La Risposta agli Incidenti Informatici

Antonio Barili

Dipartimento di Ingegneria Industriale e dell'Informazione
Università di Pavia

Introduzione

Incidente informatico

Evento che determina la compromissione degli obiettivi definiti di:

- Riservatezza (Confidentiality)
- Integrità (Integrity)
- Disponibilità (Avaliability)

di un sistema informatico/telematico o delle informazioni da esso trattate

Introduzione

Attacco informatico

Una sequenza di atti preordinati a causare un *incidente informatico* e/o a sfruttarne gli effetti

- Un incidente può essere l'effetto di *eventi casuali* o *colposi* (per imperizia, imprudenza, negligenza o inosservanza di norme imperative)

- Un attacco è sempre *doloso*
- Un attacco può essere mirato (*targeted*) o non mirato (*untargeted*)
  - La prevenzione contro gli attacchi *untargeted* è molto più efficace rispetto a quella contro gli attacchi *targeted*

Introduzione

- Oltre 2/3 degli incidenti informatici hanno origine accidentale o colposa
  - Incendi, allagamenti, problemi alle linee elettriche o ai sistemi di condizionamento, guasti alle apparecchiature di elaborazione …
- La maggioranza degli incidenti di origine dolosa è riconducibile a *insider*
- Solo una piccola parte (degli incidenti di origine dolosa) è attribuibile a *outsider*
  - Criminalità organizzata
  - Criminalità economica
  - *State/government level threats*
  - *Hacktivism*

Introduzione

- Come per ogni aspetto della sicurezza, la gestione della sicurezza informatica passa attraverso 3 fasi
    1. Analizzare e valutare i rischi
    2. Mitigare i rischi all'origine
    3. Istituire idonee misure preventive e protettive

- Come parte della fase 3: istituire idonee misure di gestione degli incidenti

<u>A monte di tutto, è necessario acquisire una adeguata comprensione del fenomeno</u>

Caso 1 – Data Exfiltration/Leak

- Ogni volta che informazioni riservate vengono communicate a terzi o diffuse in pubblico siamo in presenza di un caso di *data exfiltration* o *data leak*
    1. Insider (accesso abusivo)
    2. Outsider (criminalità economica)
    3. Usato come minaccia per favorire l'adesione a schemi estorsivi (ransomware)

Caso 2 – Frodi (BEC)

- Il panorama delle frodi è molto ampio e variegato; in questa sede ci si limita al Business Email Compromise (BEC)
- L'agente, sfruttando credenziali rubate/compromesse, impersona un soggetto aziendale munito di poteri negoziali e/o dispositivi e avvia transazioni commerciali o dispone pagamenti verso conti correnti che vengono poi 'svuotati' facendo sparire i proventi della frode
    1. Insider (raro, in genere non considerato un incidente informatico)
    2. Outsider (criminalità economica)

Caso 3 – DDoS

- Nel DDoS (Distributed Denial of Service) l'agente genera un numero enorme di richieste sui servizi esposti in rete, rendendoli inaccessibili agli utenti legittimi
    1. Insider (rarissimo)
    2. Outsider (criminalità economica, per finalità estorsive)

Caso 4 – Ransomware

- In un attacco basato su ransomware, un software malevolo (il *ransomware*) cifra i dati aziendali e viene richiesto un riscatto (ransom) per decifrarli
- In genere l'attacco è preceduto da una *exfiltration* per rafforzare la richiesta di riscatto con la minaccia di diffusione (vanificando l'eventuale esistenza di copie di backup)
    1. Outsider (criminalità organizzata, l'attacco richiede una tecnologia software e una organizzazione avanzata e tempi lunghi per la sua esecuzione)
    2. State/government level threats: attacchi contro istituzioni o imprese di interesse pubblico

Le Cause (Insider)

- Insider (cosa spinge un insider a ‘tradire’ ?)

  What’s a cat business? Catching MICE

  - (M)oney
  - (I)deology
  - (C)oercion
  - (E)go

Le Cause (Outsider)

- Attacchi *untargeted*
  - Opportunity
  - Gli attacchi untargeted vengono condotti con strumenti automatici di *scanning/reconnaissance* di vulnerabilità sfruttabili
- Attacchi *targeted*
  - Exposure (esposizione al rischio)
  - Gli attacchi targeted richiedono investimenti significativi (da parte dell'agente) e organizzazioni strutturalmente e tecnologicamente avanzate
- Esiste una zona grigia di attacchi tecnicamente *untargeted*, ma con obiettivi ben delimitati (es. frodi informatiche bancarie)

I Rimedi

- Insider e attacchi *untargeted*
  - Gestione del rischio informatico e adeguata diffusione interna delle procedure (e della loro esistenza, come deterrente)

- Attacchi *targeted*
  - Gestione del rischio informatico
  - Adeguare il livello delle misure difensive al rischio reale (nota: l'agente potrebbe avere una scala di valori diversa dalla vostra…)

I Rimedi (in dettaglio)

- *Backup* e sistemi di continuità operativa (*disaster recovery*)
- Adeguata gestione delle credenziali (abilitare 2FA ovunque possibile, sicuramente per gli amministratori del sistema e per i soggetti muniti di poteri significativi)

- Storicizzazione (sicura) degli eventi di sistema (logging)
- *Audit* periodico dei log (gli attacchi più gravi sono preceduti da un 'lungo' periodo di preparazione)

- Formazione…
  - es. perché le password vanno cambiate periodicamente?)

… e se succede lo stesso?

- Deve esistere una procedura di gestione almeno per le tipologie di incidenti più frequenti (eventi accidentali, esfiltrazioni, frodi…)
- Evitare di cancellare le tracce dell'evento nel tentativo di rimediare o ripristinare l'operatività aziendale
    - La possibilità di investigare sulle cause e individuare l'agente è un potente deterrente!
- Allertare le Istituzioni preposte alla repressione del crimine
- Notificare alle potenziali vittime indirette del rischio potenziale (GDPR)

Conclusioni

Il generale che combatte mille battaglie e riporta mille vittorie

Non è il migliore di tutti

Il generale che sottomette il nemico senza combattere

Quello è il migliore di tutti

(Sun Tzu, L'arte della Guerra, VI-V sec. A.C.)