LEZIONE 2 DALL' IDENTITÀ AL DISEGNO CYBER DI UN SISTEMA DIGITALE

Come si può facilmente rilevare le principali normative sviluppate per rafforzare la difesa di componenti digitali riguardano l'identità

Le principali normative , ad esempio, che influenzano la gestione dell'identità nei sistemi distribuiti sono:

- **Regolamento eIDAS 2:** introduce l'European Digital Identity Wallet e la fiducia transfrontaliera.
- **Direttiva NIS2:** impone autenticazione sicura nei servizi essenziali.
- **NIST SP 800-63-3:** definisce livelli di garanzia (IAL, AAL, FAL).
- **GDPR:** obbliga alla minimizzazione dei dati e alla trasparenza nel trattamento.

L'identità digitale nei sistemi distribuiti è il fondamento della fiducia operativa.
Non esiste un modello perfetto: le scelte dipendono da scala, governance e requisiti di interoperabilità.
Le architetture moderne tendono a soluzioni **ibride**, che combinano controllo centralizzato e autonomia distribuita, mantenendo la coerenza normativa (eIDAS 2, NIS2, NIST).

Come passare da questo aspetto specifico apparentemente alla visione generale di della cybersecurity di un sistema digitale?

Per fare ciò dobbiamo introdurre due concetti fondamentali: il perimetro e la superficie di attacco di un sistema digitale

Perimetro e Superficie di Attacco

Nella sicurezza informatica i concetti di perimetro e superficie di attacco definiscono i confini di fiducia e i punti di esposizione di un sistema.

Nel modello tradizionale il perimetro coincideva con la rete interna o con il firewall; oggi, secondo il NIST SP 800-207 (Zero Trust Architecture), il perimetro è una funzione logica centrata su identità e contesto, mentre la superficie di attacco è distribuita e dinamica.

Superficie di Attacco

Definizione

La superficie di attacco è l'insieme di tutti i punti, interfacce e processi attraverso cui un attaccante può tentare di compromettere la sicurezza di un sistema.

Comprende componenti tecniche, logiche e umane.

Categorie principali:

– Superficie tecnica : servizi, protocolli, dispositivi IoT, firmware.

– Superficie logica : software, API, database, identità digitali.

– Superficie umana : utenti, errori, procedure, ingegneria sociale.

Esempio

Un portale cloud con autenticazione web, API REST e database interno espone diversi livelli di interazione.

La combinazione di questi elementi costituisce la superficie di attacco.

L'hardening serve a ridurre tale superficie disattivando servizi superflui, chiudendo porte inutili e segmentando gli ambienti.

Perimetro: definizione tradizionale e limiti

Definizione tradizionale

Il perimetro di sicurezza è il confine entro cui un'organizzazione esercita controllo sulle proprie risorse e applica le politiche di protezione.

Nel modello classico coincideva con la rete interna difesa da firewall e proxy, presupponendo che l'interno fosse "trusted".

Limiti del modello tradizionale

Con cloud, smart working e identità federate (SPID, eIDAS, SSO) la distinzione "interno/esterno" non è più valida:

gli utenti accedono da reti non controllate e i dati sono distribuiti su piattaforme terze.

Perimetro identità-centrico (secondo NIST SP 800-207)

Definizione

Il perimetro non è più una barriera di rete ma una funzione logica costruita intorno a identità, dispositivo e contesto di accesso.

Elementi fondamentali:

1. Identità – rappresenta l'utente, il dispositivo o il servizio autenticato.
   Obiettivo: garantire autenticità e affidabilità.
2. Contesto – comprende rete, posizione, orario, livello di rischio.
   Obiettivo: applicare autorizzazioni dinamiche.
3. Policy dinamiche – insieme di regole di accesso basate sul rischio e aggiornate in tempo reale.

Ogni richiesta di accesso viene valutata in base a identità, contesto e rischio, seguendo il principio never trust, always verify.

Esempio

Un docente accede da casa al portale didattico: identità verificata via SPID, dispositivo registrato e fascia oraria autorizzata.

Il perimetro è logico e segue l'identità, non la rete.

Dal perimetro fisso al perimetro dinamico

Nel modello tradizionale:

- il confine di sicurezza è il firewall o la rete interna;
- l'accesso interno è implicitamente fidato;
- le autorizzazioni sono statiche;
- il controllo è centralizzato;
- la visibilità è limitata al perimetro fisico.

Nel modello Zero Trust (NIST):

- il confine di sicurezza è definito da identità e contesto;
- ogni accesso richiede verifica continua;
- le autorizzazioni sono dinamiche e basate sul rischio;
- il controllo è distribuito;
- la visibilità comprende utenti, dispositivi e sessioni.

Ogni nodo o utente diventa un micro-perimetro con regole proprie di autenticazione e monitoraggio.

Relazione tra Perimetro e Superficie di Attacco

- Il perimetro è il dominio logico dove si applicano le regole di fiducia e controllo: definisce dove si esercita la sicurezza.
- La superficie di attacco è l'insieme dei punti potenzialmente sfruttabili: definisce quanto il sistema è esposto.
- L'hardening riduce le esposizioni e rafforza il perimetro.
- Il modello Zero Trust trasforma il perimetro in un insieme di regole dinamiche basate su identità e contesto.

Sintesi concettuale

Il perimetro moderno è mobile e segue identità e contesto.

La superficie di attacco è distribuita e cresce con la complessità dei sistemi.

L'hardening riduce la superficie, la governance delle identità definisce micro-perimetri.

La sicurezza effettiva si basa su autenticazione continua, monitoraggio comportamentale e valutazione del rischio.

Esempio applicativo

In un ateneo che utilizza infrastrutture cloud:

- studenti e docenti accedono ai servizi SaaS tramite SPID o eIDAS;
- le risorse sono distribuite tra data center interni e cloud pubblici;
- le policy IAM definiscono gli accessi in base a identità, dispositivo e contesto.

Il perimetro non è più la rete interna, ma l'insieme delle regole logiche che accompagnano ogni identità digitale.

Glossario sintetico

Perimetro – confine logico dove si applicano le politiche di fiducia e controllo.

Superficie di attacco – insieme dei punti sfruttabili da un attaccante.

Zero Trust Architecture – modello basato su verifica continua di identità e contesto.

Identità digitale – attributi e credenziali che definiscono un soggetto informatico.

Contesto di accesso – condizioni (tempo, luogo, dispositivo, rischio) che determinano l'autorizzazione.

Micro-perimetro – confine logico applicato a una singola identità o risorsa.

Hardening – processo di riduzione della superficie di attacco e rafforzamento dei controlli.