VERIFICA DELLA SUPERFICIE ESTERNA

esempio-srl.it

Data della verifica	**14 agosto 2026, ore 07:20 UTC**
Periodo coperto	**dal 14 luglio al 14 agosto 2026**
Riferimento scansione	**e5e3b101**

Impronta del report (SHA-256)

`0e5e3b100e5e3b100e5e3b100e5e3b10`
`0e5e3b100e5e3b100e5e3b100e5e3b10`

Questo documento riporta ciò che era osservabile dall'esterno, senza intrusione, sul dominio indicato dal titolare dell'account che ha richiesto la verifica, alla data e all'ora indicate sopra. Non è una certificazione di conformità: le misure organizzative, di governance e di formazione non sono verificabili dall'esterno e restano dell'organizzazione.

DISCLAIMER: This automated report is for informational purposes only. The scan was performed non-intrusively based on public accessibility. Privateer is not liable for undetected vulnerabilities or subsequent breaches. This document contains confidential information intended solely for the recipient.

Data della verifica: 14 agosto 2026 **Asset: e5e3b100**

Esposizione	Porte aperte	Sottodomini
Alta	9	6
2 problemi gravi		

Sintesi per la direzione

La superficie esterna di esempio-srl.it è nel complesso presidiata, con due punti che richiedono un intervento a breve. Il portale clienti accetta ancora connessioni con protocolli obsoleti, e il dominio non ha una politica DMARC attiva: chiunque può inviare posta che sembra provenire dall'azienda senza che il destinatario abbia modo di accorgersene. Sul server di posta è invece già presente la cifratura in transito. Rispetto alla verifica precedente due rilievi risultano risolti e uno nuovo è comparso su un sottodominio pubblicato di recente.

Cosa fare, in ordine di priorità

Priorità	Cosa fare
P1	Pubblicare un record DMARC almeno in quarantena, dopo aver verificato che SPF e DKIM coprano tutti i mittenti legittimi
P2	Disattivare TLS 1.0 e 1.1 sul portale clienti, lasciando attivo TLS 1.2 e 1.3
P3	Chiedere al fornitore che ospita 203.0.113.10 di chiudere la porta 8080, che espone un pannello di amministrazione senza cifratura

Dall'ultima verifica: 1 nuovi, 2 risolti, 18 ancora aperti.

DISCLAIMER: This automated report is for informational purposes only. The scan was performed non-intrusively based on public accessibility. Privateer is not liable for undetected vulnerabilities or subsequent breaches. This document contains confidential information intended solely for the recipient.

Data della verifica: 14 agosto 2026 **Asset: e5e3b100**

Cosa è cambiato dall'ultima scansione

2 risolti · 1 nuovi · 18 ancora aperti

	Problema	Gravità
Risolto	Porta 21 (FTP senza cifratura) raggiungibile da Internet su 203.0.113.10	high
Risolto	Posta — configurazione TLS: cifrari deboli ancora offerti	medium
Nuovo	File di configurazione di uno strumento di sviluppo raggiungibile pubblicamente	medium

Inventario della superficie esterna

I nomi raggiungibili da Internet trovati per questo dominio, con i servizi esposti su ciascuno. E' l'elenco da cui partire per il conferimento di domini e spazio di indirizzamento IP previsto dall'art. 7 del d.lgs. 138/2024. L'elenco completo delle porte aperte, host per host, è nell'allegato tecnico in fondo al documento.

Nome
esempio-srl.it
www.esempio-srl.it
mail.esempio-srl.it
portale.esempio-srl.it
preventivi.esempio-srl.it
vpn.esempio-srl.it

Indirizzi IP e fornitori tecnici

Indirizzo	Rete (prefisso)	Rete di	Cosa risponde
203.0.113.10	203.0.113.0/24	Rete di hosting condiviso (esempio)	Anche nomi di terzi
203.0.113.42	203.0.113.0/24	Rete di distribuzione dei contenuti (esempio)	CDN

DISCLAIMER: This automated report is for informational purposes only. The scan was performed non-intrusively based on public accessibility. Privateer is not liable for undetected vulnerabilities or subsequent breaches. This document contains confidential information intended solely for the recipient.

Data della verifica: 14 agosto 2026 **Asset: e5e3b100**

I rilievi, per gravità

Gravità	Rilievo	Dettaglio
HIGH	Record DMARC assente — nessuna protezione contro l'uso improprio del dominio nella posta	Categoria: exposure
HIGH	Porta 8080 (pannello di amministrazione senza cifratura) raggiungibile da Internet su 203.0.113.10	Categoria: exposure
MEDIUM	TLS Version 1.0 Detected	
MEDIUM	Portale clienti — TLS 1.0 e 1.1 ancora accettati	Categoria: ssl
MEDIUM	Certificato in scadenza fra 21 giorni su preventivi.esempio-srl.it	Categoria: ssl
MEDIUM	File di configurazione di uno strumento di sviluppo raggiungibile pubblicamente	Categoria: exposure
LOW	Weak Cipher Suites Detected	
LOW	Missing Content-Security-Policy Header	
LOW	Intestazione Content-Security-Policy assente	Categoria: http
INFO	Web Server Version Disclosure	

Indirizzi non a uso esclusivo

Su questi indirizzi rispondono anche nomi che non appartengono al dominio verificato. Prima di intervenire su una porta o su un servizio elencato sopra, va verificato se è tuo: su una macchina in cloud la configurazione è tua anche quando l'indirizzo è del fornitore, mentre su hosting condiviso in pannello può non esserlo. Il fornitore qui sotto è chi possiede la rete, non necessariamente chi amministra il servizio.

Indirizzo	Cosa risponde	Rete di	Sullo stesso IP	Porte rilevate
203.0.113.10	Anche nomi di terzi	Rete di hosting condiviso (esempio)	9 altri nomi	1
203.0.113.42	CDN	Rete di distribuzione dei contenuti (esempio)	—	—

DISCLAIMER: This automated report is for informational purposes only. The scan was performed non-intrusively based on public accessibility. Privateer is not liable for undetected vulnerabilities or subsequent breaches. This document contains confidential information intended solely for the recipient.

Data della verifica: 14 agosto 2026 **Asset: e5e3b100**

Inquadramento normativo

Perimetro e limitazioni

Questo report è un'evidenza tecnica automatizzata della superficie di attacco esterna rilevata alla data indicata. Non costituisce parere legale né certifica la conformità normativa dell'organizzazione. Per una valutazione legale vincolante consultare un professionista qualificato.

Esposizione normativa rilevata

Norma	Collegamento rilevato
NIS2 Art.21(2)(h)	I protocolli TLS 1.0 e 1.1 ancora accettati dal portale clienti non garantiscono la riservatezza del traffico.
NIS2 Art.21(2)(e)	Il pannello di amministrazione raggiungibile in chiaro sulla porta 8080 riguarda la sicurezza dell'acquisizione e della manutenzione dei sistemi.
GDPR Art.32(1)(a)	Un pannello di amministrazione senza cifratura trasporta le credenziali in chiaro sulla rete.
NIS2 Art.21(2)(g)	DMARC assente espone al rischio di email spoofing e phishing

Copertura della scansione

Verifica	Esito	Note
Enumerazione sottodomini	Eseguito	6 rilevazioni
Risoluzione DNS	Eseguito	6 rilevazioni
Scansione porte	Eseguito	9 rilevazioni
Scansione vulnerabilità	Eseguito	4 rilevazioni
Analisi endpoint HTTP	Eseguito	6 rilevazioni
Analisi TLS/SSL del sito	Eseguito	
Analisi TLS dei server di posta	Eseguito	
Rilevamento WAF	Eseguito	6 rilevazioni
Controlli DNS	Eseguito	

DISCLAIMER: This automated report is for informational purposes only. The scan was performed non-intrusively based on public accessibility. Privateer is not liable for undetected vulnerabilities or subsequent breaches. This document contains confidential information intended solely for the recipient.

Data della verifica: 14 agosto 2026 **Asset: e5e3b100**

Verifica	Esito	Note
Sicurezza email	Eseguito	
Percorsi sensibili	Eseguito	1 rilevazioni
Postura dei server di posta	Eseguito	0 rilevazioni
Attribuzione degli indirizzi IP	Eseguito	2 rilevazioni
Ricerca segreti esposti	Eseguito	0 rilevazioni
Certificate Transparency	Eseguito	6 rilevazioni
Sintesi AI	Eseguito	

Limiti dichiarati di questa analisi: Le vulnerabilità rilevabili solo tramite interazione fuori banda (per esempio SSRF cieca) non vengono cercate: la verifica richiederebbe di inviare dati del dominio a un servizio di terze parti esterno a Privateer.

Perimetro della scansione

L'analisi copre esclusivamente la superficie di attacco esterna rilevabile automaticamente alla data indicata. Vulnerabilità interne, applicative o di configurazione non rilevabili esternamente esulano dal perimetro di questo report.

DISCLAIMER: This automated report is for informational purposes only. The scan was performed non-intrusively based on public accessibility. Privateer is not liable for undetected vulnerabilities or subsequent breaches. This document contains confidential information intended solely for the recipient.

Data della verifica: 14 agosto 2026 **Asset: e5e3b100**

Direttiva (UE) 2022/2555 — art. 21(2)

Le dieci misure di gestione dei rischi della direttiva, con i codici delle misure di base ACN corrispondenti (determinazione ACN del 14 aprile 2025). Per ciascuna: questo report porta evidenza tecnica su 7 misure su 10 (5 da integrare con documentazione tua); 3 misure richiedono documentazione interna. Le misure che richiedono documentazione interna — procedure, registri, formazione — non sono osservabili dall'esterno da nessuno strumento: questa tabella serve a sapere quali restano da allegare, non a sostituirle.

	Misura	Misure ACN	Dove sta l'evidenza	Rilievi
(a)	Politiche di analisi dei rischi e di sicurezza dei sistemi Forniamo l'evidenza tecnica su cui l'analisi dei rischi si basa. La politica e la sua approvazione restano dell'organizzazione.	GV.OC-04	**In parte qui, in parte tua**	0
(b)	Gestione degli incidenti Da documentare internamente: procedura di rilevamento e notifica, e registro degli incidenti. I termini sono preallarme 24h, notifica 72h, relazione finale a un mese, in vigore dal 1° gennaio 2026 per i soggetti in elenco dal 2025 e dal 1° gennaio 2027 per quelli inseriti nel 2026.	—	**Documentazione interna**	—
(c)	Continuità operativa, backup e ripristino Da documentare internamente: piano di continuità, procedure di backup e — soprattutto — la prova che un ripristino è stato eseguito. È la parte che gli auditor chiedono per prima, e nessuna verifica esterna può produrla.	—	**Documentazione interna**	—
(d)	Sicurezza della catena di approvvigionamento Attribuiamo gli indirizzi esposti al loro operatore di rete e segnaliamo quelli su cui rispondono anche nomi di terzi, così l'organizzazione sa dove verificare prima di intervenire. Questo report è anche l'evidenza da fornire ai propri clienti soggetti a NIS2.	GV.SC-01	**In parte qui, in parte tua**	0
(e)	Sviluppo e manutenzione sicuri, gestione delle vulnerabilità Verifica ricorrente dell'intera superficie esterna con l'insieme completo dei template di rilevamento: vulnerabilità note, servizi esposti, percorsi accessibili.	ID.RA-01 PR.PS-02	**In questo report**	3
(f)	Valutazione dell'efficacia delle misure adottate Ogni scansione è confrontata con la precedente: problemi nuovi, risolti e ancora aperti. È la prova documentale, datata, che le misure adottate producono un effetto sulla superficie esterna. Le verifiche di efficacia sulle misure interne restano dell'organizzazione.	ID.IM-01	**In parte qui, in parte tua**	0
(g)	Igiene informatica di base e formazione Verifichiamo l'igiene tecnica: intestazioni di sicurezza HTTP, configurazioni deboli, servizi raggiungibili da Internet che non dovrebbero esserlo. La formazione del personale e degli organi di gestione, che la stessa lettera richiede, resta dell'organizzazione.	—	**In parte qui, in parte tua**	0
(h)	Crittografia e cifratura Configurazione TLS, validità e scadenza dei certificati, cifrari deboli, STARTTLS sui server di posta, protocolli che trasmettono credenziali in chiaro.	PR.DS-02	**In questo report**	4

DISCLAIMER: This automated report is for informational purposes only. The scan was performed non-intrusively based on public accessibility. Privateer is not liable for undetected vulnerabilities or subsequent breaches. This document contains confidential information intended solely for the recipient.

Data della verifica: 14 agosto 2026 **Asset: e5e3b100**

	Misura	Misure ACN	Dove sta l'evidenza	Rilievi
(i)	Controllo degli accessi e gestione degli attivi Inventario esterno: sottodomini, porte, indirizzi IP con il loro operatore di rete, certificati, credenziali eventualmente esposte. Gestione del personale e accessi interni restano fuori perimetro. La misura ID.AM-03 è prevista solo per i soggetti essenziali.	ID.AM-03 PR.AA-01	**In parte qui, in parte tua**	3
(j)	Autenticazione a più fattori e comunicazioni protette Da documentare internamente: politica di autenticazione a più fattori e canali di comunicazione protetti. Sono configurazioni interne di accesso, che dall'esterno non si osservano.	—	**Documentazione interna**	—

Questo documento è un'evidenza tecnica di verifica periodica della superficie esterna. Non costituisce una certificazione di conformità alla direttiva NIS2 né al Regolamento (UE) 2016/679, che richiedono anche misure organizzative, di governance e di formazione non verificabili dall'esterno.

DISCLAIMER: This automated report is for informational purposes only. The scan was performed non-intrusively based on public accessibility. Privateer is not liable for undetected vulnerabilities or subsequent breaches. This document contains confidential information intended solely for the recipient.

Data della verifica: 14 agosto 2026 **Asset: e5e3b100**

Allegato tecnico

Il dettaglio delle rilevazioni, strumento per strumento: porte raggiungibili, configurazione TLS e intestazioni HTTP, record DNS e posta, percorsi sensibili. È la parte da inoltrare a chi amministra i sistemi.

Porte raggiungibili da Internet

Indirizzo IP	Porta	Servizio
203.0.113.10	80	HTTP
203.0.113.10	443	HTTPS
203.0.113.10	8080	HTTP Proxy
203.0.113.42	25	SMTP
203.0.113.42	465	
203.0.113.42	993	

TLS & Sicurezza HTTP

TLS Grade: B

Certificato in scadenza tra 21 giorni

Nessun problema TLS critico rilevato.

WAF/CDN: WAF del fornitore CDN

DNS e sicurezza della posta

Record	Stato	Dettaglio
SPF	**Presente**	v=spf1 include:_spf.esempio-srl.it ~all
DMARC	**Assente**	Nessuna protezione anti-spoofing
DKIM	**Presente**	Selettori: selector1, selector2

DISCLAIMER: This automated report is for informational purposes only. The scan was performed non-intrusively based on public accessibility. Privateer is not liable for undetected vulnerabilities or subsequent breaches. This document contains confidential information intended solely for the recipient.

Data della verifica: 14 agosto 2026 **Asset: e5e3b100**

Percorsi sensibili raggiungibili

Sottodominio	Percorso	Stato	Rischio
preventivi.esempio-srl.it	**/.git/config**	200	MEDIO

I path con status 200 indicano che il server ha risposto positivamente alla richiesta. Si raccomanda di verificare manualmente l'accessibilità del contenuto prima di considerarli rischi confermati.

DISCLAIMER: This automated report is for informational purposes only. The scan was performed non-intrusively based on public accessibility. Privateer is not liable for undetected vulnerabilities or subsequent breaches. This document contains confidential information intended solely for the recipient.