AGENZIA WEB MONZA / GUIDA 02

Sicurezza del negozio online

Protezione dell’area clienti, gestione degli accessi, download digitali e sicurezza delle comunicazioni.

Documento informativo e commerciale · Ottobre 2026

Non costituisce un preventivo né un documento contrattuale.

01 Perché la sicurezza di un e-commerce è diversa

Un e-commerce dispone normalmente di account clienti, carrelli, pagamenti, informazioni sugli ordini e accessi amministrativi. In alcuni casi distribuisce file digitali. Ogni funzione aggiunge dati, autorizzazioni e possibili rischi da gestire.

La sicurezza deve essere definita in fase di progettazione, tenendo conto delle informazioni raccolte, delle persone che possono consultarle e delle funzioni esposte online.

Nessuna misura singola rende un negozio online invulnerabile: la protezione dipende dall’intero sistema e dalla sua gestione.

02 HTTPS, cifratura e pagamenti

HTTPS con TLS protegge la comunicazione fra browser e sito durante il trasferimento. Non cifra automaticamente ogni dato memorizzato nel database e non impedisce, da solo, accessi abusivi all’applicazione.

Per i pagamenti si prediligono fornitori specializzati e integrazioni che riducano l’esposizione diretta dei dati delle carte. I requisiti applicabili dipendono dalla soluzione di pagamento scelta.

03 Account clienti, password e sessioni

L’accesso personale richiede gestione prudente delle credenziali: password archiviate con algoritmi di hashing adeguati, protezioni contro tentativi ripetuti, recupero sicuro dell’account e sessioni controllate.

L’autenticazione a due fattori può essere utile soprattutto per amministratori e, dove previsto, anche per i clienti. La sua disponibilità dipende dalle esigenze e dall’architettura concordata.

04 Autenticazione non significa autorizzazione

Un utente può essere correttamente autenticato e cercare comunque di consultare l’ordine di un altro cliente. Per questo ogni richiesta deve essere verificata anche rispetto alle autorizzazioni: proprietà di ordini, documenti, indirizzi e operazioni amministrative.

La semplice presenza di una pagina nascosta o di un pulsante non visibile non costituisce protezione sufficiente. I controlli devono essere applicati lato server o nel livello affidabile dell’applicazione.

05 Download digitali: controllo reale dei file

File venduti, manuali riservati e documenti personalizzati non devono essere esposti con URL pubblici prevedibili quando è richiesta una distribuzione protetta. Occorre verificare il diritto di accesso prima di consentire il download.

- Archiviazione privata o controllata, secondo l’infrastruttura.
- Link temporanei o accessi firmati quando appropriati.
- Associazione fra acquisto, cliente e file autorizzato.
- Eventuali limiti di durata, numero di download o licenze.
- Registrazione degli eventi utili a verificare comportamenti anomali, con limiti di conservazione adeguati.

Il download protetto è una funzionalità da progettare e preventivare secondo le esigenze commerciali.

06 Upload, allegati e documenti riservati

Quando il sito accetta file caricati dagli utenti, sono necessari controlli su tipi e dimensioni, permessi di accesso, archiviazione e, dove utile, scansioni o verifiche di sicurezza.

I file privati non devono essere resi consultabili da utenti diversi dal destinatario previsto. Anche la cancellazione e la conservazione devono seguire regole definite.

07 Email, dominio e rischio di impersonificazione

Le email di ordini e accesso devono provenire da mittenti correttamente configurati. SPF, DKIM e DMARC contribuiscono all’autenticazione dei messaggi e alla protezione del dominio contro alcuni abusi.

L’integrazione iniziale Brevo prevista nell’offerta e-commerce consente di utilizzare un canale dedicato per gli invii configurati. Non equivale a una garanzia assoluta di consegna o all’eliminazione del rischio spam.

08 Protezione applicativa e servizi Cloudflare

Servizi come Cloudflare possono aiutare a filtrare richieste malevole e a mitigare alcune forme di attacco al traffico web, secondo piano e configurazione. Non sostituiscono controlli delle autorizzazioni, aggiornamenti del software o protezioni del database.

La scelta delle misure dipende da esposizione, architettura, account privilegiati e caratteristiche del progetto.

09 Aggiornamenti, backup e ripristino

Le dipendenze, i componenti, i plugin e le configurazioni devono essere mantenuti nel tempo. Backup verificabili e procedure di ripristino riducono l’impatto di errori, guasti o incidenti, ma vanno definiti con frequenza e conservazione adeguate.

Il backup non equivale alla continuità operativa e non sostituisce la protezione dell’accesso agli ambienti di produzione.

10 Chi può accedere ai dati dei clienti

Gli accessi amministrativi devono essere attribuiti secondo responsabilità e necessità operative. È opportuno limitare i permessi, revocare quelli inutilizzati e proteggere le credenziali di personale e fornitori.

Nei sistemi con ruoli diversi, il personale addetto agli ordini non deve necessariamente poter modificare configurazioni tecniche o accedere a ogni informazione aziendale.

11 Controlli e responsabilità condivise

L’agenzia progetta e implementa le misure concordate; il titolare dell’attività gestisce le responsabilità proprie del commercio e dei dati trattati. Hosting, provider di pagamento e altri fornitori hanno obblighi e termini distinti.

Sicurezza significa anche formazione, procedure interne, credenziali ben custodite e gestione dei cambiamenti dopo la consegna.

12 Cosa viene definito per il progetto

In fase di analisi individuiamo dati trattati, funzioni di autenticazione, accessi, necessità di download o upload, servizi terzi e misure coerenti con i rischi. Il preventivo chiarisce i controlli implementati e le eventuali funzioni avanzate.

Agenzia Web Monza — www.agenziawebmonza.it

Documento informativo: non è un audit, una certificazione di sicurezza o una promessa di protezione assoluta.