Raccomandazioni AGID su TLS e CIPHER SUITE

Approfondimento in merito ai protocolli di sicurezza e alle Cipher Suite da utilizzare per instaurare canali di comunicazione sicuri.

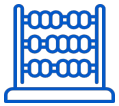
Andrea Ceresoni
Cybersecurity

DIPARTIMENTO
PER LA TRASFORMAZIONE
DIGITALE

Agenda

Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione

- **Piano triennale:** La sicurezza nel piano triennale 2020-2022
- **Stato di sicurezza dei portali della PA:** Monitoraggio dei portali istituzionali della PA
- **TLS :** Funzionamento del protocollo TLS del protocollo crittografico
- **Vulnerabilità protocollo TLS:** Algoritmi in continua evoluzione
- **TLS best practices:** TLS Deployment Best Practices



Sicurezza e privacy by design.

I servizi digitali devono essere progettati ed erogati in modo sicuro e garantire la protezione dei dati personali.

Obiettivi

- **Security**: Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione

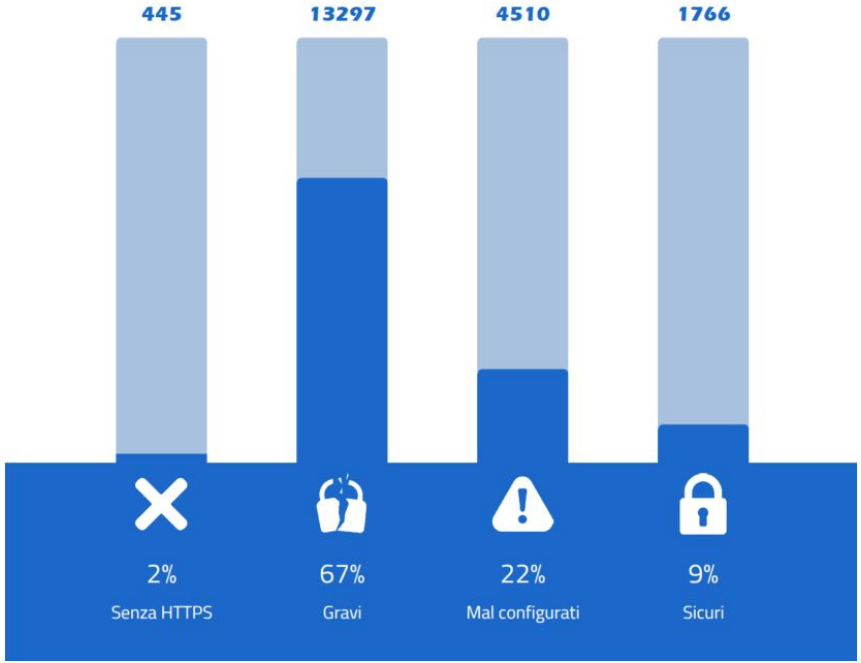
Risultati attesi

- **Target 2021:** Incremento del 25 % dell'uso del protocollo TLS sui portali istituzioni della PA.
- **Target 2022:** Incremento del 75%, rispetto alla baseline, nell'utilizzo del protocollo HTTPS.

La baseline di riferimento è la scansione effettuata da AgiD nella prima prima settimana di dicembre 2020.

21.682 domini monitorati

- **No HTTPS**: 445 (2%)
- **Gravi problemi di sicurezza:** 13.297 (67%)
- **HTTPS mal configurato:** 4.510 (22%)
- **HTTPS sicuro:** 1.766 (9%)



Che cosa è HTTPS.

HTTPS (Hypertext Transfer Protocol Secure) è un protocollo di comunicazione Internet che protegge l'integrità e la riservatezza dei dati tra il computer dell'utente e un sito internet.

I dati inviati tramite HTTPS sono protetti tramite il protocollo **TLS** (Transport Layer Security), che fornisce tre livelli chiave di protezione:

- **Cifratura**
- **Integrità dei dati scambiati**
- **Autenticazione**

HTTPS = HTTP + TLS (SSL)

Perché è importante

- **Cifratura**
  TLS codifica i messaggi la comunicazione tra client e server in modo tale che solo le persone autorizzate siano in grado di poterli leggere.

- **Integrità dei dati**
  TLS si assicura che nessuna informazione scambiata tra client e server venga danneggiata, manomessa o falsificata.

- **Autenticazione**
  TLS consente a ciascuna parte della comunicazione di verificare che l'altra parte sia chi dichiara di essere tramite l’uso di certificati.

Perché è importante

RGPD art. 32

IL Regolamento Generale sulla Protezione dei Dati è molto chiaro in merito alla cifratura e integrità dei dati di tipo **PII** e **PHI**

"...**Il titolare del trattamento e il responsabile del trattamento mettono** in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la **cifratura** dei dati personali.
b) la capacità di assicurare su base permanente la **riservatezza**, **l'integrità**, la **disponibilità** e la resilienza dei sistemi e dei servizi di trattamento"

Perché è importante

Qualche dato

Nel 2019 il numero totale di record esposti è aumentato del 284%

- **7,098 data breach segnalati**
- **15.1 billion records rubati**

“Fonte: https://www.helpnetsecurity.com/”

Come funziona?

Una connessione TLS inizia con una fase di handshake in cui un client e un server concordano un segreto condiviso dopo aver negoziato parametri importanti come le suite di crittografia.

TLS Handshake

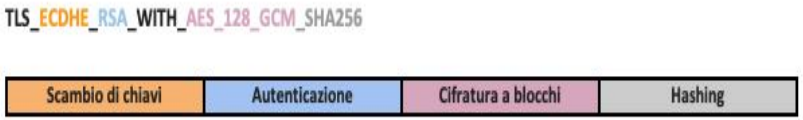
Come funziona la negoziazione TLS

- Il client si connette al server (tramite TCP).
- Il client invia una serie di specifiche
  - Version of SSL/TLS
  - Suite di cifratura
- Dopo aver completato la configurazione di base, il server invia il suo certificato.
- Il client verifica tramite il certificato che il server sia veramente che afferma di essere client e server si scambiano una chiave che verrà utilizzata da client e server per lo scambio di dati
- A questo punto client e server possono scambiarsi i dati in modo sicuro

Cipher suite o suite di cifratura

Cosa è una ciphersuite

- Una suite di cifratura è una selezione di primitive crittografiche e altri parametri che definiscono esattamente come verrà implementata la sicurezza.



Versione TLS e Cipher Suite sicure.

Molte implementazioni crittografiche del passato si sono dimostrate vulnerabili con il passare del tempo e con l'aumento della capacità di calcolo dei computer.

Per questo motivo le suite di cifrature vengono aggiornate con algoritmi sempre più complessi al fine di garantire una comunicazione sicura.

Periodicamente è necessario controllare tutte le versioni e rimanere aggiornati per evitare configurazioni errate e nuove vulnerabilità.

Esiste un documento aggiornato frequentemente dove è possibile verificare cipher suite e versione TLS sicure.
https://www.agid.gov.it/it/sicurezza/tls-e-cipher-suite

Il documento è in costante aggiornamento

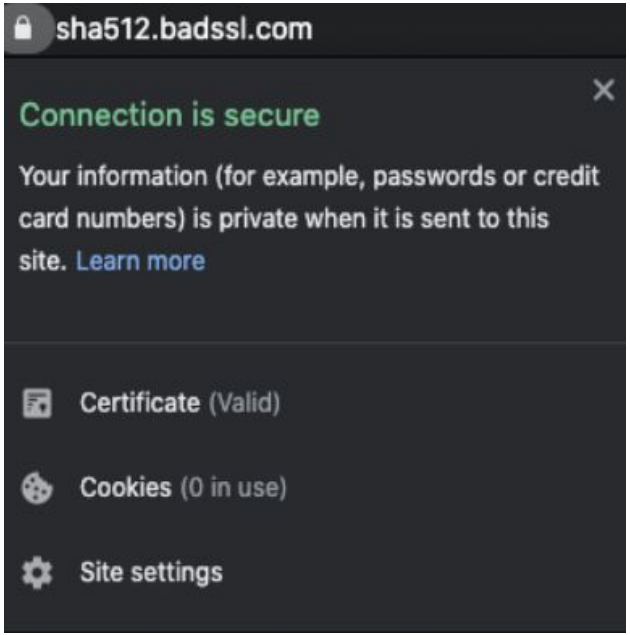
Timeline vulnerabilità TLS/SSL (non aggiornata)

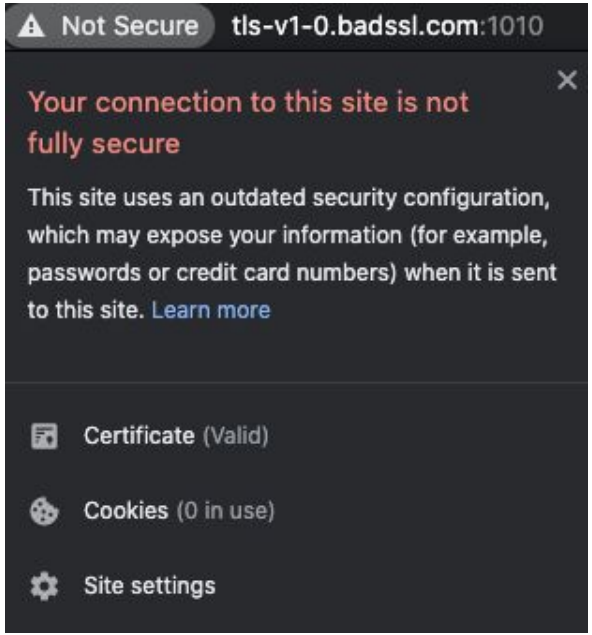
Validazione del certificato da parte del client

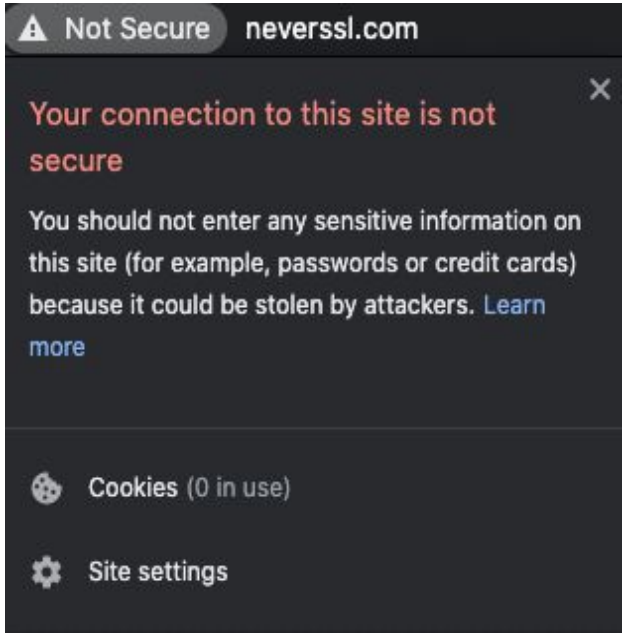
Quando il server su richiesta del client manda un certificato x.509 il client effettua le seguenti verifiche per accertare che sia valido.

- **Verifica che il certificato non sia scaduto**
- **Verifica che il certificato sia stato emesso da una certification authority di fiducia**
- **Verifica che il nome specificato di dominio sul certificato corrisponde al dominio effettivo del server**
- **Verifica che il certificato non sia stato revocato dalla certification authority**

Esempi TLS


sha512.badssl.com
Connection is secure
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more
Certificate (Valid)
Cookies (0 in use)
Site settings


Not Secure
tls-v1-0.badssl.com:1010
Your connection to this site is not fully secure
This site uses an outdated security configuration, which may expose your information (for example, passwords or credit card numbers) when it is sent to this site. Learn more
Certificate (Valid)
Cookies (0 in use)
Site settings


Not Secure
neverssl.com
Your connection to this site is not secure
You should not enter any sensitive information on this site (for example, passwords or credit cards) because it could be stolen by attackers. Learn more
Cookies (0 in use)
Site settings

Riepilogo finale per una corretta configurazione

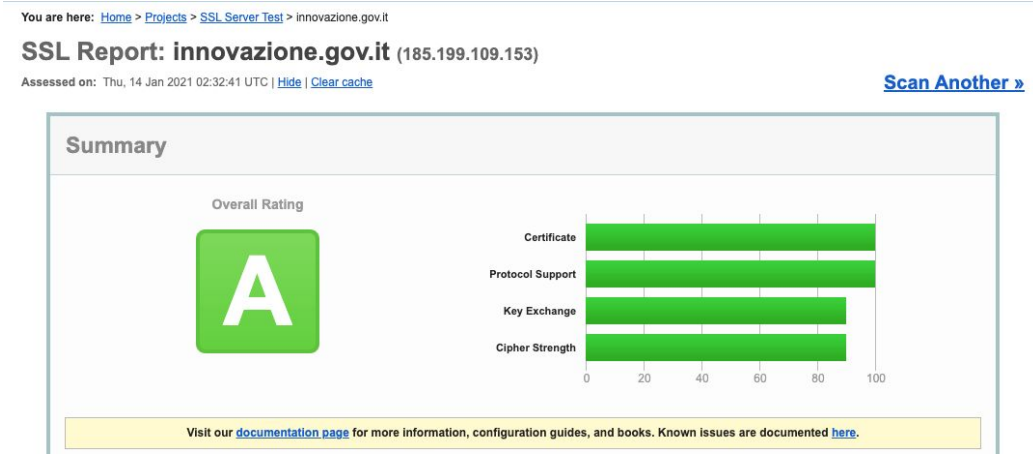
- **Utilizzare solo versione 1.2/1.3:** Tutte le versione precedenti soffrono di vulnerabilità note
- **HTTPS only**
  Utilizzare solo ed esclusivamente HTTPS per evitare che i dati siano intercettati o alterati

- **Usare ciphersuite aggiornate**
  Verificare che le cipher in uso non siano vulnerabili. Mid e Agid tengono aggiornati il documento
- **Certificati**
  Usare e monitorare che i certificati non siano scaduti e che siano firmati certification authority di fiducia
- **Redirect automatico HTTP >HTTPS**
  Redirezionare in automatico i client che si connettono in http verso https al fine di evitare trasmissione di dati in chiaro

Riepilogo finale per una corretta configurazione

- **Rinegoziazione della sessione**
  Le rinegoziazione della sessione lato client è vulnerabile a una serie di attacchi e dovrebbe essere disabilitata
- **Compressione TLS**
  La compressione TLS DOVREBBE essere disabilitata; essa è stata rimossa dalla versione 1.3 di TLS perché sfruttata in passato da diversi exploit, tra cui il noto CRIME.
- **Estensione Heartbeat**
  L'uso dell'estensione Heartbeat è NON RACCOMANDATO e nel caso fosse necessario il suo utilizzo, si raccomanda di verificare che non sia vulnerabile all'attacco Heartbleed.

Verifica della corretta configurazione TLS del proprio portale



Seguici su

https://innovazione.gov.it/

@InnovazioneGov

@DipartimentoTrasformazioneDigitale

@company/ministeroinnovazione/

DIPARTIMENTO
PER LA TRASFORMAZIONE
DIGITALE