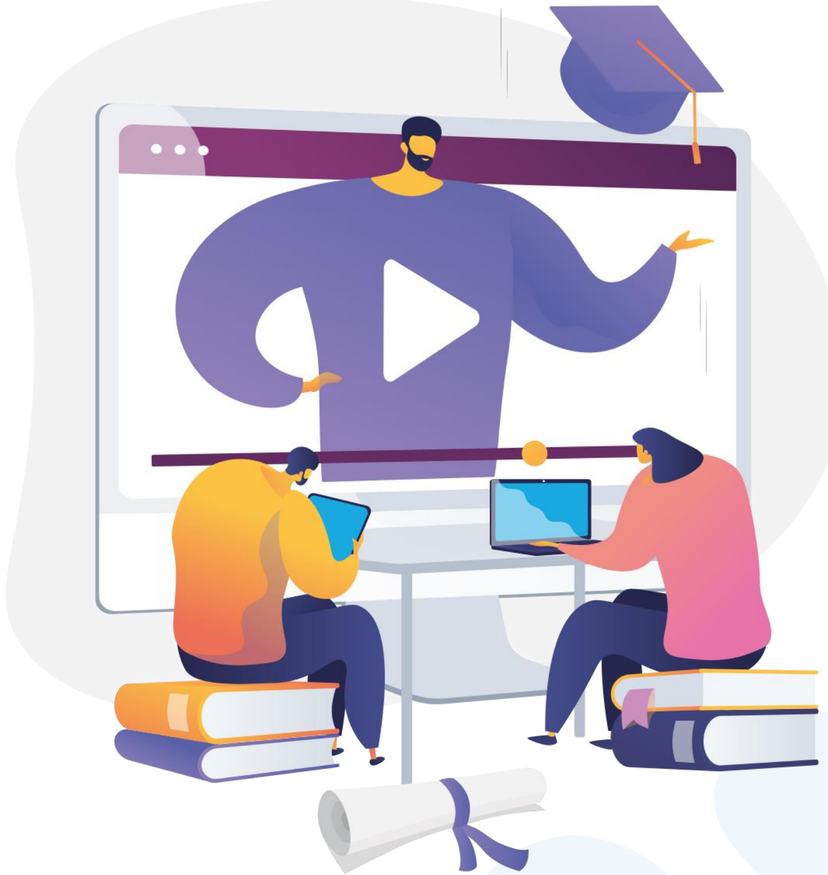
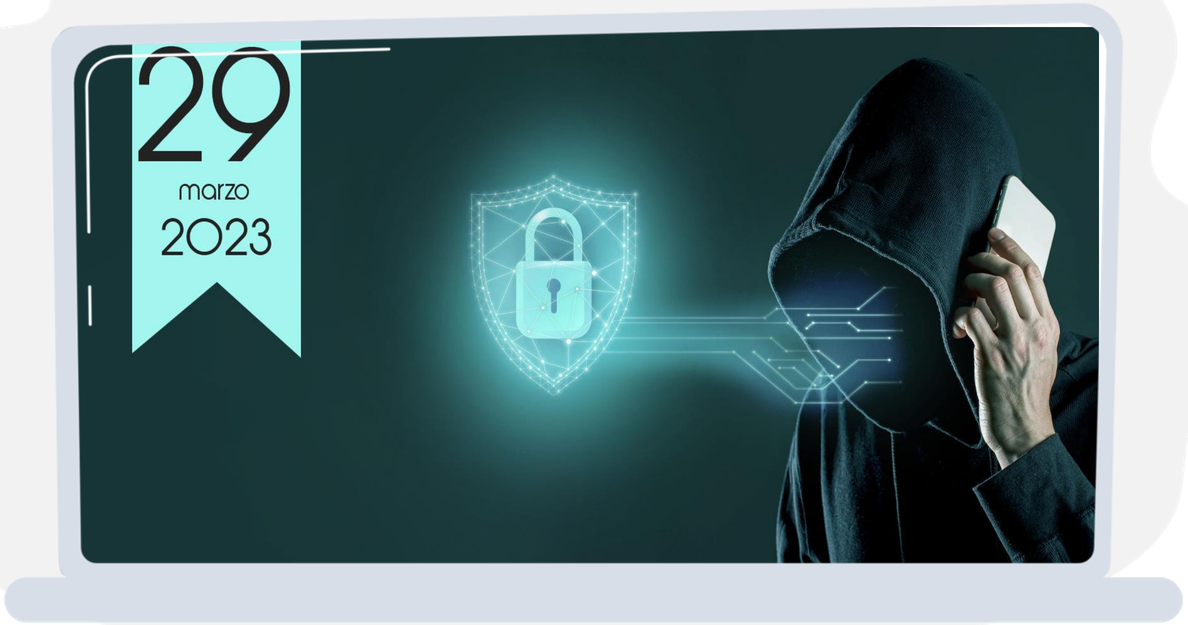
DIGITAL Academy

by register.it



Certificati SSL e DNSSEC

La "Chain of trust" a garanzia dell’affidabilità del proprio dominio



La Digital Academy

1 Webinar

2 Certificazioni

3 Network

Web Agency Network

La “**Web Agency Network**" è una **rete di rivenditori accreditati** garantita da Register.it.

Lo scopo è quello di **mettere in contatto i clienti di Register.it** che cercano rivenditori di zona garantiti **con i Business Partner accreditati e certificati**.

Entrano a far parte della "**Web Agency Network**" i clienti Business Partner che **hanno ottenuto almeno una certificazione della Digital Academy** di Register.it.

Programma Business Partner

Il **programma Business Partner di Register.it** si rivolge ad agenzie e professionisti del web e del digitale in tutta Italia come web agency, web developer e web designer.

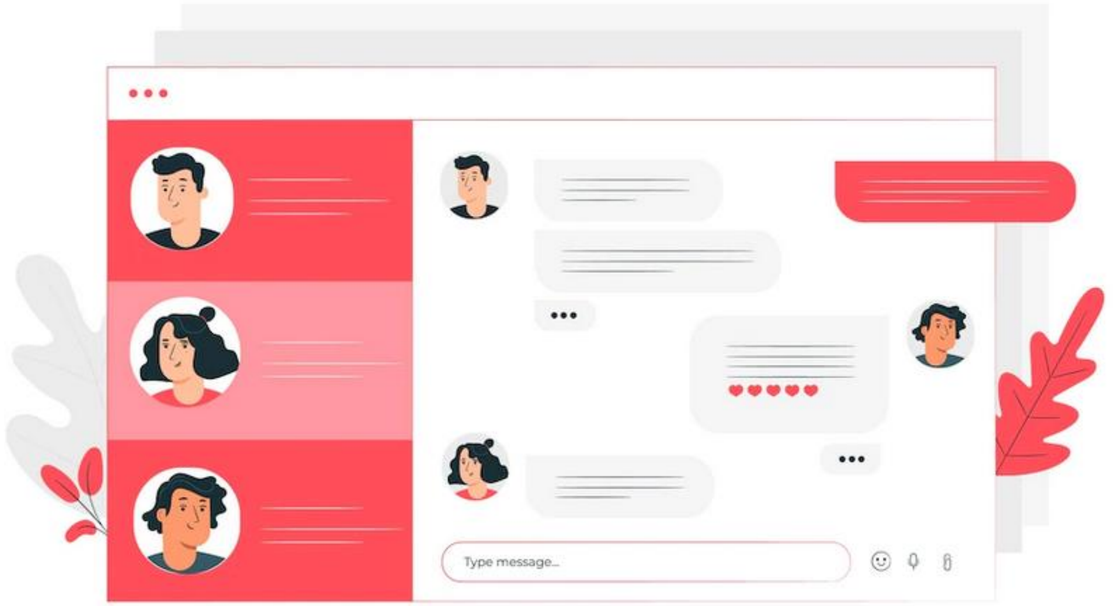
I clienti **Business Partner** hanno numerosi vantaggi come **sconti riservati** su tutta la vasta gamma di prodotti di Register.it, **consulenza personalizzata**, **assistenza tecnica prioritaria** e molto altro.

.Lo speaker

Alessio Rossi
CISO Southern Europe team.blue
Sviluppo, implementazione e mantenimento di politiche e programmi di gestione della compliance e della sicurezza aziendale.

Hai dubbi o domande?

Scrivici in chat!



Argomenti di questo webinar

- **Introduzione e premesse**

  Il significato della «Chain of Trust» nel mondo dei servizi digitali

- **Certificati SSL**

  - **Tipologie di certificati SSL, caratteristiche di sicurezza e scenari di attacco**
    A cosa servono, come funzionano , il processo dei emissione e quali scenari di attacco prevengono o mitigano i certificati SSL

  - **SSL: Impatti sul GDPR, sanzioni del Garante per la Privacy e penalizzazioni SEO in loro assenza**
    Cosa si rischia in termini di sanzioni e visibilità del sito/dominio in assenza di certificati SSL

  - **Impatti su score reputazionale del sito web e filtri dei sistemi di EP / EDR.**
    Scorecard negative e alert dei sistemi di Endpoint Protection e Endpoint Detaction and Response in assenza di certificarti SSL

  - **Esempio d'installazione dei certificati SSL su Plesk**
    Breve tutorial su come installare un certificato SSL su Plesk

Argomenti di questo webinar

- **DNSSEC**
  - **In cosa consiste il protocollo DNSSEC e la sua importanza**
    Autenticità e integrità dei record DNS
  - **Controlli di validità della "Chain of trust"**
    Il meccanismo di autenticazione a cascata verificato dai resolver
  - **Scenari di attacco verso i quali il DNSSEC è efficace**
    DNS Cache Poisoning e DNS Spoofing
  - **L’impatto del DNSSEC sullo score reputazionale del dominio**
    Scorecard del dominio in assenza di DNSSEC
  - **Esempi di configurazione di record DNSSEC sulle zone del dominio**
    Struttura, informazioni e modalità di configurazione di un record DNSSEC
  - **Implicazioni tecniche nell’utilizzo del DNSSEC**
    Attenzioni e accorgimenti da adottare quando si configura un record DNS per evitare malfunzionamenti
  - **Esempio di attivazione di DNSSEC da Pannello di Controllo**
    Breve tutorial su come abilitare il DNSSEC da Pannello di Controllo

Introduzione e premesse

Affidabilità dei servizi digitali

Il concetto di «Chain of Trust»

Il concetto di **affidabilità** e di modalità con cui questa è verificabile dagli utenti assume una connotazione specifica nel mondo dei servizi digitali.

I criteri di valutazione di un servizio o prodotto erogato o venduto materialmente in un negozio o in un punto vendita e la rintracciabilità "fisica" dell'esercente in caso di problemi, non sono direttamente applicabili nel mondo dei servizi digitali, se non ricorrendo a strumenti che permettano di "derogare" la valutazione dell'affidabilità a soggetti terzi autorevoli o strumenti di verifica a loro volta certificati da soggetti autorevoli.

Questo è il principio su cui si basa la **"Chain of Trust"** dei servizi digitali, nelle sue varie modalità di implementazione: **derogare ad un soggetto terzo autorevole o a strumenti certificati da soggetti terzi autorevoli la conferma dell'affidabilità del servizio e del soggetto che lo eroga.**

Certificati SSL

Tipologie di certificati SSL - caratteristiche di sicurezza

- Garanzia di **affidabilità e sicurezza** nella trasmissione dei dati da e verso un sito web, criptando le informazioni e le comunicazioni che si scambiano su Internet.
- **Ranking** del sito come **"sicuro"** su Google e sugli altri motori di ricerca.
- **Segnalazione del sito** come **"sicuro"** dalle funzioni di "navigazione web sicura" di tutte le maggiori soluzioni di endpoint security.

Tipologie di certificati SSL – DV/DVW, EV, OV

DIFFERENZE TRA LE VARIE TIPOLOGIE

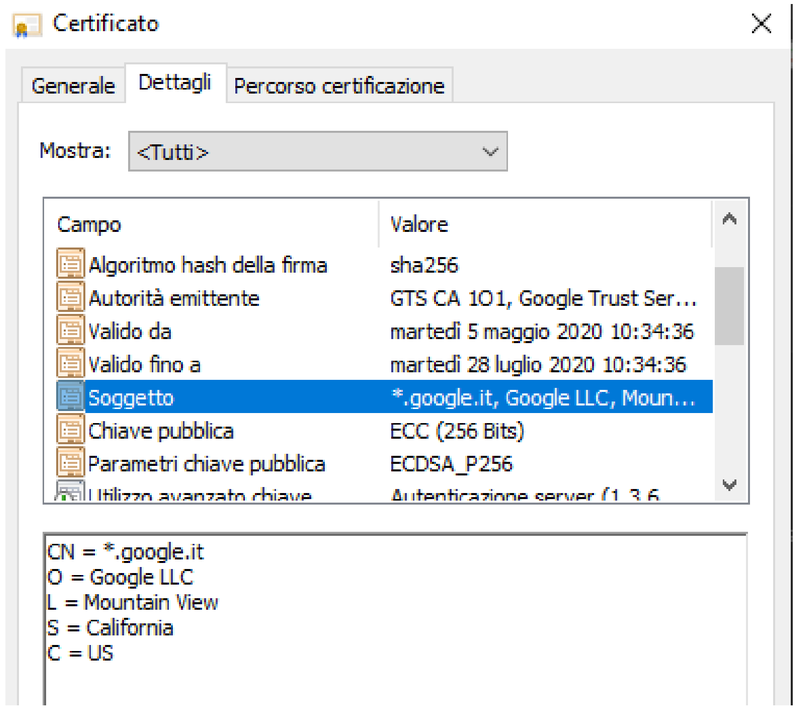
- **Certificati con convalida del dominio (DV) e con convalida del dominio Wildcard (DVW)**
  Convalidano la proprietà del dominio, possono essere acquisiti in modo anonimo e non legano un dominio a una persona, luogo o entità. La CA controlla il diritto del richiedente di utilizzare un nome di dominio specifico. Nella barra di navigazione compare il simbolo del lucchetto e nessun'altra informazione.

- **Certificati a convalida estesa (EV)**
  La CA verifica il diritto del richiedente di utilizzare il nome di dominio specifico e conduce inoltre un'accurata verifica del proprietario/azienda, secondo specifiche linee guida. Fornisce ai clienti maggiori garanzie di attendibilità ed è utilizzabile in caso di frode durante le transazioni su quel sito web. Nella barra di navigazione compare il lucchetto chiuso, diversamente evidenziato rispetto ai certificati DV nella maggior parte dei browser, il nome dell'organizzazione ed eventualmente anche all'ID del paese.

Tipologie di certificati SSL – DV/DVW, EV, OV

DIFFERENZE TRA LE VARIE TIPOLOGIE

- **Certificati con convalida dell'organizzazione (OV)**
  Rispetto ai certificati SSL EV, oltre al proprietario del dominio, vengono effettuate delle ulteriori verifiche sull'affidabilità dell'azienda/organizzazione proprietaria. Anche in questo caso oltre a trovare il lucchetto evidenziato nella maggior parte dei browser più usati, il nome dell'organizzazione ed eventualmente anche l'ID del paese sarà possibile accedere a maggiori informazioni sull'organizzazione cliccando sul lucchetto.



SSL: Impatti sul GDPR, sanzioni del Garante per la Privacy

L'**Autorità garante per la protezione dei dati personali** si per si è già espressa con provvedimenti e pubblicazioni sul significato più tecnico di "protezione dei dati personali" ai fini dell'integrità e della riservatezza dei dati, affermando che

«L'interazione di un utente con un sito web ai fini della trasmissione di dati personali debba essere protetta con protocolli crittografici SSL (Secure Socket Layer), garantendo una migliore sicurezza a fronte dei rischi di furto di identità sempre presenti nell'interazione web con normali protocolli http in chiaro.»

SSL: Impatti sul GDPR, sanzioni del Garante per la Privacy

Nell'ottobre 2022 l'Autorità è arrivata a sanzionare per 15.000 euro un'azienda che, non utilizzando certificati SSL, non ha di fatto rispettato gli artt. 5, par. 1, lett. f), 25, par. 1, e 32 del GDPR, che prevedono che il titolare del trattamento

«...tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, debba mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso, la cifratura dei dati personali».

SSL: Penalizzazioni SEO in loro assenza

Le tecniche di **Search Engine Optimization (SEO)** ovvero l'ottimizzazione dei parametri finalizzata a rendere più facilmente ricercabile un sito web e i suoi contenuti dai motori di ricerca e a migliorarne il posizionamento (ranking) tra i risultati.

I vari motori di ricerca, per determinare la posizione dei siti web nella pagina risultati, considerano vari fattori differenti e molteplici variabili. Un **fattore di peso primario** per gli algoritmi di ricerca **è la sicurezza**.

Un motore di ricerca famoso e considerato affidabile non posizionerà mai nei primi risultati un sito non sicuro e tenderà anzi dagli un ranking basso anche in presenza di altri fattori che ne permetterebbero un ranking superiore. **Ne va dell'affidabilità percepita del motore di ricerca stesso**.

Un sito web che non dispone di un certificato SSL, non potendo garantire né una connessione sicura né tantomeno fornire alcuna credenziale per autenticarne la proprietà del dominio riceverà dai motori di ricerca **un ranking SEO molto basso** e la sua visibilità sul web ne sarà inevitabilmente compromessa.

Impatti su score reputazionale del sito web

Sul mercato esistono diversi prodotti o servizi che raccolgono informazioni pubbliche (fonti OSINT), analizzano in modo non invasivo le pagine e le interfacce web e, all'occorrenza, utilizzano anche tecniche più complesse per recuperare informazioni non pubbliche **per fornire lo scoring di un servizio web**.

Lo complessità di queste valutazioni può essere molto variabile ma in ogni caso un servizio web erogato da un **dominio senza certificato SSL** riceverà sicuramente da questi strumenti uno **scoring** complessivamente **negativo** o comunque insufficiente a garantire un servizio sicuro.

Esempio d'installazione dei certificati SSL su Plesk

- Come generare il file CSR

Come generare il file CSR per i Certificati SSL

Dopo l'acquisto di un **certificato SSL** la prima cosa da fare per associarlo al dominio ed ottenerlo è la generazione del file CSR e della relativa **chiave privata (KEY)**.

|| *ATTENZIONE!! I files CSR e KEY devono essere salvati in locale sul tuo PC e conservati per tutta la validità del Certificato SSL.*

Nell'Area Clienti di Register è disponibile uno strumento per la creazione del file CSR, di seguito ti riportiamo i passaggi da seguire:

1) Accedi all'Area Clienti inserendo le tue credenziali di accesso su Register
2) Clicca sul Certificato SSL da attivare nel menu laterale destro del pannello di controllo, nella sezione "DA ATTIVARE"

3) Clicca sul link "**strumento**" che sarà visibile nel testo della pagina

https://www.register.it/assistenza/generazione-file-csr-per-il-certificato-ssl/

Esempio d'installazione dei certificati SSL su Plesk

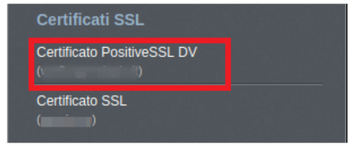
- Come installare un certificato SSL su Hosting Cpanel

Come installare SSL su Hosting Cpanel

|IMPORTANTE
|Per procedere all'installazione SSL occorre aver precedentemente generato il file CSR, aver inviato la richiesta di verifica alla Certification Authority e completato le validazioni previste. Clicca qui se non sai come fare.

!!ATTENZIONE!! Per poter procedere con l'installazione è obbligatorio avere la chiave privata, questo file si trova nel file .zip che hai scaricato prima di avviare la richiesta del certificato ed ha un'estensione .key

1) Accedi all'area di gestione del dominio su cui vuoi installare il certificato SSL, clicca sul link della sezione di gestione del Certificato SSL che trovi nel menù laterale destro



e sull'apposita icona per scaricare il **file .CRT**

https://www.register.it/assistenza/installare-certificato-SSL-cpanel/

DNSSEC

In cosa consiste il protocollo DNSSEC e la sua importanza

Il **Domain Name System Security Extensions (DNSSEC) è** un protocollo di sicurezza che garantisce e permette di verificare l'autenticità e l'integrità dei record DNS.

Un **D**omani **N**ame **S**ystem è un sistema che ha il compito di "tradurre" o "risolvere" la URL del sito in un indirizzo IP numerico che identifica il sito nel web, permettendo così la visualizzazione dei contenuti del sito web associato a quel nome a dominio.

Le informazioni per effettuare questa mappatura sono contenute nei record DNS. **L'affidabilità del DNS** dipende, quindi, **dall'autenticità e dall'integrità di queste informazioni.**

Il DNSSEC aggiunge un livello di sicurezza introducendo firme crittografiche con protocollo a chiave asimmetrica sui record DNS

In cosa consiste il protocollo DNSSEC e la sua importanza

La firma digitale dei record DNS prevede innanzitutto che la funzionalità DNSSEC sul DNS generi una **coppia di chiavi** da utilizzare per la **cifratura asimmetrica** che realizza la firma.

- La **chiave privata** è il parametro segreto che rimane interna nel sistema DNS ed è utilizzata per firmare (cifrare) i record DNS della zona.

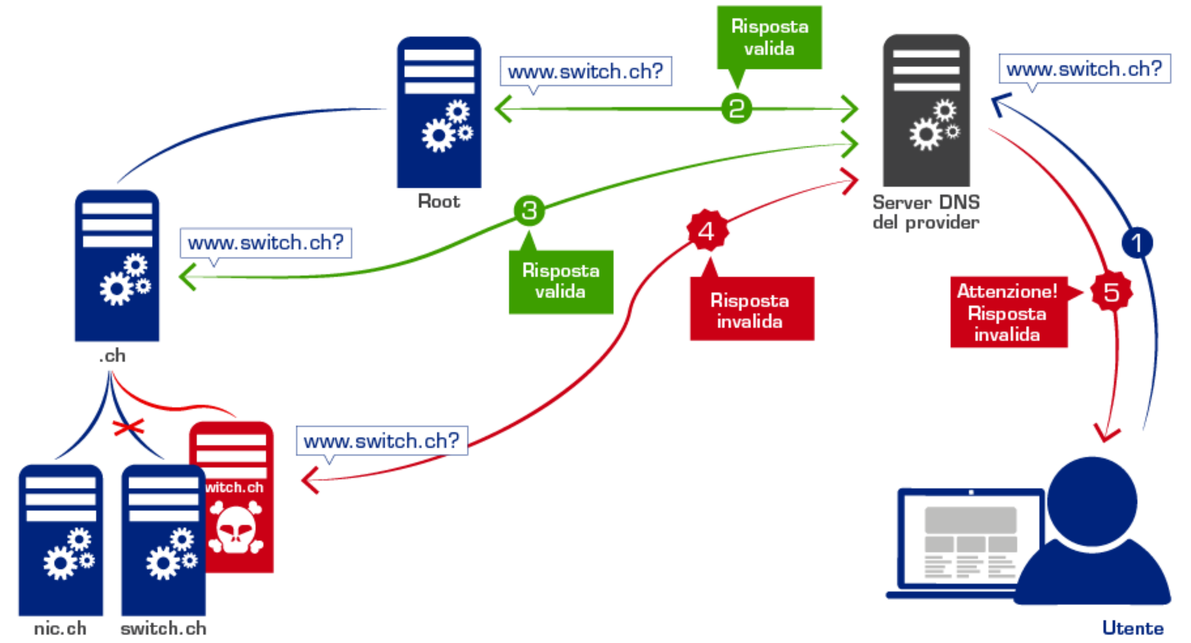
- La **chiave pubblica** viene pubblicata dal DNS tramite un record apposito, DNSKEY Record, rendendola disponibile per poter decifrare la firma dei record DNS e quindi la loro autenticità e integrità.

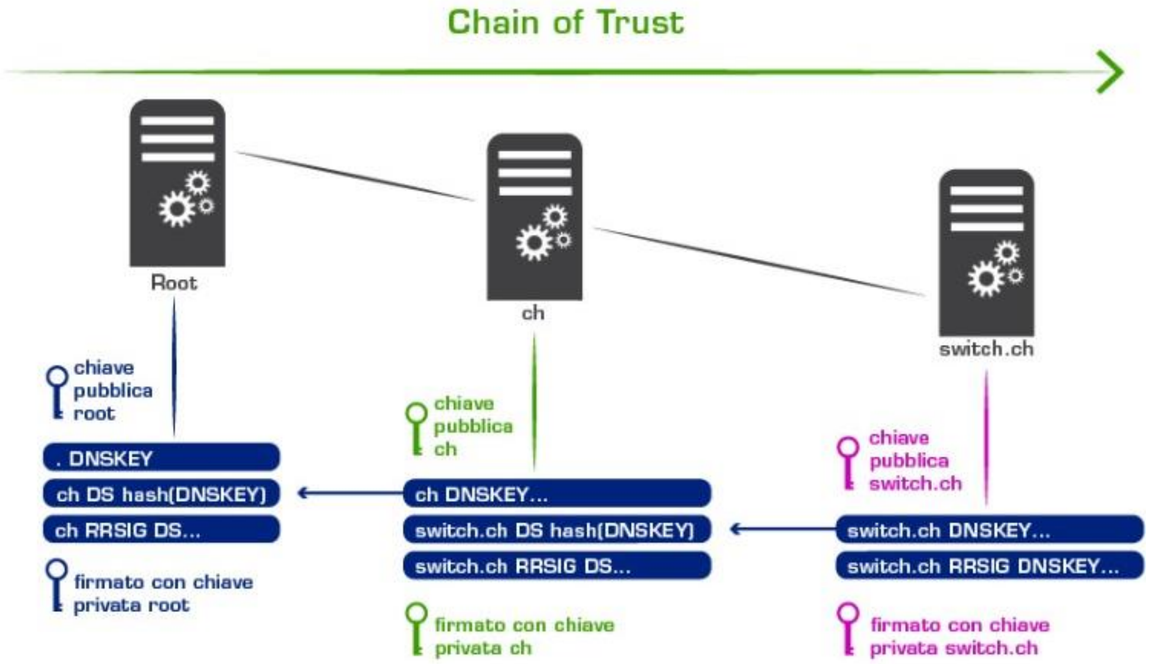
L’affidabilità della chiave pubblicata costituisce il punto critico di tutto l’algoritmo ed è "demandata" ad una "Chain of Trust" di autorità simile alla gerarchia dei DNS utilizzata per la risoluzione dei nomi a dominio.

Controlli di validità della "Chain of Trust"

- Ogni livello della gerarchia di risoluzione dei sistemi DNS invia una copia della chiave pubblica al livello successivo nella gerarchia.

  L'istanza superiore riporta questa riproduzione nella sua zona (DS Record) e ne garantisce l'autenticità mediante una firma. La chiave pubblica di questa istanza viene trasmessa a sua volta all'istanza superiore. **La catena si basa quindi sull'interattività della deroga verso il livello superiore che è autorevole per garantire l'autenticità per il lo specifico livello di dominio.**





Scenari di attacco verso i quali il DNSSEC è efficace

DNS Spoofing – Tipologia di attacco Man In The Middle

Il sistema vittima effettua una query DNS che viene catturata dall'attaccante che **si spaccia per il DNS destinatario** inviando alla vittima una risposta contenente informazioni false per **ridirezionare** la connessione della vittima **verso un dominio diverso**, solitamente predisposto **per effettuare attività fraudolente** o veicolare altri tipi di attacchi sulla vittima.

In assenza di DNSSEC che verifica l'autenticità della risposte all'attaccante, può essere sufficiente **intercettare l'ID della query DNS** inviata e rispondere al mittente inserendo l'ID atteso prima del DNS destinatario per **spacciare la risposta per quella del reale DNS server**.

Scenari di attacco verso i quali il DNSSEC è efficace

DNS Cache Poisoning – Attacco di Injection

Questo tipo di attacco sfrutta la necessità dei DNS di utilizzare cache con un determinato periodo di vita (TTL) in cui sono presenti porzioni del record di corrispondenze IP/URL per rispondere più velocemente alle richieste.

L'attacco va ad inserire nella cache dei name server dei **record fake** creati ad hoc **per reindirizzare la connessione della vittima** con un TTL molto grande in modo che restino per molto tempo nella cache del name server prima di essere sostituiti con quelli presenti nel database.

Anche in questo caso, **in assenza del DNSSEC** per autenticare le risposte, se l'attacco riesce e la cache viene avvelenata (poisoned) **la vittima riceverà in risposta l'indirizzo malevolo** spacciato invece di quello presente nel record DNS autentico.

L’impatto del DNSSEC sullo score reputazionale del dominio

Analogamente allo scoring di sicurezza del siti web sono state sviluppate varie soluzioni che permettono di effettuare rapidamente, online, una **valutazione dei parametri significativi per l’affidabilità della configurazione dei DNS** su determinati domini.

Questi strumenti valutano principalmente:

- Se il nome a dominio è raggiungibile attraverso i protocolli IPv4 e IPv6
- Se tutti i nameserver associati al nome a dominio sono operativi
- Se sul nome a dominio è **abilitata la funzionalità DNSSEC** (Domain Name Security Extensions)

In base a questi valori viene emesso un punteggio che risente in modo importante dell’eventuale assenza di DNSSEC.

Esempi di configurazione di record DNSSEC sulle zone del dominio

TIPI DI RECORD AGGIUNTI DAL DNSSEC E LORO FUNZIONE

- **DNSKEY**
  Chiave pubblica che il resolver DNS utilizza per verificare le firme DNSSEC nei record DNS firmati (RRSIG)

- **RRSIG (resource record signature**)
  Contiene la firma DNSSEC per un record set. I resolver DNS verificano la firma con una chiave pubblica, memorizzata nel record DNSKEY.

- **DS (delegation signer)**
  Record che fa riferimento alla DNSKEY di una zona delegata. Il record DS si trova nella zona del nome a dominio e fa riferimento ai dati DNSSEC del sottodominio su name server esterno, in modo da poter verificare la correttezza dei dati DNSSEC del sottodominio. Il record DS viene inserito nella zona padre insieme ai record NS delegati. Questo record mappa la "Chain of Trust "

Esempi di configurazione di record DNSSEC sulle zone del dominio

TIPI DI RECORD AGGIUNTI DAL DNSSEC E LORO FUNZIONE

- **NSEC (next secure record)**
  Contiene un collegamento al nome del record successivo nella zona ed elenca i tipi di record esistenti per il nome del record. I resolver DNS utilizzano i record NSEC per verificare l'inesistenza di un nome e di un tipo di record come parte della convalida DNSSEC.

- **NSEC3 (next secure record version 3)**
  Contiene collegamenti al nome del record successivo nella zona (in ordine di ordinamento dei nomi con hash) ed elenca i tipi di record esistenti per il nome coperto dal valore hash nella prima etichetta del nome proprio del record NSEC3. Questi record possono essere utilizzati dai resolver per verificare l'inesistenza di un nome e di un tipo di record nell'ambito della convalida DNSSEC. I record NSEC3 sono simili ai record NSEC, ma NSEC3 utilizza nomi di record con hash crittografico per evitare l'enumerazione dei nomi di record in una zona.

- **NSEC3PARAM (next secure record version 3 parameters)**
  I server DNS autoritativi utilizzano questo record per calcolare e determinare quali record NSEC3 includere nelle risposte alle richieste DNSSEC per nomi/tipi non esistenti.

Implicazioni tecniche nell’utilizzo del DNSSEC

- Le risposte alle query DNS possono essere molto lunghe e contenere più record **DNSKEY** e **RRSIG**.
- Potenziali **errori nell’inserimento delle DNSKEY,** ove non generate e inserite con strumenti automatici.
- Maggiori requisiti computazionali e cache dei resolver ricorsivi DNSSEC è molto più grande in data la necessità di gestire firme e chiavi.
- Se i client utilizzano resolver che non supportano il DNSSEC le zone con DNSSEC configurato non saranno visibili.

Esempio di attivazione di DNSSEC da Pannello di Controllo

Come abilitare il protocollo DNSSEC sul dominio

Puoi abilitare il protocollo DNSSEC direttamente dalla tua Area Clienti con un semplice click.

Per farlo segui questi semplici passaggi.

1) Accedi alla tua Area Clienti Register.it. Non sai come fare?

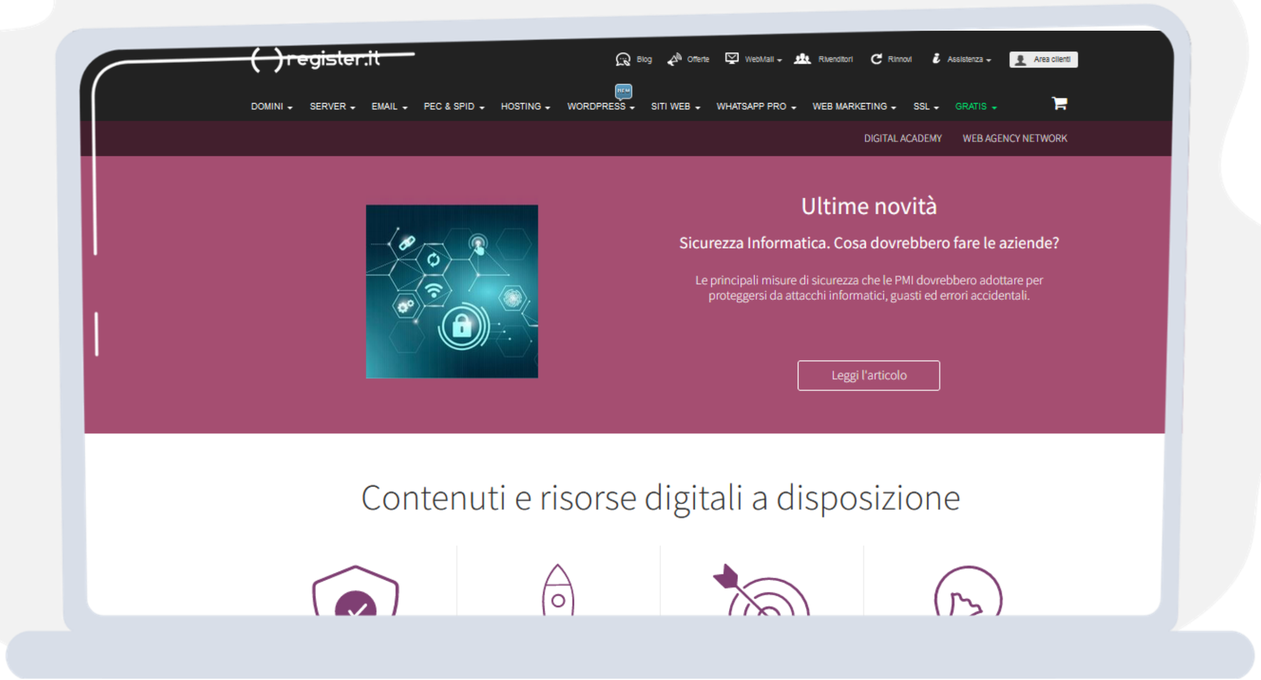
2) Clicca sul nome del tuo dominio, lo trovi nella colonna destra all'interno della sezione I TUOI PRODOTTI

https://www.register.it/help/come-abilitare-il-protocollo-dnssec-sul-dominio/

Questions and Answers

.Grazie!

Continua a seguirci...



register.it

part of team.blue