Appunti della lezione di Cybersecurity

Corso universitario — Lezione 3 Prof. Talamo

Indice

1 Registry e mappatura su DNS

- I registry virtualizzano risorse e si occupano della distribuzione degli stessi.
- Se un attaccante compromette un registry, può alterare l'associazione tra un'identità logica e il suo indirizzo fisico (es. record DNS) e quindi impadronirsi dell'identità di un soggetto agli occhi degli altri sistemi.
- Un attacco al registry si propaga su tutti gli oggetti che dipendono da quella mappatura.
- Per accedere al DNS è necessario un protocollo specifico: la sua implementazione e gestione diventano quindi superfici d'attacco critiche.

2 Esempio: attacco a infrastruttura cloud (caso pratico)

- Caso esemplificativo: attacco che ha interessato un provider (es. scenario tipo Amazon).
- L'attaccante ha preso il controllo del registry virtuale: la risposta dell'operatore è stata chiudere il registry compromesso e aprirne uno nuovo.
- L'avversario si era invece posizionato sulle macchine virtuali, rendendo l'impatto più esteso e meno evidente; parte dell'utenza resta inconsapevole del danno subito.
- Domande critiche: perché l'infrastruttura presenta questa architettura? Quale componente é stato effettivamente attaccato? (registry, hypervisor, VM, rete, ecc.)

3 Architettura vs infrastruttura di sicurezza

Architettura sistemistica l'insieme dei componenti hardware e software e la loro organizzazione (es. macchine, hypervisor, rete, DB).

Infrastruttura della sicurezza le soluzioni, le politiche e i processi che si adottano per proteggere i contesti rilevanti all'interno dell'architettura.

4 Standard e protezione delle vulnerabilità

- Negli anni 2000 si svilupparono iniziative in Europa e negli USA per progettare infrastrutture digitali sicure: l'obiettivo era progettare sistemi orientati alla protezione delle identità e dei contesti.
- Una *potenziale vulnerabilità* viene qui definita come un "contesto" che contiene informazioni e che decidiamo di proteggere perché distinguibile e identificabile.
- L'elemento comune èl'esistenza di un'identità associata ad un contesto informativo; intorno a questo concetto nascono protocolli e linee guida (es. best practices, norme per il trattamento dati).

5 Filosofia dei contesti e livello di astrazione

- L'approccio basato sui contesti introduce un livello di astrazione: invece di difendere singoli componenti isolati, si individuano contesti identificati (es. servizi, archivi, funzioni) e si progetta la difesa attorno a questi.
- Questo approccio è empirico e spesso non visibile nella progettazione iniziale dell'architettura.

6 Esempio reale: gestione di un "Comune"

Descriviamo un esempio pratico per capire la logica dei contesti.

- **Contenitori/servizi presenti:**
  - Comando vigile (archivio multe, dati anagrafici, archivio personale, integrazione videosorveglianza)
  - Museo (archivi propri, biglietteria con carte di credito)
  - Portale cittadino con accesso via login collegato a un database centrale
- **Analisi del rischio e vettori d'attacco:**
  - La sezione *museo* può essere particolarmente critica per la presenza di dati di pagamento (biglietteria online): un attacco qui potrebbe portare a frodi finanziarie.
  - Un attaccante che compromette il portale di accesso può potenzialmente raggiungere l'intero sistema se il portale funge da punto di ingresso comune al database centrale.
  - La scelta di difendere solo una parte dell'infrastruttura (es. il "comando vigile") rischia di lasciare scoperti altri contesti più sensibili.
- **Identità del contesto:** l'identità da proteggere non è solo username/password, ma l'identità del contesto (es. il ticket + carta di credito nella biglietteria).

7 Perimetro e superficie d'attacco

- Il perimetro è il confine che racchiude tutti i contesti appartenenti a una struttura (es. l'insieme dei servizi di un Comune).
- La superficie d'attacco è l'insieme dei punti di vulnerabilità compresi all'interno di quel perimetro: punti di accesso, API, portali, database, servizi esterni collegati, ecc.
- Definire il perimetro aiuta a raggruppare contesti e a calcolare la superficie d'attacco in modo strutturato.

8 Esercizio proposto

1. Scegliere un'architettura di riferimento (es. architettura database, architettura di servizio su cloud).
2. Disegnare il perimetro: elencare i contesti che appartengono alla struttura.
3. Per ogni contesto decidere quale sia la superficie d'attacco (vettori principali, dipendenze esterne, punti di ingresso).
4. Applicare l'analisi a una piattaforma cloud moderna (es. Microsoft Azure): mappare i servizi Azure usati (VM, App Service, Azure AD, Database, Storage, Gateway) e valutare perimetro e superficie d'attacco.

—