Crittografia, privacy e protezione dei dati: un delicato equilibrio

Linee guida aziendali, su privacy e sicurezza per una ispezione SSL/TLS completa

zscaler™

Riassunto

La crittografia a chiave pubblica SSL/TLS è lo standard di settore per la protezione dei dati ed è utilizzata per garantire la sicurezza delle transazioni web per gran parte della rete internet. La sua crittografia sicura protegge i dati privilegiati in transito e offre affidabilità e anonimato agli utenti. D'altro canto però, fornisce anche una copertura per gli malintenzionati che utilizzano i protocolli SSL/TLS sfruttando proprio affidabilità e anonimato per coprire le proprie attività.

I responsabili IT delle aziende dovrebbero sfruttare metodologie di ispezione SSL/TLS complete per ridurre i rischi celati nel traffico crittografato. Questo testo esamina il rischio correlato alle minacce crittografate, considera le implicazioni aziendali, per la privacy e la sicurezza legate alla gestione di tale rischio ed espone delle misure costruttive per bilanciare le esigenze di sicurezza con i diritti sulla privacy dei dipendenti. In fin dei conti, il modo migliore con cui i responsabili IT possono garantire i diritti del singolo dipendente è quello di proteggere l'organizzazione da minacce e attacchi.

Internet prima era molto più semplice: un parco giochi aperto per l'élite tecnicamente esperta...

Al giorno d'oggi, è diventato il luogo in cui si svolgono molte attività moderne complesse, nonché la vita normale. Con l'ubiquità sorge però un nuovo rischio. Per sua stessa natura, una rete "internet per tutti" include un paradiso per gli malintenzionati, determinati a trarre vantaggio da quelli di noi che la usano per condurre affari e dedicarsi alla vita di tutti i giorni.

I dati privilegiati devono essere protetti, soprattutto quando sono in transito. La crittografia offre il modo più pratico per farlo. I dati codificati con i protocolli di crittografia SSL/TLS standard del settore non possono praticamente (leggere: economicamente) essere decodificati da un malintenzionato che li intercetta. (Vedere la Figura 1 e fare riferimento alla barra laterale “Transport Layer Security [TLS] e Secure Sockets Layer [SSL]”). La crittografia aiuta anche a stabilire la fiducia e a preservare l'anonimato. È questa combinazione di funzionalità che rende la crittografia SSL/TLS ideale per proteggere le comunicazioni su internet, dalla semplice navigazione web agli acquisti e-commerce.

Negli ambienti aziendali di oggi, è essenziale proteggere le risorse aziendali *e* preservare la privacy dell'individuo. SSL/TLS serve entrambe le missioni apparentemente opposte, ma, nelle mani sbagliate, tale tecnologia può diventare potenzialmente pericolosa. Cosa succede quando I malintenzionati la utilizzano per crittografare malware e nascondere le proprie attività? Come può l'impresa moderna combattere questa minaccia?

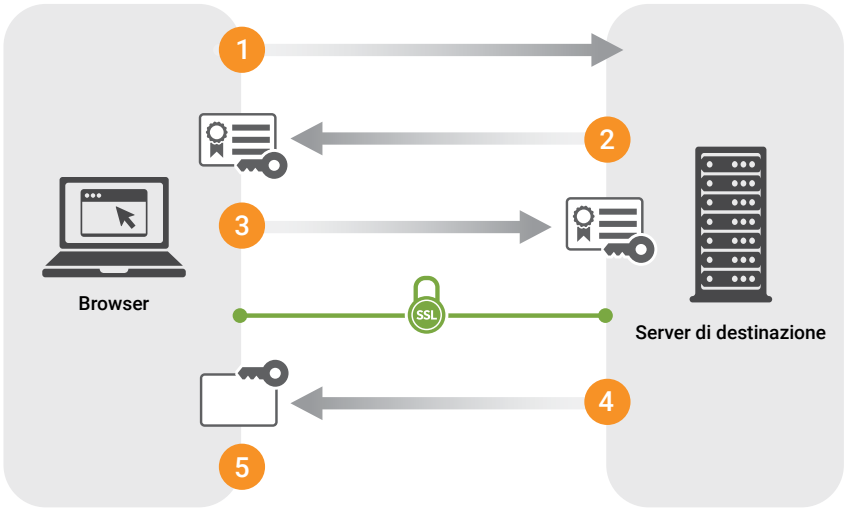
Da aperto a sicuro: come SSL/TLS consente la protezione online

Internet si è evoluta. In passato, la navigazione, su Yahoo, Google, Microsoft o sul sito web dell'università locale, non richiedeva privacy o protezione. Digitando un URL nella barra degli indirizzi del browser si veniva indirizzati direttamente a quel sito, senza che fossero introdotti cookie o deviazioni, e con dati potenzialmente sfruttabili molto limitati o del tutto assenti lungo il percorso. Oggi, condividiamo comunemente informazioni sia personali che private e conduciamo affari sulla stessa rete. Ora *Viviamo* su internet. Anche le nostre stesse abitudini di navigazione sono diventate dati preziosi. Questa modifica richiede una modalità più privata e sicura di interagire con i servizi web.

Inserire una tecnologia di crittografia. La crittografia Secure Sockets Layer (SSL) (e il suo successore Transport Layer Security o TLS) instaura *tunnel sicuri* tra un browser e un sito di destinazione, utilizzando certificati a "chiave pubblica" convalidati da terze parti. Tali certificati e le relazioni che instaurano creano un insieme di *catene di fiducia* interconnesse: "Mi fido di te perché qualcuno di cui mi fido si fida". Quando

un'azienda acquista un tale certificato da un fornitore di fiducia riconosciuto dal browser (ad es. , Verisign, Thawte), quell'azienda diventa un membro fidato di quella catena. Quando si accede a un sito protetto con SSL/TLS, il browser e il sito web si scambiano credenziali (il certificato) e parametri, in modo che la comunicazione successiva sia crittografata. Quella comunicazione, anche se dovesse essere catturata, è incomprensibile per chiunque tranne che per il browser e il server del sito web. I protocolli SSL e TLS forniscono questa funzionalità di crittografia da diversi decenni.

Come funziona l'SSL/TLS in una connessione browser-server



1. Un utente apre un browser e invia una richiesta HTTPS.
2. Il server di destinazione restituisce una chiave pubblica crittografata abbinata al certificato SSL/TLS.
3. Il client browser convalida il certificato, crea e invia una chiave crittografata al server di destinazione. (Se il certificato del server non viene convalidato, la comunicazione termina).
4. Il server di destinazione decodifica la chiave ricevuta e consegna al client i contenuti crittografati (e la chiave).
5. Il client decodifica il contenuto.

Figura 1. Come funziona l'SSL/TLS in una connessione da browser a server di destinazione.

L'SSL/TLS offre tre importanti funzionalità per la navigazione web:

Privacy

I dati contenuti nel tunnel sicuro non possono essere visualizzati o condivisi con un'altra parte.

Fiducia

Esiste la convalida che il browser sta effettivamente parlando al server/sito web prefissato.

Anonimato

I comportamenti di navigazione dell'utente sono nascosti a qualsiasi parte tra l'utente e il server.

Il Transport Layer Security (TLS) e il Secure Sockets Layer (SSL)[1] sono protocolli di rete intesi a creare un tunnel sicuro tra due dispositivi, utilizzando la crittografia. Ciò fornisce comunicazioni sicure su una rete di computer altrimenti pubblica. SSL e TLS proteggono i dati tramite metodi crittografici che utilizzano chiavi sia pubbliche che private per la crittografia e la decrittografia e si basano su certificati per autenticare le parti comunicanti.

[1] https://it.wikipedia.org/wiki/Transport_Layer_Security

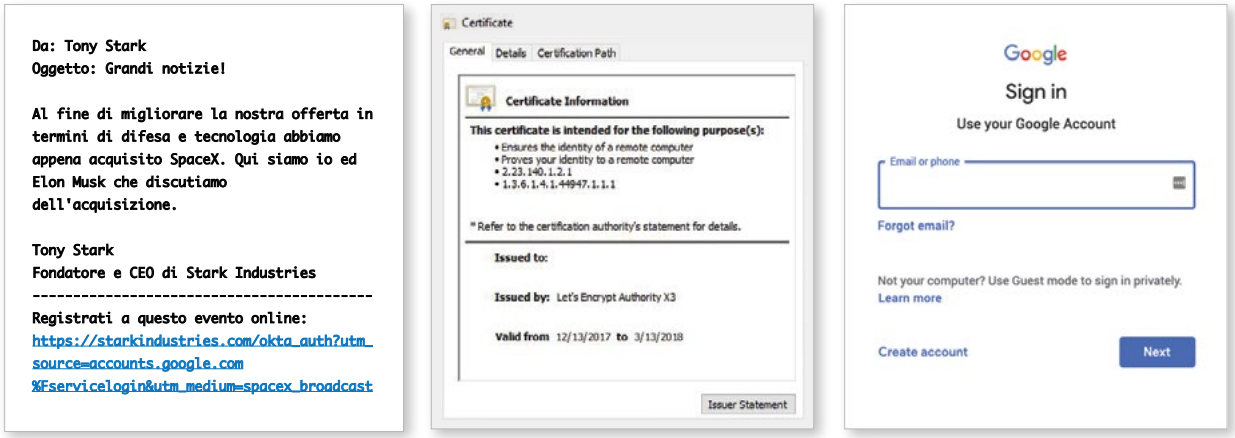
L'anonimato protegge le informazioni sul browser e sul soggetto dietro a esso, ma non sugli indirizzi IP del browser e del server. Questo divario è stato risolto con l'avvento dei proxy anonimi[2] e delle reti di anonimato, come TOR.[3]

Rischio della crittografia n. 1: gli attori malevoli sfruttano la fiducia

La crittografia SSL/TLS offre la sicurezza della privacy: nessuno tra il browser e la destinazione sa cosa si sta guardando o quali dati vengono condivisi, ma ecco la catena della fiducia: I malintenzionati cercano di sfruttare la fiducia (vedere la Figura 1) e hanno reso l'affidabilità intrinseca di SSL/TLS ancora più importante delle capacità di privacy e anonimato del tunnel.

In che modo gli attori malevoli sfruttano la fiducia: esempi di attacchi invisibili

Obiettivi esemplificativi di un attacco nascosto: rubare le credenziali dell'utente, esfiltrare i dati.
(Questi esempi sono stati tutti forniti tramite canali crittografati con SSL).



Spear Phishing
In questo esempio, un attore malevolo impersona un CEO per sollecitare un clic su un URL di un sito dannoso mascherato.

Certificato SSL
La legittimità aumenta con il certificato generato da un'autorità di certificazione gratuita.

Domain Squatting
Dominio dannoso che assomiglia e si comporta in modo simile a uno legittimo. Accesso necessario.

Figura 2. Esempi di come gli attori malevoli sfruttano la fiducia tramite la consegna crittografata con SSL/TLS.

Ad esempio, una semplice ricerca su internet potrebbe non necessitare della crittografia, ma Google la effettua comunque. Anche se i dati potrebbero non essere sensibili, la *certezza* di sapere che si tratta di Google a fornire la pagina offre quell'elemento essenziale di fiducia. La catena di fiducia della

https://en.wikipedia.org/wiki/Anonymizer

https://it.wikipedia.org/wiki/Tor_(software)

crittografia stessa fornisce tale convalida. Come la maggior parte dei siti web moderni, Google oggi offre tutte le sue pagine tramite SSL/TLS con URL "HTTPS". L'era della navigazione a testo aperto "in chiaro" sta finendo. (Con Zscaler ci troviamo in una posizione unica per poter osservare gli andamenti del traffico internet e oltre l'83% del traffico di dati che scorre attraverso Zscaler è ora crittografato con SSL/TLS.[4])

Il modello di tunnel sicuro è, per progettazione, sicuro, ma è comunque sfruttabile, in particolare quando si tratta della fiducia degli utenti. Qualsiasi organizzazione (e persino un individuo) può acquistare un certificato SSL/TLS. Tale organizzazione può utilizzare quel certificato per cooptare o imitare destinazioni internet legittime (o persino componenti di una pagina web legittima), compromettendo a tutti gli effetti un sito con un certificato legittimo. In questo modo, gli attori malevoli ingannano la persona dietro al computer e ottengono l'accesso ai dati di valore degli utenti, che possono poi decodificare, *anche se sono crittografati durante il transito.*Gli attori malevoli si presentano come un'entità degna di fiducia. Poiché il traffico è crittografato, la loro raccolta di dati non viene rilevata e bypassano i controlli o gli strumenti aziendali messi in atto per fermarli.

Rischio della crittografia n. 2: I malintenzionati nascondono malware

L'incremento degli attacchi di phishing, spoofing e ransomware ha eroso la fiducia per internet: come faccio a sapere se sto visitando un sito legittimo? Come faccio a sapere se qualcosa sul sito (pubblicità, articolo, elemento) è stato compromesso? Come faccio a sapere se questo sito apparentemente legittimo ospita un malware crittografato?

Gli attori malevoli spesso compromettono (o impersonano) fornitori di terze parti, come Content Delivery Networks (CDN), che forniscono contenuti a siti legittimi, erogando quindi malware su un sito legittimo che a tutti gli effetti è altrimenti “protetto” da HTTPS.

I malintenzionati usano la crittografia SSL/TLS per nascondere il loro lavoro e la minaccia che rappresentano si sta progressivamente intensificando. Non si tratta però di una nuova minaccia, gli attori malevoli hanno infatti sempre avuto l'opportunità di nascondere malware all'interno di un codice sicuro, è l'economicità soggiacente che è cambiata. Negli ultimi anni, i certificati SSL/TLS *gratuiti* sono diventati prontamente disponibili, riducendo notevolmente i costi (e lo sforzo) per crittografare malware distruttivi.

---

https://www.zscaler.com/threatlabz/encrypted-traffic-dashboard

Con Zscaler, negli ultimi anni, abbiamo assistito a una crescita esponenziale del volume di minacce portate nei tunnel crittografati. Oltre il 54% delle minacce avanzate rilevate viene ora distribuito su canali crittografati SSL/TLS.[5] Ancora più preoccupante è il fatto che, nel 2018, gli attacchi di phishing crittografati con SSL/TLS sono aumentati del 300% .[6]

Gli attori malevoli usano gli stessi protocolli SSL/TLS per crittografare la fonte del loro malware (ad esempio, un sito crittografato "drive-by", purpose-built che ospita il malware) e le comunicazioni in uscita del malware. Tale crittografia presenta l'illusione di dati "affidabili", offrendo agli attori malevoli libero accesso per infiltrarsi nelle imprese, accedere alle risorse e oscurare l'esfiltrazione dei dati.

Rischio della crittografia n. 3: gli attori malevoli mascherano la sottrazione dei dati

Se un attore malevolo esterno riesce a infiltrarsi in una rete aziendale con l'intento di rubare risorse digitali, lo stesso deve affrontare la sfida di riuscire a portare i dati al di fuori del perimetro di sicurezza dell'azienda. A un attore malevolo interno si presenta lo stesso problema: come riuscire a portare le informazioni proprietarie al di fuori dell'organizzazione?

Gli attori malevoli nascondono malware all'interno dei dati crittografati in entrata. In alcuni casi, il malware esplode all'interno di un'organizzazione, infettando i sistemi interni, quindi contatta i server esterni di comando e controllo (C&C) per sottrarre i dati aziendali importanti e portarli all'esterno dell'organizzazione.

La crittografia può mascherare la perdita di dati dolosa (e anche incidenti occasionali). Senza l'ispezione SSL/TLS in uscita, come può un responsabile IT determinare se i dati riservati rimangono privati? L'ispezione SSL/TLS deve affrontare sia il traffico di dati in entrata (tenere fuori I malintenzionati), sia quello in uscita (mantenere le informazioni private all'interno). Nell'esempio in uscita, l'ispezione SSL è fondamentale per prevenire la perdita di dati, nonché per identificare e correggere la vulnerabilita' nella sottrazione dei dati' sugli attacchi zero day.[7]

Equilibrare accesso e sicurezza in una nuova era della privacy

L'evoluzione della connettività Internet preannuncia una nuova era della privacy, dal testo in chiaro alla trasmissione di dati crittografati, dalla fiducia implicita a quella esplicita, che non si riflette solo sulla domanda

---

https://www.zscaler.com/resources/solution-briefs/add-advanced-threat-protection-to-close-your-security-gaps.pdf

https://www.zscaler.com/blogs/research/february-2018-zscaler-ssl-threat-report

https://searchsecurity.techtarget.com/definition/zero-day-vulnerability

dei consumatori per la gestione dei dati privati, ma in orientamenti normativi che definiscono il diritto di un utente alla privacy, come ad esempio il Regolamento generale sulla protezione dei dati (GDPR) europeo,[8] il Personal Information Protection and Electronic Documents Act canadese[9] e diverse leggi sulla privacy negli Stati Uniti esistenti (California, Maine, Nevada) e proposte (Hawaii, Illinois, Massachusetts, Mississippi, New Mexico, New York, Rhode Island, Texas e Washington).

Non tutto il traffico di navigazione o internet è uguale. Nella maggior parte dei casi, la privacy è affidata al singolo soggetto. È probabile che un utente occasionale in uno stato democratico navighi in privato, mentre un utente web che risiede in un luogo governato da un regime autoritario può utilizzare una rete di anonimato come Tor per proteggere le comunicazioni dalla visibilità della censura quando comunica con la famiglia all'estero. In ogni caso, i dati sono di proprietà dell'utente e pochi, con la possibile eccezione di quel governo autoritario, si mostrerebbero contrari a tutelare il diritto alla privacy di ciascun utente. Entrambi gli utenti si assumono il rischio di perdita o intercettazione dei dati, un rischio limitato alle proprie case e ai propri dispositivi.

Tutto questo cambia all'interno di un'azienda o se l'accesso a internet è fornito dal governo. Molti concorderebbero sul fatto che gli utenti aziendali debbano godere di un certo livello di privacy su internet: non c'è ragione per cui le abitudini di acquisto, le destinazioni delle vacanze, gli hobby o le destinazioni di navigazione di un utente dovrebbero diventare visibili agli altri dipendenti. Le varie leggi che regolano la privacy, in molti casi, supportano tale fine. L'SSL/TLS ha consentito quel tipo di privacy e persino l'anonimato di navigazione, per anni.

Tuttavia, quel tipo di privacy che ci si aspetta comporta costi e rischi: possiamo continuare a godere della privacy, se I malintenzionati possono sfruttare quel privilegio per il proprio guadagno? In un contesto aziendale, il rischio non è più solo per il singolo dipendente, ma per l'intera organizzazione. Nel contesto delle capacità della tecnologia di crittografia, i moderni responsabili IT delle aziende devono valutare il rischio di minacce in arrivo in relazione alla promessa di privacy, un delicato atto di bilanciamento tra i diritti del singolo dipendente e la necessita dell'azienda di tutelarsi.

In un'organizzazione, la visione di un diritto alla privacy assoluta è meno chiara. Qualsiasi azienda che utilizza Internet, e, ammettiamolo, si tratta praticamente di tutte le aziende, ha la responsabilità nei confronti dei propri dipendenti, azionisti e clienti di tutelarsi e aderire alle linee guida legali e normative. I responsabili IT utilizzano controlli tecnici e procedurali per prevenire e rilevare attacchi e comportamenti rischiosi. Per ridurre

---

https://eugdpr.org/

https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

il rischio e proteggere la "casa", tali controlli devono essere applicati a tutto il traffico di dati interno, in entrata e in uscita.

L'ambiente normativo può aggiungere complessità alla gestione dei dati aziendali. Alcune giurisdizioni europee richiedono alle società di proteggere i dati personali dei dipendenti per garantire la privacy, e in alcuni casi l'anonimato, della navigazione web personale. Ad esempio, il tedesco Telekommunikationsgesetz[10] ("legge sulle telecomunicazioni" o TKG) è generalmente considerato applicabile alle società che forniscono ai dipendenti l'accesso a internet per uso personale. Il TKG richiede specificamente che gli utenti siano soggetti alla "segretezza delle telecomunicazioni". Richiede inoltre che un'organizzazione protegga adeguatamente il servizio da danni e o intercettazione, e allo stesso tempo protegga adeguatamente i dati di navigazione degli utenti. Le società conformi al TKG devono bilanciare la "segretezza delle telecomunicazioni" degli utenti con la protezione delle risorse.

Secondo un recente Rapporto sulla trasparenza di Google,[11] fino al 93% del traffico del browser Chrome è crittografato. Con gli attori malevoli che creano minacce avanzate tramite canali crittografati per eludere i controlli di sicurezza aziendali, come può un'azienda proteggere sia se stessa che i suoi dati, mantenendo i diritti sulla privacy dei dipendenti in conformità con le normative sulla protezione dei dati?

Aprire il tunnel: decrittografia e ispezione SSL/TLS

In un'azienda, un attacco malware non è limitato a un singolo individuo. Una volta che un utente malintenzionato ha ottenuto l'accesso alla al terminale di un dipendente, può in genere spostarsi altrove ("a est/ovest[12]") nel regno di quel dipendente e infettare altri sistemi e computer all'interno della rete aziendale.

I controlli di sicurezza informatica possono ispezionare facilmente le comunicazioni in testo aperto che entrano o escono da un'organizzazione, ma la crittografia SSL/TLS dei dati in entrata o in uscita complica l'ispezione. È possibile preservare la presunta privacy di un tunnel sicuro, se le minacce crittografate presentano un tale pericolo sia per il singolo utente *che per* l'impresa più grande?

La risposta è SÌ. La lotta al rischio correlato alle minacce crittografate distruttive inizia con l'ispezione dei dati SSL/TLS. Una società ha l'obbligo istituzionale e legale di proteggere i propri beni e ciò include la protezione delle comunicazioni dei propri dipendenti.

---

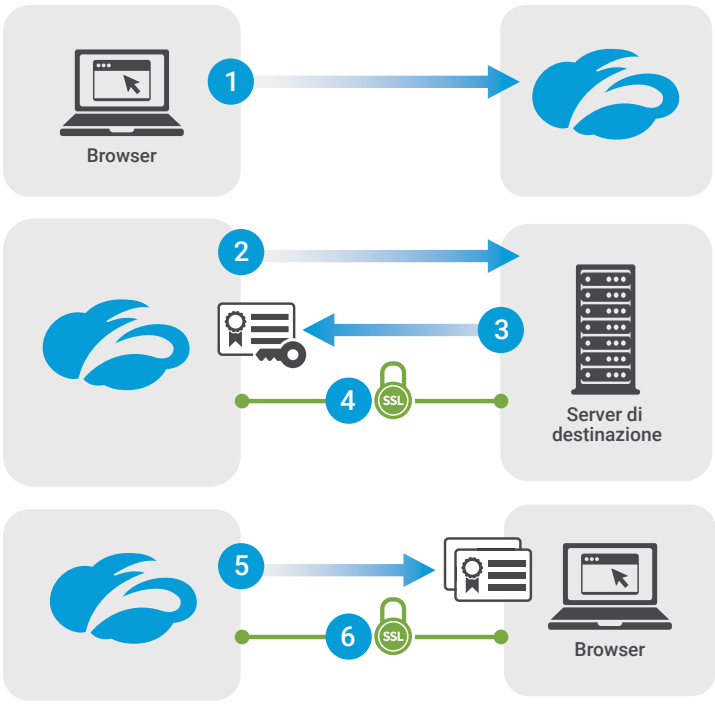
https://germanlawarchive.iuscomp.org/?p=692

https://transparencyreport.google.com/https/overview?hl=it

https://searchnetworking.techtarget.com/definition/east-west-traffic

Per ispezionare i dati SSL/TLS, l'organizzazione deve deviare a tutti gli effetti quella catena di comunicazione di fiducia, interrompendola mediante un tunnel tra il browser e il dispositivo di ispezione, nonché un tunnel successivo tra il dispositivo di ispezione e la destinazione.

Modalità di controllo dei dati crittografati SSL/TLS da parte di Zscaler: flusso di lavoro



1. Un utente apre un browser e invia una richiesta HTTPS.
2. Il servizio Zscaler intercetta la richiesta HTTPS. Attraverso un tunnel SSL separato, il servizio invia la propria richiesta HTTPS al server di destinazione e conduce negoziazioni SSL.
3. Il server di destinazione invia al servizio Zscaler il suo certificato con la sua chiave pubblica.
4. Il servizio Zscaler e il server di destinazione completano l'handshake SSL. I dati dell'applicazione e i messaggi successivi vengono inviati attraverso il tunnel SSL.
5. Il servizio Zscaler conduce negoziazioni SSL con il browser dell'utente. Invia al browser il certificato intermedio Zscaler o il root intermedio personalizzato dell'organizzazione, nonché un certificato server firmato dall'autorità di certificazione intermedia di Zscaler. Il browser convalida la catena di certificati nell'archivio certificati del browser.
6. Il servizio Zscaler e il browser completano l'handshake SSL. I dati dell'applicazione e i messaggi successivi vengono inviati attraverso il tunnel SSL.

Una volta completato l'handshake, il motore delle policy di Zscaler valuta le regole della policy SSL/TLS, applica blocchi/bypass globali, controlla i certificati di emittenti non attendibili e visualizza le notifiche (se necessario).

Figura 3. Flusso di lavoro della modalità di controllo dei dati crittografati SSL/TLS da parte di Zscaler.[13]

In questo esempio, l'ispezione non interrompe la relazione di fiducia tra individuo e fonte. Il dipendente ripone fiducia nell'organizzazione che fornisce il dispositivo di navigazione, piuttosto che nell'origine dei dati. Il dispositivo di ispezione "vedrà" la destinazione e il contenuto dei dati.

Quindi la domanda rimane: *un'organizzazione può svolgere questa essenziale funzione protettiva, pur rispettando le altre due funzionalità della crittografia, anonimato e privacy?* Operando nel modo corretto, assolutamente sì. La minaccia rappresentata da malware crittografato rende l'ispezione SSL/TLS un mandato di controllo della sicurezza informatica per l'impresa moderna e le organizzazioni devono bilanciare le proprie esigenze di sicurezza con i diritti alla privacy dei propri dipendenti. Un'organizzazione che non controlla il traffico SSL/

13 https://help.zscaler.com/zia/about-ssl-inspection

TLS si espone a rischi inutili, tra cui perdita di informazioni personali, proprietà intellettuale rubata, spionaggio industriale o persino infezioni da ransomware. (La percentuale di organizzazioni che ispezionano i dati crittografati è cresciuta: tra i clienti aziendali di Zscaler, quasi la metà dei quali residenti in Europa, il 72% controlla il traffico SSL/TLS).

In un'azienda, l'anonimato individuale online può essere preservato... fino a un certo punto

Nel valutare i modelli di ispezione SSL/TLS, dobbiamo prima guardare all'anonimato. In alcune organizzazioni, la fornitura dell'accesso a internet è un diritto concesso e regolato da un contratto di lavoro dipendente, stabilito e controllato dalla politica aziendale al pari del comportamento dei dipendenti sul posto di lavoro.

L'applicazione di questa politica richiede un monitoraggio. Un tunnel SSL/TLS espone la sua origine e destinazione a qualsiasi cosa e a chiunque tra browser e server. La registrazione di queste transazioni è essenziale per l'analisi comportamentale e il rilevamento degli incidenti. Le revisioni dei registri possono aiutare a garantire l'adesione alle policy e contribuire al miglioramento continuo dell'efficacia delle policy. (L'analisi retrospettiva dei registri viene persino spesso utilizzata nelle indagini penali).

Con un protocollo di ispezione SSL/TLS in atto sul posto di lavoro, i dipendenti non devono aspettarsi un completo anonimato durante la navigazione online, poiché l'accesso a internet è un privilegio concesso dall'organizzazione ai propri dipendenti e regolato dal contratto di lavoro di ciascun dipendente. Per proteggere le risorse aziendali, l'organizzazione può scegliere di tenere traccia degli URL di destinazione, del comportamento di navigazione e dell'accesso al dispositivo dell'utente. La politica aziendale di un'organizzazione stabilisce un limite per tale uso di internet, nonché delle ripercussioni per la violazione di tale politica.

Per essere chiari, l'ispezione SSL/TLS non significa la fine dell'anonimato individuale online. Le aziende possono bilanciare le esigenze di privacy dei dipendenti con misure di sicurezza informatica aggiornate. È necessario un monitoraggio completo dei dati per effettuare un'efficace ispezione SSL/TLS, ma l'accesso ai dati risultanti da tale ispezione può essere limitato. I dipendenti possono rimanere anonimi durante l'analisi dei registri, anche durante le indagini e la valutazione (ad esempio, revisione e risposta a potenziali violazioni delle politiche), fino a quando non si presenta la necessità di coinvolgimento. Questo anonimato viene in genere indicato come indicizzazione dei registri o offuscamento.

A volte, i responsabili IT dovranno ispezionare e analizzare i registri per intero. Ad esempio, un responsabile della sicurezza informatica esaminerà regolarmente i registri per identificare i callback di malware tramite tunnel SSL/TLS. Quando ne viene trovato uno, la sicurezza IT deve attivare un flusso di lavoro per la pulizia

della macchina, coinvolgendo il dipendente per eliminare il malware dallo specifico dispositivo infetto (o persino riformattarlo o distruggerlo). Questo processo può essere implementato per supportare un " approccio a quattro occhi,[14]" con un amministratore della sicurezza e un rappresentante dei lavoratori (ad esempio un dirigente dell'associazione dei dipendenti o magari un consulente esterno) che esaminano contemporaneamente i registri della console.

Quando i registri individuano un'infezione, un singolo utente aziendale non può rimanere anonimo e deve essere "reso noto" per rivelare l'identità, in modo che la sicurezza IT possa rimediare alla minaccia prima che influisca sull'organizzazione a livello più ampio.

L'esfiltrazione dei dati, ossia la "fuoriuscita" indesiderata di dati da un'organizzazione, rappresenta un'altra situazione che può richiedere l'eliminazione dell'offuscamento. In genere, un processo di revisione dei registri può determinare che il traffico SSL/TLS precedente e non filtrato possa effettivamente essere destinato a un sito web di destinazione criminale o non approvato. In questo caso, potrebbe essere necessario coinvolgere le forze dell'ordine e rendere noti i dati per supportare un'indagine.

I dipendenti devono aspettarsi che la navigazione sia anonima in correlazione ai colleghi aziendali, ai dirigenti e persino ai team di sicurezza aziendale, fintantoché un rischio o una minaccia per le organizzazioni non fa scattare la necessità di rimuovere tale anonimato. Nelle situazioni di cui sopra, è essenziale che l'organizzazione abbia un'*esigenza documentata* per eliminare l'offuscamento, attraverso una Politica di utilizzo accettabile (Acceptable Use Policy, AUP) che spesso viene incorporata nel contratto di lavoro del dipendente. L'uso di internet tramite dispositivi o reti aziendali dovrebbe essere concesso solo quando accettato dal dipendente (in genere all'inizio del rapporto di lavoro).

Proteggere i dati: decodifica SSL/TLS in un ambiente regolato dal GDPR

A prima vista, "l'apertura" del tunnel di comunicazione crittografata SSL/TLS, per l'ispezione dei dati e l'applicazione delle policy, potrebbe far credere che i dati non siano più privati. Questa è una preoccupazione comune, sollevata dai dipartimenti legali aziendali e dai sostenitori della privacy. Alcuni additano il GDPR come base per sostenere che questo regolamento vieta a un'organizzazione di decrittografare e ispezionare i dati personali crittografati con SSL/TLS. A nostro avviso, questo non è corretto.

Anche le sessioni normali e non crittografate richiedono che vengano applicati esattamente gli stessi obblighi a tutte le parti (ISP, provider di rete, proxy di memorizzazione nella cache) tra il browser e il server. Le linee guida del GDPR impongono *comunque* a ciascuna parte di trattare i dati personali con lo stesso livello di

---

https://whatis.techtarget.com/definition/four-eyes-principle

sensibilità. La crittografia non modifica gli obblighi imposti a un titolare del trattamento dei dati o persino a un responsabile del trattamento. A ridurre ulteriormente questa tesi errata va aggiunto che i dati personali vengono elaborati dal dispositivo del dipendente fornito dall'azienda in modo non cifrato, *anche quando si utilizza un tunnel crittografato.* Non ci può essere alcuna garanzia assoluta di privacy in tale contesto aziendale.

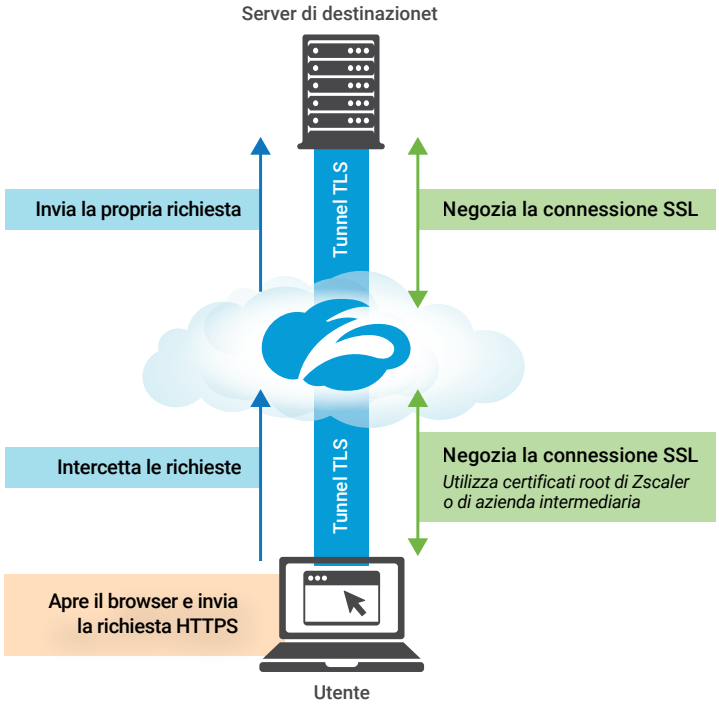
L'ispezione SSL/TLS viene utilizzata per applicare la politica e identificare potenziali minacce nascoste nel traffico di dati crittografati. Per identificare le minacce, un dispositivo di ispezione decodifica i dati, li esamina in base a una serie di firme "note come malevole" e ispeziona il flusso di dati per determinare il rischio di minacce, come malware in entrata o dati aziendali che fuoriescono i modo anomalo. Se i dati non presentano alcuna minaccia, vengono impacchettati nuovamente e inviati nel percorso di transizione. Se eseguita in questo modo, l'ispezione SSL/TLS non riduce la privacy dei dipendenti. I dati non vengono condivisi con nessuno, né vengono utilizzati in modo tale da violare i diritti dell'interessato. Il processo di ispezione SSL/TLS protegge le risorse organizzative dalla minaccia di attacco, senza incidere sui diritti individuali alla privacy.

Zscaler offre un'ispezione SSL/TLS completa per proteggere il traffico dei dati dei clienti e fornire un "perfect forward secrecy" (PFS).[15]Zscaler non archivia mai i dati su disco: una volta completata l'ispezione dei dati, il flusso dei dati continua senza ostacoli, senza che alcuna registrazione dei dati di origine venga conservata oltre che nel registro della transazione stessa. Oltre a proteggere i dati in transito, Zscaler protegge tutte le chiavi SSL/TLS durante l'ispezione. (Fare riferimento alle Figure 3 e 4 per scoprire come Zscaler controlla i dati crittografati con SSL/TLS. Scopri di più su come Zscaler protegge tutti i dati e tutte le chiavi di crittografia qui[16])

https://www.zscaler.com/blogs/corporate/tls-13-busting-myths-and-debunking-fear-uncertainty-doubt

https://help.zscaler.com/zia/safeguarding-ssl-keys-and-data-collected-during-ssl-inspection

Modalità di ispezione dei dati crittografati con SSL/TLS da parte di Zscaler: flusso di lavoro



Zscaler funge da inline SSL proxy. Termina la connessione SSL stabilita dal client e stabilisce una nuova connessione SSL con il server. Dal punto di vista di un client, Zscaler diventa il server e dal punto di vista del server SSL originale, Zscaler diventa il client.

Ispezione SSL/TLS di Zscaler basata su cloud:

- Scalabilità per ispezionare tutto il traffico
- Semplificazione della gestione dei certificati
- Semplificazione dell'amministrazione della rete
- Protezione del traffico con crittografie AES/GCM/ECDHE per PFS
- Implementazione di controlli efficaci delle politiche
- Mantenimento della sicurezza dei dati dell'utente (poiché rimangono effimeri e non vengono mai archiviati sul cloud)

Figura 4. Modello di proxy inline della modalità di ispezione di Zscaler dei dati crittografati con SSL/TLS.[17]

È utile esaminare il diritto alla privacy come un risultato e rivedere il modo in cui tale risultato viene raggiunto, piuttosto che chiarire le singole fasi che sembrano avere un impatto sullo stesso. L'ispezione del traffico e il risultato binario del blocco o non blocco non sono uguali all'accesso, al monitoraggio o alla memorizzazione dei dati crittografati.

L'ispezione SSL/TLS completa rafforza il GDPR aziendale e la conformità generale per il rispetto della privacy, perché aiuta a proteggere la privacy dell'organizzazione, i suoi dipendenti e le sue risorse. Senza l'ispezione SSL/TLS, il rischio di esporre dati personali interni (PII) è maggiore, sottoponendo l'organizzazione al rischio di non essere conforme.

17 https://help.zscaler.com/zia/about-ssl-inspection

Le normative sulla protezione dei dati supportano la privacy e la sicurezza

Le normative sulla privacy dei dati, in particolare la legislazione europea come il GDPR,[18] il Network and Information Systems Regulation 2018 (NIS) britannico[19] e il TKG[20]sono stati messi in atto per garantire alle organizzazioni la protezione dei dati personali, preservando al contempo un accesso gratuito ed equo a internet. Queste normative bilanciano i diritti degli individui con i requisiti aziendali di implementare misure di sicurezza per proteggere sistemi e dati. Ad esempio, i regolamenti TKG impongono alle organizzazioni di applicare "precauzioni tecniche di protezione[21]" per prevenire la perdita di dati e respingere l'attacco esterno. L'NIS afferma esplicitamente che un'organizzazione deve disporre di adeguate misure di sicurezza per garantire che i sistemi (e i dati al loro interno) non possano essere compromessi. Inoltre l'articolo 5 del GDPR[22] stabilisce che tali organizzazioni devono elaborare i dati

> *...in modo da garantire un'adeguata sicurezza dei dati personali, inclusa la protezione dal trattamento non autorizzato o illecito e da perdite, distruzioni o danni accidentali, utilizzando adeguate misure tecniche o organizzative.*

Inoltre, l'articolo 32 del GDPR (Sicurezza del trattamento) impone alle organizzazioni l'obbligo di implementare misure di sicurezza per il trattamento dei dati personali che "assicurino un livello di sicurezza adeguato al rischio". Le ispezioni SSL/TLS sono altamente "appropriate", data l'entità dei rischi per la sicurezza che mirano a mitigare.

Le minacce si nascondono nel traffico crittografato. Senza ispezione, non è possibile che un'azienda possa distinguere tra dati crittografati con SSL/TLS "buoni" e "cattivi". Nessuna impresa può adempiere ai mandati di privacy e sicurezza di TKG, NIS e GDPR, per non parlare di proteggere i propri dipendenti e gli interessi aziendali, senza un'ispezione completa del traffico dei dati crittografati.

---

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-gdpr/

http://www.legislation.gov.uk/uksi/2018/506/contents

https://germanlawarchive.iuscomp.org/?p=692

https://germanlawarchive.iuscomp.org/?p=692

https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016R0679#d1e1807-1-1

Morale: come implementare l'ispezione SSL/TLS nella propria azienda

Le ragioni di sicurezza e protezione dei dati alla base dell'ispezione SSL/TLS nell'azienda sono valide e irreprensibili. I responsabili IT devono utilizzare l'ispezione SSL/TLS per proteggere i dati, i dipendenti e le risorse della propria organizzazione: la mancata osservanza di questa precauzione può comportare danni irreparabili e persino l'inadempimento dei propri obblighi.

I responsabili IT che desiderano introdurre l'ispezione SSL/TLS nella propria organizzazione devono tenere conto di alcune importanti considerazioni:

1. **Informare i dipendenti.**
   - Assicurarsi che sia in atto un'AUP valida e che i relativi criteri siano applicati al proxy/filtro dei contenuti.
   - Garantire che tutti i dipendenti siano esplicitamente concordi con l'AUP, di solito mediante il proprio contratto di lavoro.
   - Garantire che i dipendenti siano informati su ciò che viene inteso come dato personale e per quanto tempo tali dati vengono conservati dall'organizzazione.
   - Garantire che ai dipendenti venga comunicato in modo preciso quali dati vengono ispezionati, in modo da poter prendere decisioni informate su ciò che fanno durante l'utilizzo delle risorse aziendali.
   - Ottenere l'accordo e il supporto da parte dei consigli dei lavoratori e/o dei sindacati, dimostrando che l'ispezione SSL/TLS è effettivamente a vantaggio dei dipendenti.
   - Rendere noto ciò viene fatto e come viene fatto.

2. **Scegliere una base legale per l'elaborazione dei dati ai sensi del GDPR.** Il regolamento non è il nemico qui: se un'impresa è soggetta al NIS o regolamenti simili, la base legale è "obbligo di legge"; pertanto, come notato in precedenza, un'impresa ha un "interesse legittimo" nella protezione dell'organizzazione e dei propri beni.

3. **Ottenere consulenza legale e sulla privacy da un team interno o da esperti esterni, ma essere pronti ad argomentare.** Ad esempio, alcuni avvocati e professionisti della privacy potrebbero non comprendere appieno i servizi forniti dai venditori o non avere la competenza tecnica per giudicare se le misure di sicurezza sono appropriate in relazione al rischio.

4. **Garantire che processi e controlli siano efficaci e appropriati.**
    - Offuscare o nascondere in altro modo i dati dagli utenti normali, assicurarsi che questi siano disponibili solo sulla base della "necessità di conoscere".
    - Garantire che vi sia rigore e un processo documentato per la revisione dei dati personali.
    - Rivedere e applicare questo flusso di lavoro su base regolare.
    - Conservare i dati per il periodo di tempo designato ed eliminarli in seguito.
    - Mantenere i dati al sicuro, durante il periodo in cui sono posseduti dall'azienda.

Ispezione SSL/TLS: il modo giusto per garantire l'ottemperanza delle normative

L'ispezione SSL/TLS costituisce l'insieme delle "misure di sicurezza appropriate" per proteggere la privacy dell'azienda, i suoi dipendenti e le sue risorse. L'ispezione SSL/TLS protegge le organizzazioni dalla minaccia di attacco, bilanciando al contempo i diritti di privacy individuale e, in tal modo, rafforza l'ottemperanza delle normative da parte di tali organizzazioni.

Le minacce crittografate sono tangibili, distruttive, virulente e in (esponenziale) aumento di volume. I responsabili IT aziendali che scelgono di non decrittografare il traffico mettono a rischio sia la privacy dei loro utenti, sia le risorse dell'azienda, rischiando inoltre di non ottemperare alle varie normative sulla protezione dei dati. In questa era moderna, i responsabili IT devono utilizzare l'ispezione SSL/TLS per combattere i rischi di sicurezza per l'azienda e preservare la privacy dei propri dipendenti e utenti.

Informazioni su Zscaler

Zscaler è stata fondata nel 2008 su un concetto semplice ma fondamentale: dato che le applicazioni si spostano sul cloud, anche la sicurezza deve spostarsi lì. Oggi stiamo aiutando migliaia di organizzazioni globali a trasformarsi per operare sul cloud.