LEZIONE 5 – ANALISI E VALUTAZIONE DEL RISCHIO INFORMATICO

1. SCENARIO E IL CASO AUTENTICAZIONE IDENTITÀ DIGITALE

La sicurezza informatica moderna non si fonda solo su tecniche difensive, ma su un principio analitico: **il rischio non si elimina, si misura e si governa**.
La ***valutazione del rischio informatico*** (***Cyber Risk Assessment***) è il processo sistematico con cui un'organizzazione identifica, stima e gestisce le minacce che possono compromettere i propri asset digitali.

Definizione

Il rischio informatico è la probabilità che una minaccia sfrutti una vulnerabilità producendo un impatto negativo sui principi di riservatezza, integrità o disponibilità (CIA).

Ogni misura di sicurezza deve quindi essere proporzionata al **rischio residuo**. Ora tratteremo come caso specifico il problema del rischio di furto di identità o di compromissione del processo di autenticazione. Tema al centro dei problemi sicurezza dei sistemi digitali

Autenticazione

SICUREZZA DEL PROCESSO DI AUTENTICAZIONE E FRAGILITÀ DEI MECCANISMI DI RECOVERY

1. INTRODUZIONE

La sicurezza del processo di autenticazione rappresenta uno dei cardini fondamentali nella protezione dei sistemi informatici e delle identità digitali. In un contesto caratterizzato da un'elevata interconnessione di servizi, l'autenticazione non può più essere ridotta alla semplice verifica di una password, ma deve essere interpretata come un insieme articolato di procedure, strumenti e prove che garantiscono il legame certo tra un soggetto e un'identità digitale.

Altrettanto rilevante è il processo di **recovery**, ossia il meccanismo di recupero dell'accesso in caso di perdita dei fattori di autenticazione

principali. Proprio questa componente, spesso sottovalutata, rivela le maggiori fragilità dei sistemi moderni, poiché introduce canali di identificazione alternativi – email, numeri di telefono o procedure di helpdesk – che frequentemente risultano meno sicuri dei canali di autenticazione primaria.

---

2. Identificazione e autenticazione: una distinzione concettuale

È opportuno distinguere in modo rigoroso i concetti di **identificazione** e **autenticazione**, spesso utilizzati in modo improprio come sinonimi.

- **Identificazione** è l'atto con cui un soggetto dichiara chi è: si tratta di una fase dichiarativa, nella quale un utente fornisce un identificatore (nome utente, codice fiscale, indirizzo email) che consente al sistema di individuare una specifica identità registrata.
- **Autenticazione**, invece, è il processo attraverso il quale il soggetto dimostra di essere effettivamente colui che dichiara di essere. Essa si basa su prove di conoscenza, possesso o inerenza: qualcosa che l'utente **sa** (password, PIN), **ha** (token, dispositivo, chiave crittografica) o **è** (biometria, impronta digitale, riconoscimento facciale).

L'identificazione, pertanto, stabilisce una corrispondenza nominale, mentre l'autenticazione stabilisce una **relazione di fiducia verificata**. Solo quest'ultima consente di attivare la successiva fase di **autorizzazione**, cioè la concessione dei privilegi e delle operazioni consentite all'utente autenticato.

---

3. La natura composita del processo di autenticazione

Il processo di autenticazione moderna non può essere inteso come un singolo atto, ma come una **catena di prove** che collettivamente forniscono una garanzia di identità.
L'impiego di **fattori multipli e indipendenti** (multi-factor authentication,

MFA) è oggi la pratica raccomandata per aumentare la robustezza del processo.

Le tre categorie classiche di fattori sono:

1. **Conoscenza** (password, PIN, risposta segreta) – facilmente vulnerabile a phishing, furti di credenziali e riuso in più servizi.
2. **Possesso** (smartcard, chiavi hardware, dispositivi mobili) – soggetto a furti fisici, compromissione del dispositivo, clonazione SIM.
3. **Inerenza** (biometria) – robusta ma non revocabile, vulnerabile a falsificazioni sofisticate o a errori di riconoscimento.

Un sistema di autenticazione realmente sicuro richiede la combinazione di fattori eterogenei e la protezione contro il **phishing** e l'**intercettazione del canale**. In tale direzione si muovono gli standard più recenti, come **FIDO2/WebAuthn**, che basano la sicurezza sull'autenticazione crittografica e sulla verifica della presenza fisica dell'utente.

---

4. Meccanismi di recovery e fragilità strutturali

I meccanismi di **recupero dell'accesso** sono concepiti per garantire la continuità del servizio in caso di perdita delle credenziali primarie. Tuttavia, se non progettati con pari rigore rispetto al processo di autenticazione, essi diventano il **punto di ingresso privilegiato** per gli attaccanti.

4.1 L'email come vettore di recovery

L'indirizzo di posta elettronica è spesso considerato la "radice" dell'identità digitale, poiché consente il reset della password in numerosi servizi. Tuttavia, questo approccio presenta criticità profonde:

- la compromissione della casella di posta permette di **reimpostare password** in modo massivo su tutti i servizi collegati;
- la **riassegnazione o il riuso di domini** aziendali o personali può consentire accessi non autorizzati a posteriori;
- regole di **inoltro automatico** o accessi OAuth concessi a terzi possono mantenere l'attaccante in posizione privilegiata anche dopo la bonifica dell'account.

4.2 Il numero di telefono come fattore di recupero

L'uso del numero di telefono per la ricezione di codici via SMS o chiamate automatiche presenta vulnerabilità altrettanto rilevanti:

- rischio di **SIM swap** o **port-out fraud**, mediante ingegneria sociale presso l'operatore telefonico;
- intercettazione del traffico **SS7** o compromissione della rete mobile;
- **riciclo dei numeri** dismessi, che può condurre alla ricezione di codici da parte di soggetti estranei;
- multi-dispositivo non controllato (tablet, smartwatch) che amplifica la superficie d'attacco.

4.3 Catene di identificazione alternative

Le procedure di recovery attivano spesso **catene di identificazione diverse** rispetto al login standard: link via email, OTP via SMS, domande segrete o riconoscimento facciale da remoto.
Tali catene, se più deboli, **annullano la robustezza complessiva** dell'autenticazione primaria, poiché offrono un percorso semplificato di compromissione.

---

5. Analisi dei vettori di attacco nei flussi di recovery

Diversi casi concreti mostrano come l'attaccante possa sfruttare il processo di recupero:

- **Compromissione dell'email principale**: consente reset in cascata su decine di servizi.
- **SIM swap**: il trasferimento fraudolento della linea su una nuova SIM permette di intercettare OTP.
- **Social engineering su helpdesk**: sfrutta procedure di verifica basate su dati statici (data di nascita, indirizzo) facilmente reperibili.
- **Federazioni deboli**: l'autenticazione tramite provider esterni (social login, IdP) con recovery non sicuro trasferisce la vulnerabilità a tutti i servizi federati.
- **Reimpiego di numeri o email**: in mancanza di procedure di revoca, nuovi titolari possono ricevere credenziali di reset.

Tali vettori mostrano come la sicurezza di un sistema di autenticazione non possa essere valutata isolatamente, ma debba considerare l'intera **catena di fiducia** che include anche il processo di recupero.

6. Progettare un recovery robusto

Un principio cardine, riconosciuto anche nelle linee guida internazionali, stabilisce che il **livello di garanzia del recovery** (Level of Assurance, LoA) non debba essere inferiore a quello dell'autenticazione primaria.

Le soluzioni progettuali più efficaci includono:

- **Registrazione multipla di fattori indipendenti**, ad esempio due chiavi FIDO2 o una passkey e un token hardware.
- **Codici di recupero monouso** generati in fase di onboarding, da conservare offline.
- **Verifica assistita ad alto livello di garanzia**, come identificazione video con liveness detection o validazione tramite soggetti qualificati.
- **Cooling-off period**: ritardo deliberato nell'attivazione di un nuovo fattore, con notifica multi-canale all'utente.
- **Notifica, non concessione, via email o SMS**: l'indirizzo o il numero devono servire solo per avvisare, non per autorizzare.
- **Eliminazione delle domande segrete** (knowledge-based authentication), considerate un anti-pattern per la sicurezza.

---

7. Implicazioni normative e di conformità

La sicurezza dell'autenticazione e del recovery è oggi al centro di diversi riferimenti regolatori:

- **PSD2 / SCA (Strong Customer Authentication)** richiede l'uso di almeno due fattori indipendenti e scoraggia l'impiego di canali di recovery più deboli rispetto alla procedura primaria.
- **eIDAS 2.0** introduce livelli di garanzia dell'identità digitale (low, substantial, high) e richiede coerenza tra autenticazione e processi di riemissione o recupero.

- **NIS2** estende la responsabilità dei gestori di servizi essenziali e impone la protezione dei processi organizzativi di supporto, inclusi helpdesk e identity management.

L'insieme di queste norme converge verso una visione unitaria: la **fiducia digitale** deve fondarsi su catene di autenticazione verificabili, tracciabili e resistenti anche nei punti meno visibili del processo.

---

8. Considerazioni conclusive

La sicurezza dell'autenticazione non può essere separata dalla sicurezza della sua recovery. Un sistema è tanto sicuro quanto il suo punto più debole, e il meccanismo di recupero – se progettato in modo superficiale – rappresenta spesso proprio tale anello debole.

Il superamento del paradigma "password + email di recupero" è ormai un'esigenza strutturale. La tendenza contemporanea va verso soluzioni di autenticazione crittografica (FIDO2, passkey) e verso un approccio in cui il recupero sia trattato come un **processo di autenticazione di pari livello**, non come una scorciatoia funzionale.

La maturità di un ecosistema digitale si misura, oggi, nella capacità di mantenere **continuità di fiducia** anche quando l'utente ha smarrito le proprie credenziali. Solo una visione integrata – che comprenda identificazione, autenticazione, recovery e governance della fiducia – può garantire la sicurezza effettiva dei sistemi e la tutela dell'identità digitale nel lungo periodo.

Linee Guida Operative per l'Analisi del Perimetro e della Superficie di Attacco

Fornire al valutatore una procedura standard per:

1. identificare i contesti che costituiscono il **perimetro** dell'organizzazione;
2. mappare la **superficie di attacco** fisica, di rete, logica, applicativa e umana;

3. raccogliere evidenze e anomalie;
4. classificare le vulnerabilità;
5. definire le relative **attività di mitigazione** in un formato riproducibile.

2. Risk Assessment, complessità del rischio e Grafo dei contesti

Per comprendere la complessità del processo di valutazione del rischio di un'organizzazione anche di dimensioni non rilevanti di seguito presentiamo uno schema di metodologia di assesment che rappresenta un esempio realistico di quanto normalmente gli esperti di cyber security realizzano nella loro analisi. Inoltre, al termine di questa presentazione farò vedere come si possa tradurre quanto appreso dalla fase di assesment in un grafo dei contesti(Identità e sorgenti informative) e dei flussi informativi così come abbiamo delineato nelle lezioni precedenti. La struttura combinatorio del grafo renderà evidente la complessità intrinseca di un processo reale di valutazione del rischio.

2.1. Fase 1 – Raccolta preliminare delle informazioni

Il valutatore deve ottenere:

Documentazione tecnica

1. Diagrammi infrastrutturali (fisici e logici)
2. Elenco asset (HW, SW, Cloud, identità, microservizi)
3. Configurazioni sicurezza rilevanti
4. Boundaries amministrativi (tenant, subscription, domini, segmentazioni)
5. Processi IT e sicurezza (IAM, patching, change, incident, backup)

Interlocutori

1. Responsabile sicurezza
2. IT operations
3. DevOps / sviluppatori
4. HR per la parte di identità e onboarding/offboarding
5. Fornitori esterni coinvolti nei flussi critici

Output della fase

1. Matrice stakeholder
2. Lista asset iniziale (baseline)
3. Scope dell'assessment

2.2. Fase 2 – Analisi del Perimetro

Suddivisa secondo i tre livelli del modello:

2.2.1. Perimetro fisico e infrastrutturale

Checklist:

1. Controlli accesso fisico multilivello (badge, biometria, escorting)
2. Log accessi e retention
3. Protezione rack e sale apparati
4. Stato percorsi cavi e protezioni anti-tapping
5. Segmentazione impianti (LAN, WAN, DMZ)
6. Continuità energetica (UPS, gruppi)
7. Hardening apparati di rete

Evidenze da raccogliere:

1. Planimetrie
2. Foto (se consentito)
3. Log accessi
4. Configurazioni switch/firewall

2.2.2. Perimetro logico e di gestione

Checklist:

1. Identità → struttura IAM/IdP
2. MFA e accesso condizionale
3. Privilegi elevati (PIM/JIT)
4. Segreti (vault, rotazione, gestione chiavi)
5. Trust e federazioni
6. Policy e segmentazione logica (tenant, RG, tag, RBAC)

Evidenze da raccogliere:

1. Policy IAM
2. Ruoli assegnati
3. Token lifetime
4. Configurazioni conditional access

2.2.3. Perimetro applicativo e dei servizi

Checklist:

1. Mappa API e endpoint
2. Microservizi e loro interazioni (Est–Ovest)
3. Gateway/API Management
4. SBOM e dipendenze
5. Pipeline CI/CD + controlli SAST/SCA/DAST
6. Identità di workload (mTLS, workload identity)
7. Configurazioni PaaS/SaaS

Evidenze da raccogliere:

1. API contract
2. Log applicativi
3. Posture cloud (es: Defender/ASC)
4. Configurazioni container/cluster

2.3. Fase 3 – Analisi della Superficie di Attacco 2.3.1. Superficie Fisica

1. Data center e locali tecnici
2. Possibili accessi non autorizzati
3. Debolezze nella supply chain hardware
4. Punti di tapping rete

Strumenti: sopralluogo fisico, walkthrough tecnici. **2.3.2. Superficie di Rete**

1. Censimento indirizzi IP pubblici
2. DNS footprinting
3. Servizi esposti (API, web app, tunnel)
4. Hardening TLS/cipher suite
5. Configurazioni firewall / NSG / ACL
6. Collegamenti esterni (VPN, peering)

Strumenti: scanning passivo, OSINT, configurazioni. **2.3.3. Superficie Logica**

1. Identità ad alto privilegio
2. Policy di accesso
3. Gestione dei token
4. Escalation di privilegi possibile
5. Federazioni e trust rischiosi

Strumenti: analisi IAM, log di identità, audit roles. **2.3.4. Superficie Applicativa**

1. Codice e input esposti
2. SQL/Command Injection
3. Deserializzazione insicura
4. Container breakout
5. API non protette
6. Supply chain del software

2.3.5. Superficie Umana

1. Processi non formalizzati
2. Password riutilizzate
3. Shadow IT
4. Manutentori e fornitori terzi
5. Maturità formazione sicurezza
6. Phishing e ingegneria sociale

2.4. Fase 4 – Identificazione e Classificazione delle Vulnerabilità

Il valutatore assegna a ciascuna vulnerabilità:

1. **Categoria:** fisica / rete / logica / applicativa / umana
2. **Descrizione:** breve e puntuale
3. **Evidenza:** dato osservabile (log, screenshot, output tecnico)
4. **Rischio:** basso / medio / alto / critico
5. **Impatto potenziale:** integrità / disponibilità / riservatezza / reputazione
6. **Probabilità:** bassa / media / alta
7. **Priorità di intervento:** immediata / breve termine / medio termine

Metodo consigliato: **Risk = Impatto × Probabilità** (coerente con NIST 800-30 / 800-37 / ISO 27005)

2.5. Fase 5 – Attività di Mitigazione

Ogni vulnerabilità deve avere almeno:

1. una misura tecnica (T):
i. es. attivare MFA resistente al phishing

2. una misura organizzativa (O):
i. es. ridefinire ruoli e privilegi

3. una misura procedurale (P):
i. es. aggiornare la procedura di onboarding

3. Tabella Finale – Vulnerabilità e Mitigazioni

Esempio di modello standard da includere nel deliverable.

3.1. Tabella delle vulnerabilità rilevate

ID Categoria

1. v1 Rete
2. v2 Logica
3. v3 Applicativa
4. v4 Fisica
5. v5 Umana

Vulnerabilità

API esposta senza TLS moderno

Privilegio eccessivo su account di servizio SQL Injection su endpoint /search

Rack non protetto

MFA non attivo per 32 utenti

Evidenza Impatto Probabilità Livello di rischio

Priorità

Immediata

Immediata

Breve termine

Immediata

ID Vulnerabilità

Tipo (T/O/P)

Descrizione dell’azione

Priorità Responsabile

Mitigazione

M-01 v1 M-02 v2 M-03 v3

M-04 v5 M-05 v4

associata

Report TLS Alto IAM dump Critico Test DAST Alto Sopralluogo Medio Audit M365 Alto

Media Alta Alta Media Alta

Alto Critico Critico Medio Critico

3.2. Tabella delle attività di mitigazione

T Applicare TLS 1.2+ e disattivare Alta IT Security cipher deboli

O Revisione ruoli e rimozione Alta IAM/HR privilegi eccessivi

T Sanitizzazione input + Alta DevOps parametrizzazione query

Policy che impone MFA per
P tutti; comunicazione e Alta CISO

enforcement
Fisica Installazione serrature e Media Facility

controllo accessi su rack

4. Architettura orientata ai flussi operativi e

grafo dei contesti

Per rappresentare un'architettura che metta in risalto i flussi operativi, si adotta un grafo diretto in cui ogni nodo è un **contesto minimo**: un dominio omogeneo di protezione accessibile con una sola credenziale o identità (umana o di workload), e nel quale le policy di accesso sono coerenti e indivise.

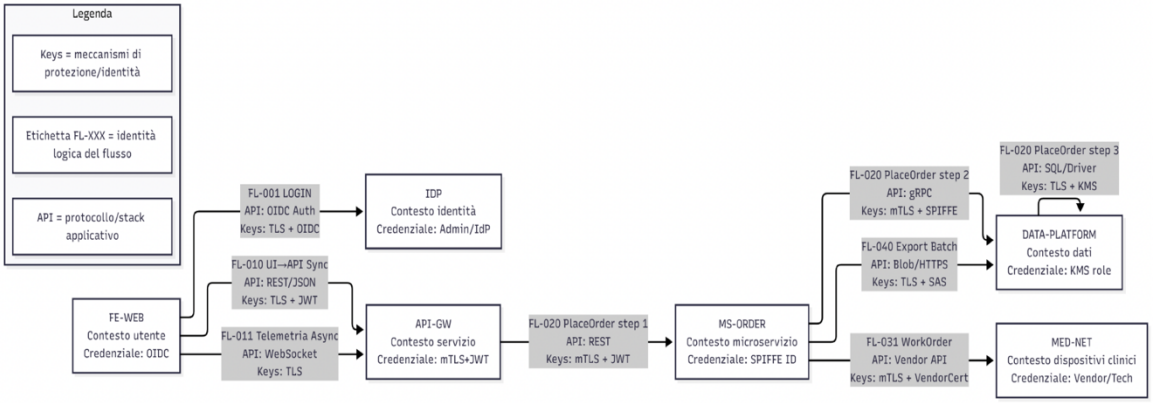
L'arco tra due nodi rappresenta un **flusso informativo end-to-end** ed è **etichettato in modo univoco** con un identificatore del flusso (es. FL-XXX), il **tipo di API/protocollo** attraversato (REST, gRPC, HL7, DICOM, MQ, file drop) e la **classe di chiavi o meccanismi crittografici** che proteggono e identificano il flusso (TLS/mTLS, OIDC/JWT, API-Key, client cert, HMAC, KMS envelope).

Tra due nodi possono esistere **più archi paralleli**, ciascuno corrispondente a una diversa classe di flusso (ad esempio lettura sincrona vs esportazione batch, telemetria vs comandi).

Quando una **singola transazione** percorre più nodi consecutivi (per esempio front-end → API → microservizio → data platform), **mantiene la stessa etichetta di flusso** lungo l'intero tragitto, così da preservarne l'identità logica e rendere tracciabili autorizzazioni, cifratura, responsabilità e punti di controllo. La costruzione del grafo segue un ordine semplice ma rigoroso: si individuano i contesti minimi mappando le credenziali effettivamente accettate; si enumerano i flussi reali che

attraversano i confini, assegnando un'etichetta stabile e non riutilizzabile; per ogni arco si annotano protocollo, formato, direzione, frequenza e chiavi/meccanismi di protezione; infine si verifica la coerenza tra le etichette di flusso e i controlli di frontiera, in modo che la stessa transazione mantenga le stesse garanzie di autenticazione, autorizzazione e confidenzialità in ciascun salto.

Il risultato è un **diagramma dei contesti e dei flussi** che privilegia l'identità e il comportamento del dato rispetto alla topologia fisica, facilita l'analisi della superficie di attacco, la definizione dei controlli "choke-point" e la stesura di playbook di difesa e audit end-to-end.



Note pratiche per l'uso del grafo. Le etichette FL-XXX sono stabili e versionate; un cambiamento sostanziale di protocollo o di chiavi produce una nuova etichetta.
Le credenziali riportate nel nodo descrivono **chi** può entrare in quel contesto con privilegi nativi, mentre le chiavi sull'arco descrivono **come** il flusso viene autenticato, autorizzato e cifrato nel passaggio di confine.

Documento di valutazione delle vulnerabilità puntuali e infrastrutturali

Il documento risultante ha l'obiettivo di effettuare una revisione dell'architettura e in particolare del grafo dei contesti per individuare le vulnerabilità infrastrutturali e le vulnerabilità specifiche di punti della superficie di attacco del perimetro.
I punti della superficie di attacco sono tutti gli elementi classificati nei paragrafi [2,3,4].

Ogni punto è valutato rispetto alla sua debolezza intrinseca come vulnerabilità delle credenziali di accesso, mancato aggiornamento del software relativo al punto osservato, carenza formativa del personale addetto a dati sensibili, ecc..

La revisione architetturale dell'infrastruttura riguarda non solo fragilità specifiche in singoli punti ma fragilità legate ai flussi informativi che vengono gestiti dall'architettura.
In altri termini, un flusso informativo che intercetta una fragilità specifica e consente azioni legali per una porzione del perimetro e che permette di raggiungere punti diversi dell'infrastruttura a maggior sensibilità, è da considerare una vulnerabilità infrastrutturale.

La valutazione delle vulnerabilità infrastrutturali viene svolta utilizzando il grafo descritto nel paragrafo precedente.

Il controllo di presenza di vulnerabilità infrastrutturali si effettua verificando che una stessa etichetta FL mantenga requisiti di sicurezza equivalenti in ogni salto e che non esistano attraversamenti "impliciti" privi di arco esplicito.

Ciò va svolto in modo sistematico sull'intero grafo.

5. Output finale dell'assessment

Il valutatore deve produrre:

1. diagramma dei perimetri (fisico / logico / applicativo);
2. diagramma delle superfici di attacco principali;
3. documento delle vulnerabilità infrastrutturali e puntuali;
4. piano di mitigazione con timeline;
5. mappa responsabilità (RACI);
6. stato di conformità rispetto allo standard (NIST 800-207, 800-53, Zero Trust);
7. viene rilasciato dal valutatore il documento certificato al cliente e messo in conservazione presso il valutatore

Conclusione un grafo con K nodi e m archi può richiedere la verifica di un numero di cammini esponenziale in questi termini.