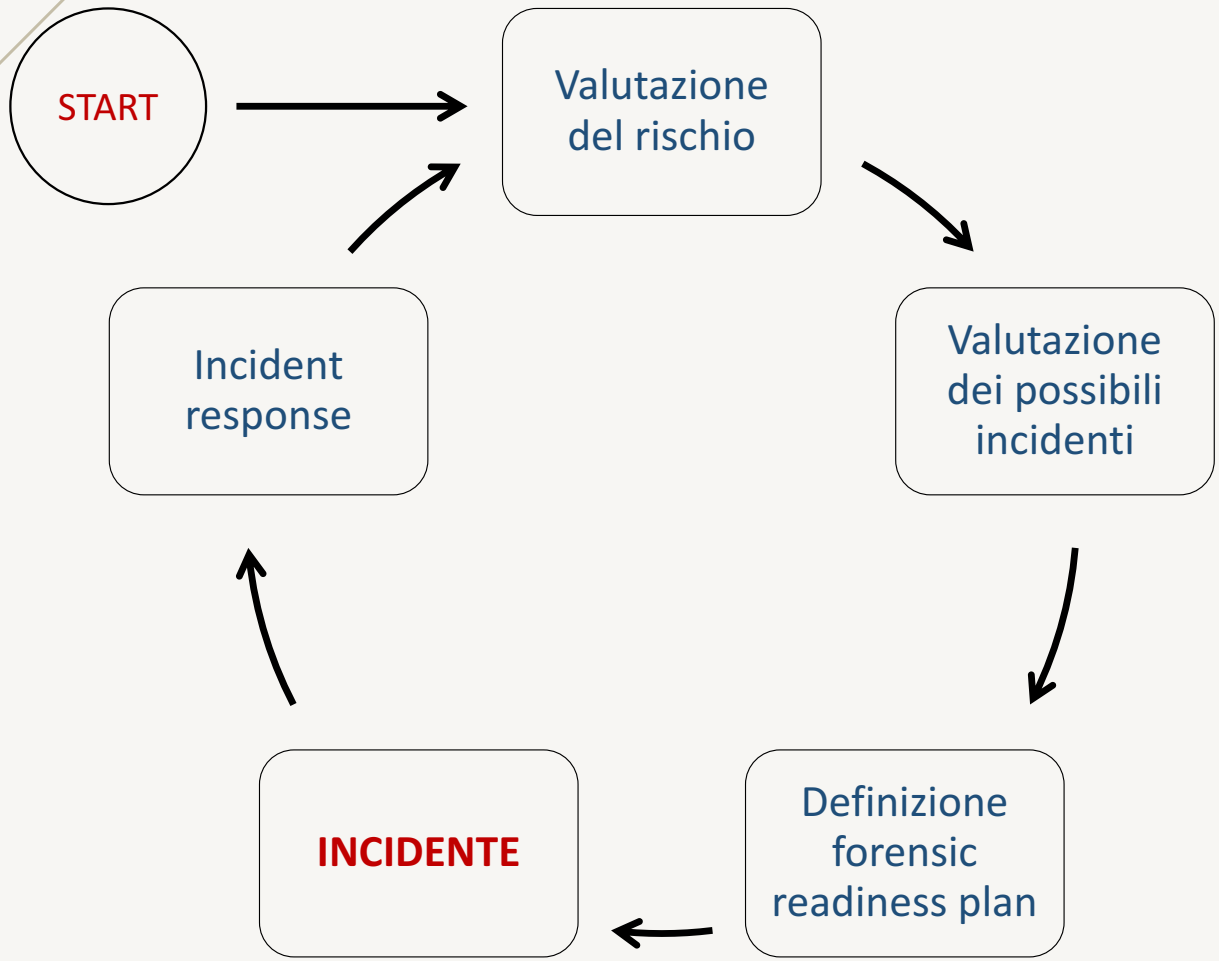
Revisione e aggiornamento

- Domande da porsi in generale
  - Cosa è andato bene?
  - Cosa invece necessita di essere migliorato?
  - Come fare meglio la prossima volta?
- Politiche di aggiornamento
  - Possono essere fatte meglio?
  - Vi sono opportunità di snellimento?
- Considerate le nuove tecnologie
  - Possono essere migliorati i meccanismi di prevenzione?

Utilizzo di prove informatiche

- Contestazioni contrattuali tra cliente e fornitore
  - Es. Decreto ingiuntivo su contratti stipulati via email
- Contestazioni disciplinari del personale
  - Es. PC usato in maniera impropria
- Dimostrazione di rispetto di norme
  - Es. Spese rientranti tra gli investimenti del superammortamento
- Assistenza all'autorità giudiziaria in caso di coinvolgimento dell'azienda
  - Es. Rivendicazione terroristica partita da PC aziendale
- Supporto alle assicurazioni se presenti
  - Es. Dimostrazione che l'azienda non aveva criticità di sicurezza

La gestione dell'incidente



- Incident Response
  - Azioni da porre in essere in caso di incidente
- Forensic Readiness Plan
  - Piano di gestione, trattamento e conservazione dei dati digitali

Forensic readiness plan

- Che cos'è?
  - Documento che definisce esattamente cosa fare quando è richiesta una prove elettronica, sia come parte di un'azione legale, sia come risposta ad indagini interne o procedure disciplinari. Il suo scopo è quello di massimizzare la quantità di dati che è prontamente disponibile e ridurre al minimo il tempo ed denaro necessari a proteggere i dati richiesti
- In che cosa consiste?
  - Identificare i tipi di prove elettroniche al fine di identificare eventuali lacune nelle attuali procedure
- Obiettivi
  - Massimizzare l'efficacia dell'azione in caso di incidente informatico, minimizzare l'effetto dell'incidente
  - Ridurre al minimo il costo di incident response

Forensic readiness plan - Fasi

- Definizione degli scenari di business
  - Per ognuno di essi, definizione delle possibili fonti e tipologie di prove digitali
  - Definizione delle modalità di raccolta delle prove digitali
    - Soddisfare requisiti di integrità e non ripudiabilità in dibattimento
- Definizione di politiche di monitoraggio a scopo di prevenzione e di individuazione di incidenti informatici
- Definizione dei casi di richiesta di approfondimento di analisi
- Definizione delle modalità di gestione del caso per preparazione le opportune azioni legali
- Formazione del personale
  - Cultura della sicurezza
  - Assegnazione dei ruoli in caso di incidente
  - Simulazioni

Tutto nell'ottica del trattamento dei dati informatici da utilizzare come prove

Core del forensic readiness plan

- Raccolta di dati digitali
- Catena di custodia
- Conservazione e integrità
- Ripristino dei sistemi coinvolti da fonti sicure

- Procedure di logging
  - Protezione dei log
- Sincronizzazione dei timestamp

Return of investiment (ROI) del Forensic readiness plan

- Il piano si ripaga con:
  - Velocità di individuazione dell'attacco
  - Identificazione e isolamento delle informazioni rilevanti
  - Prontezza nella rimozione della minaccia
  - Recupero efficace dal danno in maniera completa e in poco tempo
  - Formazione per tempo
  - Sconti dalle compagnie assicurative
- Danni da assenza di FRP:
  - Perdita di business
  - Danni reputazionali
  - Perdita di clienti
  - Perdita di denaro
  - Azioni legali da parte di controparti
  - Divulgazione di dati (furto)
  - Perdita di dati (distruzione)
  - Inutilizzabilità dei sistemi

Vincenzo Calabrò

info@vincenzocalabro.it

www.vincenzocalobro.it

LinkedIn vincenzocalabro