# Esercitazione svolta: definire il perimetro e la superficie di attacco di un semplice sistema digitale

**testi di riferimento aggiuntivi:**

**-NIST Special Publication 800-207 – Zero Trust Architecture.**
**-SP 800-53 (controlli di sicurezza) e SP 800-30 (risk assesment.**

## Descrizione generale del sistema

Il sistema e-commerce “trova compra” è una piattaforma online di vendita di prodotti, sviluppata in architettura cloud ibrida. Comprende un front-end web accessibile da browser e app mobile, un application server che espone API REST, un database relazionale gestito in cloud (PostgreSQL su AWS RDS), un gateway di pagamento esterno conforme a PCI-DSS, un servizio di autenticazione federata basato su OpenID Connect/OAuth2 e un modulo di amministrazione accessibile tramite VPN con autenticazione a due fattori.

—

## Componenti logiche principali

Zona pubblica (front-end): espone le interfacce di catalogo, ricerca e login, accessibili da Internet tramite HTTPS.
Zona applicativa (application layer): contiene la logica di business, la gestione ordini e l’autenticazione utenti; comunica solo via API con la zona dati.
Zona dati (database e storage): contiene dati personali e transazionali, non accessibile direttamente da Internet.
Servizi esterni integrati: gateway di pagamento, notifiche, sistemi di analytics, accessibili tramite token temporanei e autenticazione mutuale TLS.

—

3. Classificazione del perimetro secondo il NIST SP 800-207

Nel modello Zero Trust, il perimetro non è una barriera di rete, ma una funzione logica di controllo dell'identità e del contesto di accesso.
L'architettura è segmentata in micro-perimetri, ciascuno con policy dedicate.

Perimetri logici identificati:
• Perimetro utente: autenticazione tramite Identity Provider (IdP) con token OAuth2 e MFA.
• Perimetro API: verifica del contesto di accesso (origine, token, tempo di sessione, ruolo).
• Perimetro amministrativo: accesso consentito solo da VPN con MFA e controllo continuo dell'identità.
• Perimetro dati: accesso consentito solo ai servizi applicativi autorizzati secondo il principio del "least privilege".

Ogni accesso è verificato dinamicamente da un Policy Enforcement Point (PEP), secondo le regole definite nel Policy Decision Point (PDP), come previsto dal framework NIST SP 800-207.

**Analisi della superficie di attacco**

La superficie di attacco rappresenta l'insieme dei punti attraverso i quali un attaccante può interagire con il sistema.

Superficie di rete: include le porte HTTPS del front-end e delle API e gli endpoint VPN per accesso amministrativo. I rischi principali sono attacchi DDoS, scansioni e sfruttamento di vulnerabilità TLS.

Superficie applicativa: comprende i form di login, i moduli di registrazione e gli endpoint API REST. I rischi includono SQL injection, XSS e session hijacking.

Superficie logica: riguarda i token OAuth2, la gestione delle sessioni e dei ruoli. I rischi sono replay di token, escalation di privilegi e configurazioni errate.

Superficie dati: concerne il database accessibile solo tramite API. Il rischio principale è l'esposizione di dati sensibili tramite query o log non cifrati.

Superficie umana: include credenziali deboli, phishing e errori operativi. Il rischio è la compromissione dell'account amministratore o sviluppatore.

—

**Misure di hardening per ridurre la superficie di attacco**

Front-end: utilizzo di Web Application Firewall (WAF) e Content Security Policy; aggiornamento automatico delle librerie JavaScript.
Application layer: validazione input, logging strutturato e separato, rate limiting sugli endpoint API.
Database: accesso solo tramite rete privata, cifratura a riposo (AES-256) e in transito (TLS 1.3).
Gestione identità: autenticazione multifattore e token con scadenza breve.
Amministrazione: VPN segmentata, audit continuo e registro accessi firmato digitalmente.

**Rischi residui e controlli NIST correlati**

Accesso non autorizzato: mitigato da controlli NIST AC-2, AC-3, AC-17 e IA-2, con implementazione di MFA, policy di sessione e audit accessi.

Manipolazione dei dati: mitigata da controlli NIST SC-8 e SC-13, mediante cifratura TLS e AES e funzioni di hashing.

Attacchi web applicativi: mitigati da controlli NIST SI-10 e RA-5, con validazione input, WAF e test periodici di vulnerabilità.

Violazione dell'identità amministrativa: mitigata da controlli IA-5 e AC-6, con segregazione dei ruoli e logging continuo.

Interruzione del servizio: mitigata da controlli CP-10 e SI-4, con backup, monitoraggio e alert automatici.

**Sintesi finale**

Il perimetro dell'e-commerce è distribuito: ogni livello (utente, API, dati, amministrazione) costituisce un micro-perimetro regolato da policy dinamiche di accesso.
La superficie di attacco è gestita mediante misure multilivello di hardening, autenticazione forte e monitoraggio continuo.
L'architettura è coerente con i principi del NIST SP 800-207 (Zero Trust) e del NIST SP 800-53, in particolare per autenticazione continua, cifratura, logging e applicazione del principio del "least privilege".
Il sistema si fonda sul monitoraggio continuo (ISCM) e sulla riduzione progressiva della superficie di esposizione, in linea con il framework di gestione del rischio NIST SP 800-37 Rev.2.

# VALUTAZIONE ARCHITETTURA ZERO TRUST

## GLOSSARIO DEI TERMINI E DEFINIZIONI

**Access Control:** Processo mediante il quale si regola chi può accedere a una risorsa informatica, con quali privilegi e in quali condizioni.

**Active Directory (AD):** Directory service che gestisce identità, gruppi, criteri di sicurezza e risorse di rete.

**Asset:** Qualsiasi componente del sistema informativo che ha valore per l'organizzazione e deve essere protetto.

**CASB:** Cloud Access Security Broker, controlla l'accesso ai servizi cloud applicando policy di sicurezza.

**CSPM:** Cloud Security Posture Management, verifica la sicurezza delle configurazioni cloud.

**Conditional Access:** Accesso basato su condizioni contestuali come posizione, rischio e dispositivo.

**DLP:** Data Loss Prevention, impedisce la perdita o l'esfiltrazione di dati sensibili.

**EDR:** Endpoint Detection and Response, monitora e risponde a minacce sugli endpoint.

**IdP:** Identity Provider, sistema che autentica gli utenti e rilascia token di accesso.

**Least Privilege:** Ogni utente o processo dispone solo dei privilegi strettamente necessari.

**Micro-segmentazione:** Divisione della rete in segmenti isolati per ridurre il rischio di movimenti laterali.

**MFA:** Multi-Factor Authentication, usa più fattori per autenticare l'utente.

**NAC:** Network Access Control, controlla chi può accedere alla rete in base alla conformità del dispositivo.

**NDR:** Network Detection and Response, rileva attività sospette nella rete.

**PAM:** Privileged Access Management, gestisce gli account amministrativi e privilegiati.

**Policy Engine:** Componente logico che valuta le richieste di accesso in base a regole e contesto.

**Policy Enforcement Point:** Elemento che applica le decisioni del Policy Engine.

**SASE:** Secure Access Service Edge, integra funzioni di sicurezza e rete erogate come servizio cloud.

**SIEM:** Security Information and Event Management, raccoglie e correla log di sicurezza.

**SOAR:** Security Orchestration Automation and Response, automatizza le risposte agli incidenti.

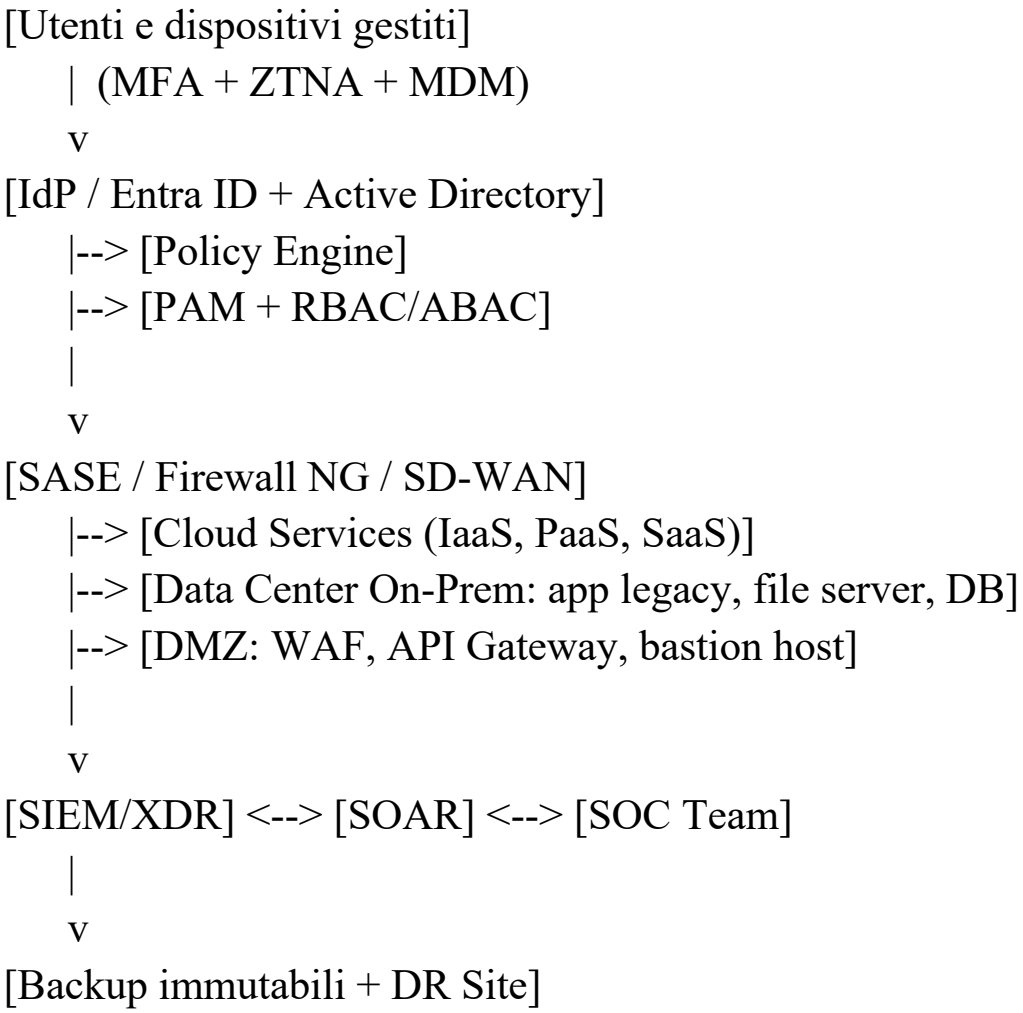
**ZTNA:** Zero Trust Network Access, accesso controllato alle applicazioni basato su identità e contesto.

**Zero Trust:** Modello che elimina la fiducia implicita nella rete e verifica continuamente identità e dispositivi.

**Zero Trust Architecture (ZTA):** Insieme di principi e componenti che applicano il modello Zero Trust all'intera infrastruttura.

## ARCHITETTURA DI UNA MEDIA ORGANIZZAZIONE

L’architettura proposta rappresenta un’infrastruttura ibrida (on-premise e cloud) per una media organizzazione, con gestione centralizzata delle identità, segmentazione della rete e applicazione dei principi Zero Trust.




## VALUTAZIONE SECONDO NIST SP 800-207 (ZERO TRUST ARCHITECTURE)

**1. Tutte le risorse sono considerate potenzialmente non affidabili:** Asset inventory, autenticazione forte e micro-segmentazione implementate. Maturità: Buono.

**2. Tutte le comunicazioni sono protette:** Cifratura TLS/mTLS e segmentazione rete. Da estendere a traffico interno. Maturità: Buono.

**3. Accesso per sessione:** Conditional Access per ogni accesso, enforcement parziale su app legacy. Maturità: Medio.

**4. Policy dinamiche basate sul contesto:** Accesso basato su rischio e postura dispositivo. Maturità: Avanzato.

**5. Monitoraggio continuo dell'integrità:** SIEM/XDR e vulnerability management attivi. Maturità: Buono.

**6. Autenticazioni e autorizzazioni dinamiche:** MFA, PAM e RBAC/ABAC implementati. Maturità: Avanzato.

**7. Raccolta e uso dei dati per miglioramento continuo:** Telemetria correlata e analisi centralizzata. Maturità: Buono.

### SINTESI E RACCOMANDAZIONI

L'architettura è allineata ai principi NIST SP 800-207 con forte controllo su identità, accesso e telemetria. Il livello di maturità complessivo è valutato come intermedio-avanzato. Si raccomanda di:

• Estendere la cifratura mTLS anche al traffico interno.

• Applicare policy dinamiche granulari anche alle app legacy.

• Integrare analytics predittive basate su AI/ML per migliorare detection e risposta.

• Aumentare la copertura di sicurezza per IoT/OT e fornitori esterni

Quello che osserviamo è che non sono tenute presenti in modo ben definite le procedure organizzative dell'organizzazione, i ruoli e le responsabilità. L'Europa ha provato a rispondere a questa mancanza

## NORMATIVE E REGOLAMENTAZIONI

### EVOLUZIONE NORMATIVA E IMPATTO

Le principali normative che influenzano la gestione dell'identità nei sistemi distribuiti:

- **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.

**Nota operativa**
Un sistema federato conforme a eIDAS 2 deve garantire livelli AAL2 o AAL3, logging sicuro e interoperabilità tra fornitori.

## Modulo di Analisi NIS2 per sistemi e-commerce

Questo modulo consente di valutare la conformità di un sistema digitale ai requisiti della Direttiva NIS2, integrando i principi del framework NIST (SP 800-207, SP 800-30, SP 800-53). Il documento guida un tecnico nell'analisi delle vulnerabilità, nella raccolta di evidenze e nell'individuazione delle misure correttive (remediation).

Glossario dei termini tecnici

- MFA (Multi-Factor Authentication): Autenticazione a più fattori: metodo di sicurezza che richiede più di un elemento di verifica per accedere a un sistema (es. password + codice SMS + token).

- WAF (Web Application Firewall): Firewall per applicazioni web: filtra e monitora il traffico HTTP verso le applicazioni web per prevenire attacchi come SQL injection o XSS.
- SIEM (Security Information and Event Management): Sistema centralizzato per la raccolta, correlazione e analisi dei log di sicurezza, utile per individuare comportamenti anomali.
- IAM (Identity and Access Management): Gestione delle identità e degli accessi: insieme di processi e tecnologie per gestire in modo sicuro le credenziali e i ruoli degli utenti.
- VPN (Virtual Private Network): Rete privata virtuale: canale cifrato che consente una connessione sicura tra un utente remoto e la rete aziendale.
- TLS (Transport Layer Security): Protocollo crittografico che protegge la trasmissione dei dati su Internet (es. HTTPS).
- Zero Trust: Modello di sicurezza che non presume la fiducia automatica di alcun utente o dispositivo, ma verifica ogni accesso in base al contesto e all'identità.
- Least Privilege: Principio di sicurezza che prevede di assegnare agli utenti solo i privilegi strettamente necessari per svolgere le loro funzioni.
- Phishing: Tecnica di inganno tramite email o messaggi che mirano a ottenere informazioni riservate (es. credenziali, dati bancari).
- Incident Response Plan (IRP): Piano che definisce le procedure e i ruoli da seguire in caso di incidente di sicurezza informatica.

Sezione 1 – Governance e Risk Management

Domanda di verifica Evidenza richiesta Remediation (azione correttiva)

È definito un Responsabile della sicurezza ICT (CISO)? Nomina o organigramma Definire ruoli e responsabilità in documento ufficiale.

Esiste un registro dei rischi aggiornato? Risk register o foglio Excel Adottare modello NIST 800-30 con valutazione rischio × impatto.

Le politiche di sicurezza sono approvate dal management? Policy firmate o pubblicate Formalizzare approvazione periodica.

Sezione 2 – Asset & Supply Chain

Domanda di verifica Evidenza richiesta Remediation (azione correttiva)

Esiste un inventario degli asset (hardware, software, dati)? Database o elenco aggiornato Creare inventario centralizzato (CMDB).

I fornitori critici sono valutati periodicamente? Audit o checklist Inserire SLA di sicurezza e obbligo di notifica incidenti.

Le dipendenze cloud (AWS, OAuth2, gateway PCI-DSS) sono monitorate? Contratti, log, controlli Verificare certificazioni e continuità del servizio.

Sezione 3 – Controlli Tecnici e Architetturali

Domanda di verifica Evidenza richiesta Remediation (azione correttiva)

L’autenticazione MFA è attiva per tutti gli accessi sensibili? Configurazioni IAM Estendere MFA anche agli utenti privilegiati e sviluppatori.

Sono presenti test periodici di vulnerabilità o penetration test? Report trimestrali Pianificare test RA-5 e SI-10 annuali.

I log sono firmati digitalmente e centralizzati (SIEM)? Configurazione o tool Integrare SIEM con alert automatici e report NIS2.

Sezione 4 – Incident Response e Business Continuity

Domanda di verifica Evidenza richiesta Remediation (azione correttiva)

Esiste un piano di risposta agli incidenti (IRP)? Procedura scritta Redigere piano con ruoli, tempi e comunicazioni.

Sono previste prove di continuità operativa?Verbali di test Simulare failover e recovery almeno annualmente.

È predisposta una notifica incidenti entro 24 ore come previsto da NIS2? Template o protocollo Creare protocollo interno con escalation immediata.

Sezione 5 – Crittografia e Protezione Dati

Domanda di verifica Evidenza richiesta Remediation (azione correttiva)

I dati sensibili sono cifrati in transito e a riposo? Configurazioni TLS e database Verificare cifratura AES-256 e rotazione chiavi.

I privilegi sono assegnati secondo il principio del least privilege? IAM policies Riesaminare i ruoli utente secondo Zero Trust.

Sono definite policy di scadenza password e timeout sessione? Configurazioni di sistema Impostare regole di rotazione e revoca token.

Sezione 6 – Formazione e Cultura della Sicurezza

Domanda di verifica Evidenza richiesta Remediation (azione correttiva)

Sono previsti corsi periodici di awareness per il personale? Calendario corsi Implementare programma formativo NIS2.

Sono simulate campagne di phishing o social engineering? Report simulazioni Eseguire test periodici di sensibilizzazione.

È definita una policy per accesso remoto sicuro? Policy interna

Aggiornare policy con requisiti MFA e VPN segmentata.

La soluzione Nis2 risponde alle esigenze di formalizzare meglio le procedure associate alla gestione della cybersecurity in un'organizzazione. Il prezzo è maggiore rigidità e burocrazia.

## CONCLUSIONI

Non esiste il 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).

Michael E. Whitman, Herbert J. Mattord – *Principles of Information Security*

7ª edizione, Cengage Learning, 2023. ISBN 978-0-357-68523-4.