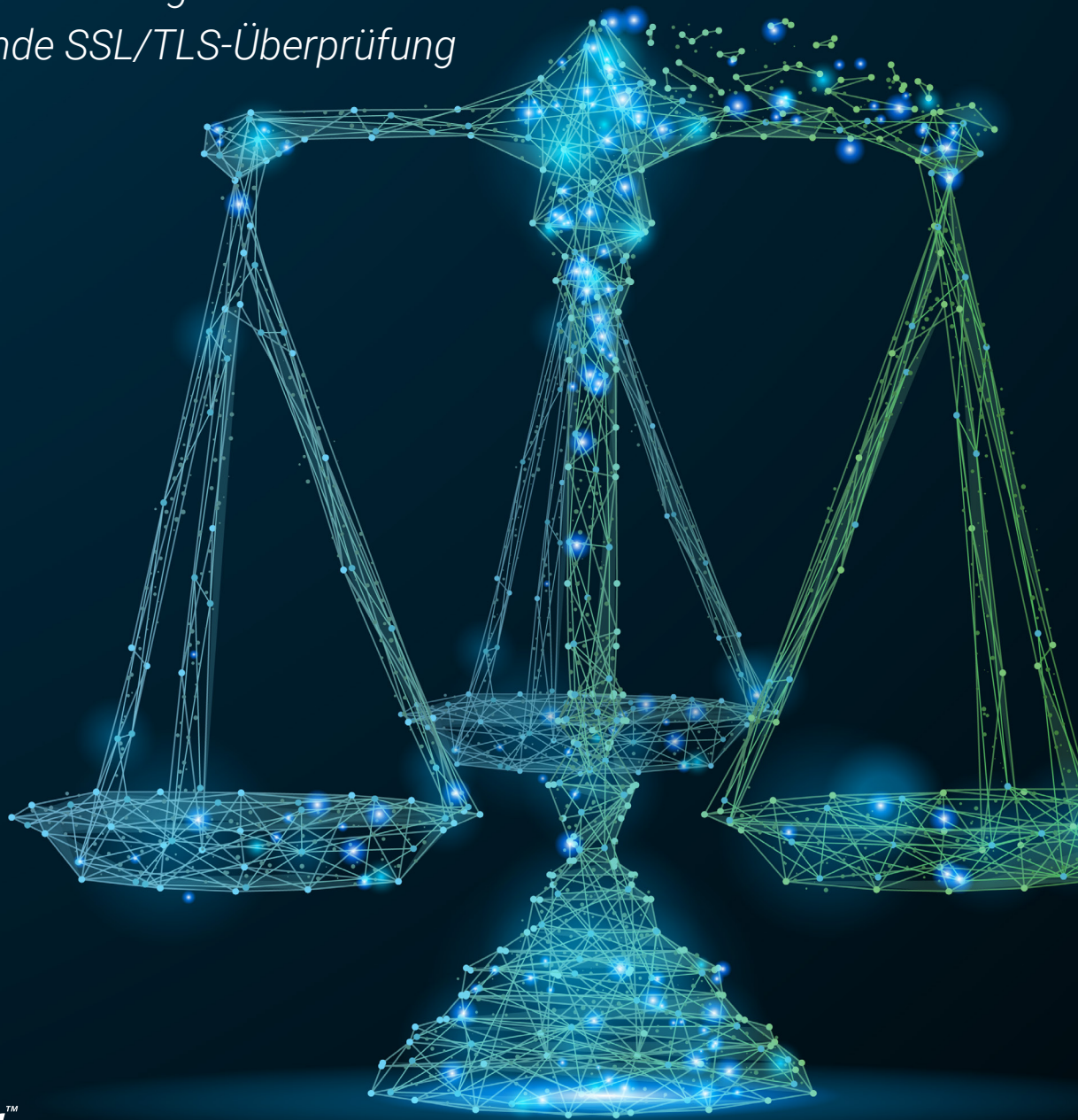
Verschlüsselung, Privatsphäre & Datenschutz: Ein Balanceakt

Geschäfts-, Datenschutz- und Sicherheitsanforderungen für umfassende SSL/TLS-Überprüfung



zscaler™

Abstrakt

SSL/TLS-Verschlüsselung mittels Public-Key-Verfahren ist der Industriestandard für Datenschutz und wird für einen Großteil der Web-Transaktionen im Internet angewendet. Diese sichere Verschlüsselung schützt privilegierte Daten während der Übertragung und gibt Benutzern Vertrauen und Anonymität. Die Methode deckt jedoch auch Betrüger, die das Vertrauen und die Anonymität von SSL/TLS missbrauchen, um ihre Aktivitäten zu verschleiern.

IT-Verantwortliche von Unternehmen müssen umfassende SSL/TLS-Überprüfungsmethoden anwenden, um die in verschlüsseltem Traffic verborgenen Risiken zu minimieren. Dieses Whitepaper untersucht das Risiko von verschlüsselten Bedrohungen, beleuchtet, welche Auswirkungen die Verwaltung dieses Risikos auf Geschäft, Datenschutz und Sicherheit hat und präsentiert konstruktive Maßnahmen zur Ausbalancierung von Sicherheitsansprüchen einerseits und Datenschutzrechten von Mitarbeitern andererseits. Letztendlich schützen IT-Verantwortliche ihre Organisation am besten vor Bedrohungen und Angriffen, wenn sie die Rechte der einzelnen Mitarbeiter sicherstellen.

Das Internet war früher viel einfacher – ein offener Spielplatz für die technisch versierte Elite...

Heutzutage ist es zu dem Ort geworden, an dem ein Großteil des modernen Geschäfts- und Privatlebens stattfindet. Mit der Allgegenwart entstehen neue Risiken. Ein „Internet für alle" ist naturgemäß auch eine Oase für Betrüger, die diejenigen von uns ausnutzen wollen, die das Internet zur Abwicklung von Geschäften und zur Erledigung alltäglicher Dinge verwenden.

Privilegierte Daten müssen geschützt werden, insbesondere bei der Übertragung. Verschlüsselung ist die praktischste Methode hierfür. Mit branchenüblichen SSL/TLS-Verschlüsselungsprotokollen kodierte Daten können von Eindringlingen praktisch nicht (sprich: erschwinglich) dekodiert werden. (Siehe Abbildung 1 sowie Verweis „Transport Layer Security [TLS] und Secure Sockets Layer [SSL] in der Seitenleiste.) Verschlüsselung trägt auch zum Vertrauensaufbau und zur Wahrung der Anonymität bei. Diese Kombination von Funktionen macht SSL/TLS-Verschlüsselung zum idealen Schutz der Internetkommunikation, vom einfachen Web-Browsing bis zum E-Commerce-Einkauf.

In der heutigen Geschäftswelt ist es unerlässlich, die Unternehmensressourcen zu schützen *und* die Privatsphäre des Einzelnen zu wahren. SSL/TLS erfüllt beide scheinbar gegensätzlichen Aufgaben. In falschen Händen können SSL/TLS-Technologien allerdings gefährlich sein. Was passiert, wenn Betrüger damit Malware verschlüsseln und ihre Aktivitäten verbergen? Wie kann das moderne Unternehmen diese Bedrohungen bekämpfen?

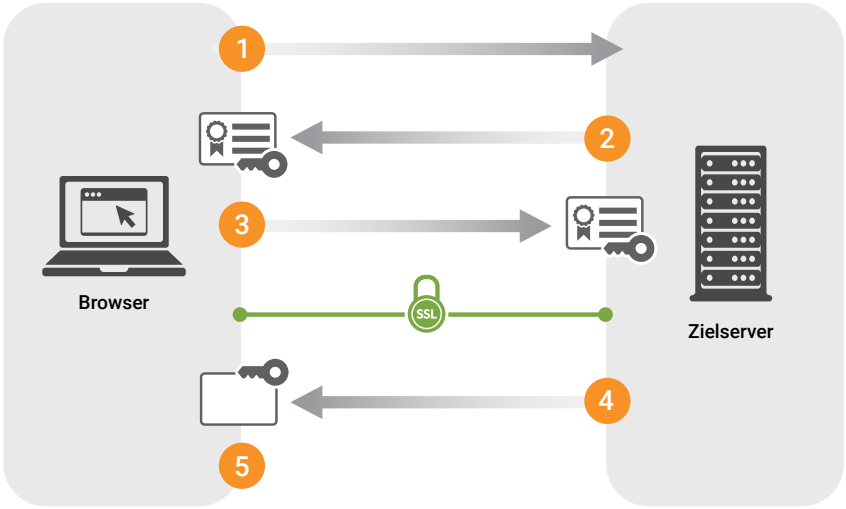
Von offen zu sicher: Wie SSL/TLS Online-Schutz ermöglicht

Das Internet hat sich weiterentwickelt. Früher war für das Browsing – ob zu Yahoo, Google, Microsoft oder der lokalen Website Ihrer Universität – weder Privatsphäre noch Schutz erforderlich. Nach Eingabe einer URL in die Adressleiste des Browsers gelangten Sie direkt zur betreffenden Seite, ohne dass dabei Cookies und Umwege eingeführt oder potenziell ausnutzbare Daten ausgetauscht wurden. Heutzutage teilen wir üblicherweise sowohl persönliche als auch private Informationen und betreiben Geschäfte über dasselbe Netzwerk. Wir leben im Internet. Sogar unsere Browsing-Gewohnheiten selbst sind zu wertvollen Daten geworden. Diese Veränderung erfordert eine privatere und sicherere Art der Interaktion mit Webdiensten.

Der Einsatz von Verschlüsselungstechnologie. Bei der Verschlüsselung mittels Secure Sockets Layer (SSL) und deren Nachfolger Transport Layer Security (TLS) werden *sichere Tunnel* zwischen Browser und Ziel-Website eingerichtet, die von Dritten validierte „Public-Key"-Zertifikate verwenden. Diese Zertifikate und die daraus resultierenden Beziehungen bilden eine Reihe von miteinander verknüpften *Vertrauensketten*: „Ich

vertraue Dir, weil jemand, dem ich vertraue, Dir vertraut." Wenn ein Unternehmen ein solches Zertifikat von einem vom Browser anerkannten Vertrauensanbieter erwirbt (z. B. Verisign, Thawte), wird dieses Unternehmen ein vertrauenswürdiges Mitglied der Kette. Wenn Sie zu einer per SSL/TLS geschützten Website navigieren, tauschen Browser und Website Berechtigungsnachweise (das Zertifikat) und Parameter aus, sodass die folgende Kommunikation verschlüsselt wird. Selbst wenn diese Kommunikation erfasst wird, ist sie für niemanden außer für den Browser und den Website-Server verständlich.

Wie SSL/TLS in einer Verbindung zwischen Browser und Server funktioniert



1. Ein Benutzer öffnet einen Browser und sendet eine HTTPS-Anfrage.
2. Der Zielserver schickt einen kodierten öffentlichen Schlüssel zusammen mit einem SSL/TLS-Zertifikat zurück.
3. Der Browser-Client validiert das Zertifikat, erstellt einen kodierten Schlüssel und sendet diesen an den Zielserver zurück. (Bei Nichtbestätigung des Zertifikats wird die Kommunikation beendet.)
4. Der Zielserver dekodiert den erhaltenen Schlüssel und übermittelt kodierten Inhalt (und Schlüssel) an den Client.
5. Der Client entschlüsselt den Inhalt.

Abbildung 1. Wie SSL/TLS in einer Verbindung vom Browser zum Zielserver funktioniert.

SSL/TLS bietet drei wichtige Funktionen für das Web-Browsing:

Datenschutz

Daten innerhalb des sicheren Tunnels können weder gesehen noch an andere Personen weitergegeben werden.

Vertrauen

Es ist verifiziert, dass der Browser tatsächlich mit dem/der beabsichtigten Server/Website kommuniziert.

Anonymität

Das Browser-Verhalten der Benutzer ist für alle Drittparteien zwischen Benutzer und Server unsichtbar.

Transport Layer Security (TLS) und Secure Sockets Layer (SSL)[1] sind Netzwerkprotokolle zur Erstellung eines sicheren Tunnels zwischen zwei Geräten mittels Verschlüsselung. Dies ermöglicht eine sichere Kommunikation über ein ansonsten öffentliches Computernetzwerk. SSL und TLS schützen Daten mithilfe von Verschlüsselungsmethoden, die sowohl öffentliche als auch private Schlüssel für Kodierung und Dekodierung verwenden und Genehmigungen aufgrund von Zertifikaten der Kommunikationspartner erteilen.

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

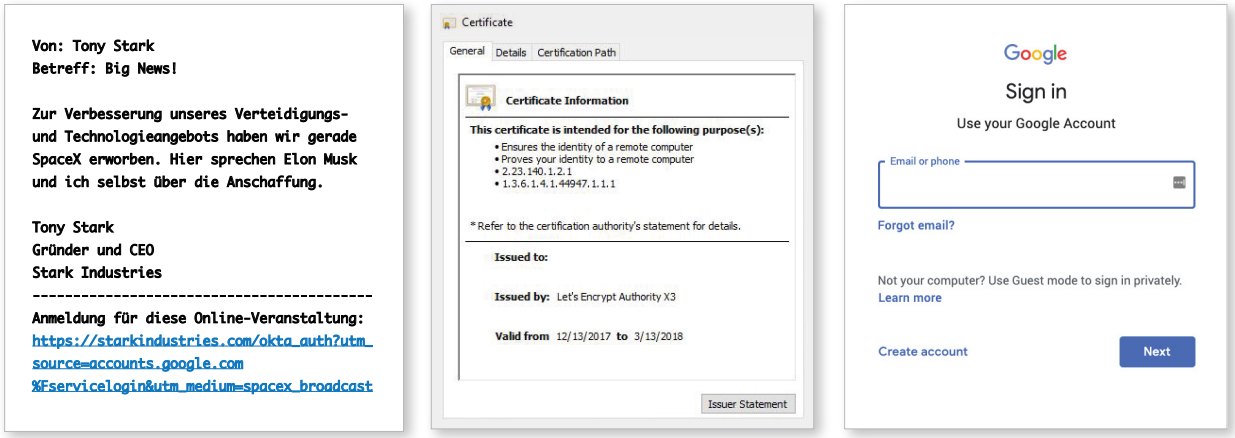
Anonymität schirmt zwar Informationen über den Browser und die Person dahinter ab, nicht jedoch die IP-Adressen von Browser und Server. Diese Lücke soll durch die Einführung von anonymisierenden Proxies geschlossen werden[2] und Anonymitäts-Netzwerke wie TOR.[3]

Verschlüsselungsrisiko #1: Betrüger missbrauchen Vertrauen

SSL/TLS-Verschlüsselung schützt Ihre Privatsphäre: niemand zwischen Ihrem Browser und Ihrem Ziel weiß, was Sie sich ansehen oder welche Daten ausgetauscht werden. Bedenken Sie jedoch vor allem die Vertrauenskette – Betrüger versuchen, Vertrauen zu missbrauchen (Siehe Abbildung 1) – und legen Sie deshalb auf das inhärente Vertrauen von SSL/TLS noch größeren Wert als auf die Datenschutz- und Anonymitätsfunktionen des Tunnels.

Wie Betrüger Vertrauen missbrauchen – Beispiele für heimliche Angriffe

Beispiele für Ziele von heimlichen Angriffen: Diebstahl von Zugangsberechtigungen und Exfiltration von Daten.
(Diese Angriffe finden alle über SSL-verschlüsselte Kanäle statt.)



Spear Phishing
In diesem Beispiel gibt sich ein Betrüger als CEO aus, um für Klicks auf dem URL einer getarnten schädlichen Website zu werben.

Die Legitimität des SSL
Zertifikats wird mittels eines Zertifikats von einer kostenlosen Zertifikatsstelle untermauert.

Domain Squatting
Schädliche Domain, die einer legitimen ähnlich sieht und sich wie diese verhält. Login erforderlich.

Abbildung 2. Beispiele dafür, wie Betrüger über SSL/TLS-verschlüsselte Bereitstellung Vertrauen missbrauchen.

Eine einfache Internetsuche mag zwar keine Verschlüsselung benötigen, aber Google führt diese dennoch durch. Selbst wenn es sich nicht um sensible Daten handelt, sorgt die *Gewissheit*, dass Google die Seite betreut, für das wesentliche Vertrauenselement. Dieselbe Vertrauenskette liefert die Validierung für die Verschlüsselung. Wie alle modernen Websites stellt Google inzwischen

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

https://en.wikipedia.org/wiki/Tor_(anonymity_network)

alle seine Seiten per SSL/TLS mit „HTTPS“ URLs bereit. Das Zeitalter des offenen Browsing „im Klartext“ geht zu Ende. (Hier bei Zscaler sind wir in der einzigartigen Lage, Trends beim Internet-Traffic zu beobachten, und mehr als 83 % des Datenverkehrs, der durch Zscaler fließt, wird inzwischen über SSL/TLS verschlüsselt.[4])

Das Tunnelmodell ist im Prinzip sicher. Aber es ist trotzdem ausnutzbar, besonders im Hinblick auf vertrauenswürdige Benutzer. Jede Organisation (und selbst eine Einzelperson) kann ein SSL/TLS-Zertifikat erwerben. Mit diesem Zertifikat können legitime Internetziele (oder sogar Komponenten einer legitimen Website) mitgenutzt oder imitiert werden. Auf diese Weise wird eine Website mithilfe eines legitimen Zertifikats effektiv kompromittiert. Betrüger täuschen so den Menschen hinter dem Computer und erhalten dadurch Zugang zu wertvollen Benutzer-Daten, die sie anschließend dekodieren, *selbst wenn die Daten in verschlüsselter Form übertragen werden.* Die Betrüger geben sich als vertrauenswürdig aus. Da der Traffic verschlüsselt ist, bleibt ihre Datenerfassung unentdeckt, und sie umgehen Kontrollen und Tools von Unternehmen, durch die sie gestoppt werden sollen.

Verschlüsselungsrisiko #2: Betrüger verstecken Malware

Die Zunahme von Angriffen durch Phishing, Spoofing und Ransomware hat das Vertrauen in das Internet untergraben: Woher weiß ich, dass ich eine legitime Website ansehe? Woher weiß ich, dass bestimmte Inhalte auf dieser Website (Werbung, Artikel, Elemente) nicht kompromittiert sind? Woher weiß ich, dass diese scheinbar legitime Website keine verschlüsselte Malware enthält?

Betrüger kompromittieren (oder imitieren) häufig Drittanbieter wie Content Delivery Networks (CDNs), die Inhalte auf legitimen Websites bereitstellen, und schmuggeln auf diese Weise Malware auf eine legitime Website, die ansonsten in jeder Hinsicht HTTPS-„gesichert“ ist.

Betrüger nutzen SSl/TLS-Verschlüsselung zum Verbergen ihrer Aktivitäten, und die durch sie verursachte Gefahr nimmt ständig zu. Dies ist keine neue Bedrohung. Betrüger fanden schon immer Wege, Malware in einem sicheren Code zu verstecken. Es ist die Marktsituation, die sich verändert hat. In den letzten Jahren sind *kostenlose* SSL/TLS-Zertifikate leicht verfügbar geworden, was die Kosten (und den Aufwand) für die Verschlüsselung destruktiver Malware erheblich verringert.

Hier bei Zscaler haben wir in den letzten Jahren eine exponentielle Zunahme von Bedrohungen in verschlüsselten Tunneln beobachtet. Mehr als 54% aller erkannten Advanced Threats werden inzwischen über SSL/TLS verschlüsselte Kanäle übertragen.[5] Noch besorgniserregender ist, dass SSL/TLS verschlüsselte Phishing-Angriffe 2018 um 300% gestiegen sind.[6]

---

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

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

Betrüger verwenden dieselben SSL/TLS-Protokolle, um die Quelle ihrer Malware (z.B. eine speziell für diesen Zweck erstellte verschlüsselte „Drive-by-Site" mit der gespeicherten Malware) und die ausgehende Kommunikation der Malware zu verschlüsseln. Diese Verschlüsselung erweckt den Eindruck von „vertrauenswürdigen" Daten und gibt Betrügern damit freie Hand, um Unternehmen zu infiltrieren, auf Vermögenswerte zuzugreifen und die Datenexfiltration zu verschleiern.

Verschlüsselungsrisiko #3: Betrüger verschleiern Datenexfiltration

Wenn es einem externen Betrüger gelingt, ein Unternehmensnetzwerk mit der Absicht des Diebstahls von digitalen Vermögenswerten zu infiltrieren, muss er einen Weg finden, um Daten aus dem Sicherheitsperimeter des Unternehmens nach außen zu leiten. Ein interner Betrüger steht vor dem gleichen Problem: Wie gelangen firmeneigene Daten außerhalb der Organisation?

Betrüger verstecken Malware in eingehenden verschlüsselten Daten. In einigen Fällen detoniert diese Malware innerhalb einer Organisation, infiziert interne Systeme und kontaktiert anschließend externe Command-and-Control-Server (C&C), um wertvolle Unternehmensdaten aus der Organisation zu schleusen.

Verschlüsselung kann schädliche (und selbst gelegentlich versehentliche) Datenlecks verschleiern. Wie kann ein IT-Verantwortlicher ohne ausgehende SSL/TLS-Überprüfung feststellen, ob vertrauliche Daten geheim bleiben? SSL/TLS-Überprüfung muss sowohl eingehenden Daten-Traffic (zum Fernhalten von Betrügern) als auch ausgehenden Daten-Traffic (zum Schutz interner Daten) umfassen. Im Fall von ausgehendem Traffic ist SSL-Überprüfung notwendig, um Datenverlust zu verhindern und Schwachstellen für die Datenexfiltration bei Zero-Day-Angriffen zu identifizieren und zu beseitigen.[7]

Ausbalancierung von Zugang und Sicherheit im neuen Zeitalter des Datenschutzes

Die Entwicklung der Internet-Konnektivität läutet ein neues Zeitalter des Datenschutzes ein – vom Klartext zur verschlüsselten Datenübertragung, von implizitem zu explizitem Vertrauen. Dies spiegelt sich nicht nur in der Nachfrage der Verbraucher nach privater Datenverwaltung sondern auch in gesetzlichen Vorschriften wider, die das Recht des Benutzers auf Datenschutz definieren, wie z.B. die europäische Datenschutz-Grundverordnung (DSGVO)[8], Kanadas Personal Information Protection and Electronic Documents Act[9]sowie

---

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

https://eugdpr.org/

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

bestehende (Kalifornien, Maine, Nevada) und vorgeschlagene (Hawaii, Illinois, Massachusetts, Mississippi, New Mexico, New York, Rhode Island, Texas und Washington) Datenschutzgesetze in mehreren US-Staaten.

Nicht der gesamte Browsing- oder Internet-Traffic kann gleich betrachtet werden. In den meisten Fällen konzentriert sich Datenschutz auf den Einzelnen. Ein gelegentlicher Benutzer in einem demokratischen Staat kann wahrscheinlich privat browsen, während ein Web-User an einem autoritär regierten Ort ein Anonymitätsnetzwerk wie TOR verwenden muss, um die Kommunikation mit Verwandten im Ausland vor der Zensur zu verbergen. In beiden Fällen sind die Daten Eigentum des Benutzers und kaum jemand – abgesehen vielleicht von einer solchen autoritären Regierung – würde das Recht jedes Benutzers auf Datenschutz anzweifeln. Beide Benutzer tragen das Risiko des Datenverlusts oder des Abgehörtwerdens – ein Risiko, das sich auf ihre eigenen Wohnungen und Geräte beschränkt.

Anders verhält es sich innerhalb von Unternehmen oder bei staatlich bereitgestelltem Internetzugang. Die meisten würden zustimmen, dass die Benutzer eines Unternehmens ein gewisses Maß an Datenschutz im Internet haben sollten – es spricht nichts dafür, dass die Einkaufsgewohnheiten, Urlaubsziele, Hobbys oder Browsing-Ziele eines Benutzers für andere Mitarbeiter sichtbar sein sollten. Die verschiedenen Datenschutzgesetze unterstützen diesen Anspruch in vielen Fällen. SSL/TLS macht diese Privatsphäre, und selbst anonymes Browsing, seit Jahren möglich.

Der erwartete Datenschutz ist allerdings mit Kosten und Risiken verbunden: Können wir uns eine solche Privatsphäre weiterhin erlauben, wenn Betrüger dieses Privileg für ihre Zwecke missbrauchen können? Im Unternehmenskontext bedeutet dies, dass das Risiko sich nicht mehr auf den einzelnen Mitarbeiter beschränkt, sondern die gesamte Organisation betrifft. IT-Verantwortliche moderner Unternehmen müssen im Rahmen der Fähigkeiten von Verschlüsselungstechnologie die Risiken eingehender Bedrohungen gegen den Anspruch auf Privatsphäre abwägen – ein heikler Balanceakt zwischen den Rechten des einzelnen Mitarbeiters und dem legitimen Schutzanspruch des Unternehmens.

In einer Organisation sind die Argumente für ein Recht auf absolute Privatsphäre also weniger eindeutig. Jedes Unternehmen, das das Internet nutzt – und das tun im Prinzip alle Unternehmen – trägt gegenüber seinen Mitarbeitern, Aktionären und Kunden die Verantwortung dafür, sich selbst zu schützen sowie gesetzliche und behördliche Vorschriften einzuhalten. IT-Verantwortliche wenden zur Erkennung und Verhinderung von Angriffen und riskantem Verhalten technische und prozedurale Kontrollen an. Um das Risiko zu verringern und das „Haus" zu schützen, müssen diese Kontrollen auf den gesamten internen, eingehenden und ausgehenden Daten-Traffic angewendet werden.

Das regulatorische Umfeld kann die Verwaltung von Unternehmensdaten komplexer machen. In einigen europäischen Ländern sind Unternehmen per Gesetz verpflichtet, personenbezogene Daten von Mitarbeitern zu schützen, um deren Privatsphäre, und in manchen Fällen auch deren Anonymität, beim Web-Browsing

zu wahren. Ein Beispiel ist das deutsche Telekommunikationsgesetz[10] Das Telekommunikationsgesetz (TKG) gilt generell für Unternehmen, die Mitarbeitern Internetzugang zur privaten Nutzung gewähren. Das TKG schreibt ausdrücklich vor, dass Nutzer dem „Telekommunikationsgeheimnis" unterliegen müssen. Es verlangt von Organisationen auch einen adäquaten Schutz des Dienstes vor Schäden und/oder Eingriffen UND einen angemessenen Schutz der Browsing-Daten der Benutzer. TKG-konforme Unternehmen müssen das „Telekommunikationsgeheimnis" der Benutzer mit dem Schutz der Vermögenswerte in Einklang bringen.

Laut aktuellem Google Transparency Report,[11] sind bis zu 93% des Browser-Traffic von Chrome verschlüsselt. Wie kann ein Unternehmen angesichts von Advanced Threats über verschlüsselte Kanäle, durch die Betrüger Firmenkontrollen umgehen, sich selbst und seine Daten schützen und gleichzeitig die Rechte der Mitarbeiter auf Privatsphäre in Übereinstimmung mit Datenschutzbestimmungen wahren?

Öffnung des Tunnels – SSL/TLS-Entschlüsselung und -Überprüfung

In einem Unternehmen beschränken sich Malware-Angriffe nicht auf einzelne Personen. Sobald ein Angreifer Zugang zum Gerät eines Mitarbeiters hat, kann er sich in der Regel innerhalb der Reichweite dieses Mitarbeiters weiter ausbreiten („nach Osten/Westen[12]") und andere Systeme und Computer im Unternehmensnetzwerk infizieren.

Cybersicherheitskontrollen können ein- und ausgehende Klartextkommunikation einer Organisation problemlos überprüfen, die SSL/TLS-Verschlüsselung von ein- und ausgehenden Daten erschwert jedoch die Untersuchung. Kann die vermeintliche Privatsphäre eines sicheren Tunnels gewahrt bleiben, wenn verschlüsselte Bedrohungen eine solche Gefahr für den einzelnen Benutzer *und* das gesamte Unternehmen darstellen?

Die Antwort ist JA. Die Bekämpfung destruktiver verschlüsselter Bedrohungen beginnt mit SSL/TLS-Datenüberprüfung. Unternehmen haben eine institutionelle und gesetzliche Pflicht, ihre Vermögenswerte zu schützen, und dazu gehört auch der Schutz der Mitarbeiterkommunikation.

Zur Überprüfung von SSL/TLS-Daten muss die Organisation die Vertrauenskette der Kommunikation effektiv umleiten, indem sie diese durch einen Tunnel zwischen Browser und Überprüfungsgerät und einen weiteren Tunnel zwischen Überprüfungsgerät und Zielort unterbricht.

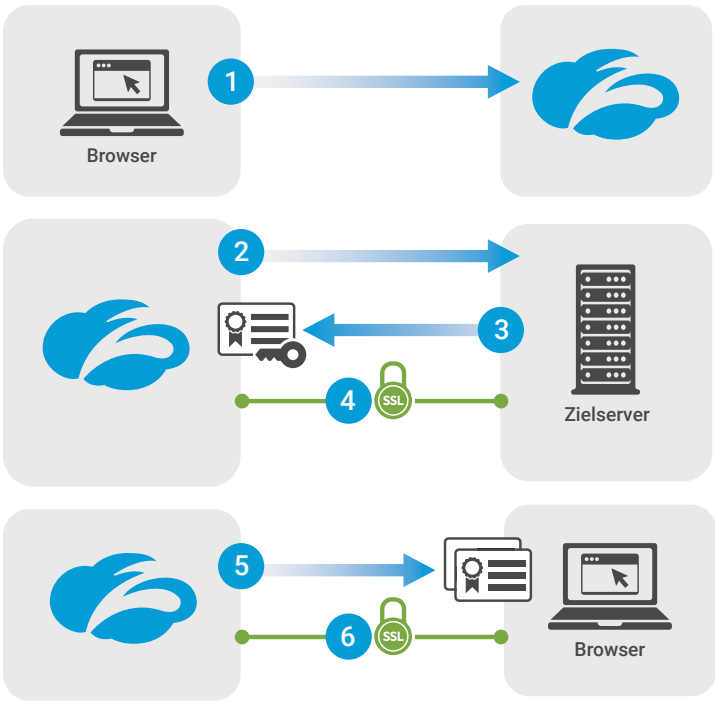
---

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

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

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

Wie Zscaler SSL/TLS verschlüsselte Daten überprüft – Workflow



1. Ein Benutzer öffnet einen Browser und sendet eine HTTPS-Anfrage.
2. Der Zscaler-Service fängt die HTTPS-Anfrage ab. Über einen separaten SSL-Tunnel sendet der Service seine eigene HTTPS-Anfrage an den Zielserver und führt SSL-Verhandlungen durch.
3. Der Zielserver sendet sein Zertifikat mit dem öffentlichen Schlüssel an den Zscaler-Service.
4. Zscaler-Service und Zielserver schließen eine SSL-Vereinbarung ab. Anwendungsdaten und nachfolgende Nachrichten werden über den SSL-Tunnel gesendet.
5. Der Zscaler-Service führt SSL-Verhandlungen mit dem Browser des Benutzers durch. Der Browser erhält das Zwischenzertifikat von Zscaler oder den benutzerdefinierten intermediären Root-Zugang Ihrer Organisation sowie ein von der Zertifizierungsstelle von Zscaler signiertes Serverzertifikat. Der Browser bestätigt die Zertifikatskette im Zertifikatsspeicher des Browsers.
6. Zscaler-Service und Browser schließen eine SSL-Vereinbarung ab. Anwendungsdaten und nachfolgende Nachrichten werden über den SSL-Tunnel gesendet.

Nach Vereinbarungsabschluss bewertet der Richtlinien-Engine von Zscaler die SSL/TLS-Richtlinien, wendet globale Blockierungen/Umgehungen an, überprüft Zertifikate von nicht vertrauenswürdigen Ausstellern und zeigt Benachrichtigungen an (falls erforderlich).

Abbildung 3. Workflow der Überprüfung von SSL/TLS-verschlüsselten Daten durch Zscaler.[13]

In diesem Beispiel wird die Vertrauensbeziehung zwischen Person und Quelle durch die Überprüfung nicht zerstört. Der Mitarbeiter vertraut nicht der Datenquelle, sondern der Organisation, die das Browsing-Gerät bereitstellt. Das Überprüfungsgerät „sieht" den Zielort und den Dateninhalt.

Bleibt also die Frage: *Kann eine Organisation wesentliche Schutzmaßnahmen durchführen und dennoch die beiden anderen Bestandteile von Verschlüsselung, nämlich Anonymität und Privatsphäre, respektieren?* Bei korrekter Ausführung definitiv. Aufgrund der Bedrohung durch verschlüsselte Malware ist SSL/TLS-Überprüfung als Cybersicherheitskontrolle für das moderne Unternehmen unverzichtbar geworden. Organisationen müssen ihre Sicherheitsanforderungen mit dem Recht ihrer Mitarbeiter auf Datenschutz in Einklang bringen. Ohne Überprüfung des SSL/TLS-Traffic setzt sich eine Organisation unnötigen Risiken aus, einschließlich PII, gestohlenem geistigen Eigentum, Industriespionage oder sogar Infizierung mit Ransomware. (Der Prozentsatz von Organisationen, die verschlüsselte Daten überprüfen, ist gestiegen: Von den Unternehmenskunden von Zscaler – fast die Hälfte davon in Europa – überprüfen 72% SSL/TLS-Traffic.)

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

Individuelle Online-Anonymität kann in einem Unternehmen gewahrt bleiben...in gewissem Umfang

Bei der Bewertung von Modellen zur SSL/TLS-Überprüfung müssen wir zunächst die Anonymität in Betracht ziehen. In manchen Organisationen ist Internetzugang für Mitarbeiter ein vertraglich garantiertes und geregeltes Recht, das auf gleiche Weise durch Richtlinien festgelegt und kontrolliert wird wie das Verhalten der Mitarbeiter am Arbeitsplatz.

Die Durchsetzung dieser Richtlinien erfordert Überwachung. Ein SSL/TLS-Tunnel macht Quelle und Ziel zwischen Browser und Server für jeden sichtbar. Die Protokollierung dieser Transaktionen ist für Verhaltensanalysen und Vorfallerkennung unerlässlich. Log-Prüfungen können dazu beitragen, die Einhaltung von Richtlinien sicherzustellen und die Wirksamkeit der Richtlinien kontinuierlich zu verbessern. (Retrospektive Log-Analyse wird häufig bei strafrechtlichen Ermittlungen eingesetzt.)

Wenn am Arbeitsplatz ein SSL/TLS-Überprüfungsprotokoll vorhanden ist, sollten Mitarbeiter beim Online-Browsen keine vollständige Anonymität erwarten, da der Internetzugang ein Privileg ist, das die Organisation ihren Mitarbeitern gewährt und das im Arbeitsvertrag jedes Mitarbeiters geregelt ist. Zum Schutz der Unternehmensressourcen kann die Organisation die Ziel-URLs, das Browsing-Verhalten und den Gerätezugriff eines Benutzers verfolgen. Die Unternehmensrichtlinien legen sowohl die Grenzen für die Internetnutzung als auch die Folgen von Verstößen gegen diese Richtlinien fest.

Um es klar auszudrücken: SSL/TLS-Überprüfung bedeutet kein Ende der individuellen Internetanonymität. Unternehmen können den Anspruch der Mitarbeiter auf Datenschutz mit aktuellen Cybersicherheitsmaßnahmen in Einklang bringen. Umfassende Datenkontrolle ist für eine effektive SSL/TLS-Überprüfung zwar erforderlich, der Zugriff auf die überprüften Daten kann jedoch eingeschränkt werden. Mitarbeiter können während der gesamten Log-Analyse anonym bleiben, selbst im Fall von Ermittlungen und rechtlichen Schritten (z.B. Untersuchung und Konsequenzen potenzieller Richtlinienverstöße), solange kein Eingreifen erforderlich ist. Diese Anonymisierung wird in der Regel als Log-Indexierung oder Tarnung bezeichnet.

Zeitweise müssen IT-Verantwortliche die Logs vollständig untersuchen und analysieren. Beispielsweise überprüft der für Cybersicherheit Zuständige die Logs regelmäßig, um Malware-Rückrufe über SSL/TLS-Tunnel zu identifizieren. Bei Entdeckung muss die IT-Sicherheit einen Workflow zur Maschinenbereinigung auslösen, in den der Mitarbeiter einbezogen wird, um die Malware vom betreffenden infizierten Gerät zu entfernen (oder es sogar neu zu formatieren oder zu zerstören). Dieses Verfahren kann implementiert werden, um einen „Vier-Augen[14]"-Ansatz zu unterstützen, bei dem sowohl ein Sicherheitsadministrator als

---

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

auch ein Arbeitnehmervertreter (z.B. der Vorsitzende einer Mitarbeitervereinigung oder auch ein externer Rechtsberater) die Konsolen-Logs gleichzeitig überprüfen.

Wenn Logs eine Infizierung feststellen, kann ein einzelner Benutzer des Unternehmens nicht anonym bleiben, sondern muss zur Preisgabe der Identität „enttarnt" werden, damit die IT-Sicherheit die Bedrohung beseitigen kann, bevor sie auf das gesamte Unternehmen übergreift.

Datenexfiltration – das ungewollte „Entweichen" von Daten aus einer Organisation – ist eine weitere Situation, die eine Enttarnung erfordern kann. In der Regel kann bei einem Log-Prüfverfahren festgestellt werden, ob vorheriger, ungefilterter SSL/TLS-Traffic tatsächlich für eine kriminelle oder ungenehmigte Ziel-Website bestimmt war. In diesem Fall müssen möglicherweise Strafverfolgungsbehörden eingeschaltet und Daten zur Unterstützung der Ermittlungen offengelegt werden.

Mitarbeiter können davon ausgehen, dass ihr Browsing für Kollegen, Management und selbst die Sicherheitsteams des Unternehmens anonym bleibt...bis ein Risiko oder eine Bedrohung für das Unternehmen die Aufgabe der Anonymität erforderlich macht. In den obigen Situationen ist es wichtig, dass die Organisation ein *dokumentiertes Recht* auf Enttarnung in einer Acceptable Use Policy (AUP) festgeschrieben hat, die meist im Arbeitsvertrag des Mitarbeiters enthalten ist. Internetnutzung über firmeneigene Geräte oder Netzwerke sollte nur dann gewährt werden, wenn der Mitarbeiter dieser Bedingung zugestimmt hat (normalerweise bei Arbeitsantritt).

Sicherung der Daten: SSL/TLS-Entschlüsselung in Umgebungen, die der DSGVO unterliegen

Nominell scheinen Daten nach dem „Öffnen" des SSL/TLS-verschlüsselten Kommunikationstunnels zur Datenüberprüfung und Richtliniendurchsetzung nicht mehr privat zu sein. Dies ist ein gemeinsames Anliegen von Rechtsabteilungen und Datenschutzanwälten. Einige verweisen auf die DSGVO als Grundlage für das Argument, dass es Organisationen laut DSGVO verboten ist, per SSL/TLS verschlüsselte personenbezogene Daten zu entschlüsseln und zu überprüfen. Unserer Ansicht nach ist dies nicht korrekt.

Selbst bei normalen, unverschlüsselten Sessions gelten für alle Parteien (ISP, Netzbetreiber, Caching-Proxy) zwischen Browser und Server die exakt gleichen Pflichten. Die DSGVO verlangt *auch* in diesem Fall von jeder Partei, personenbezogene Daten mit demselben Grad an Sensibilität zu behandeln. Durch Verschlüsselung ändern sich die Pflichten von Datenverantwortlichen und auch Verarbeitern nicht. Darüber hinaus widerspricht dem fehlerhaften Argument, dass die personenbezogenen Daten auf dem firmeneigenen Gerät des Mitarbeiters unverschlüsselt verarbeitet werden, *selbst wenn ein verschlüsselter Tunnel verwendet wird.* Es kann in diesem Unternehmenskontext kein absoluter Datenschutz gewährleistet werden.

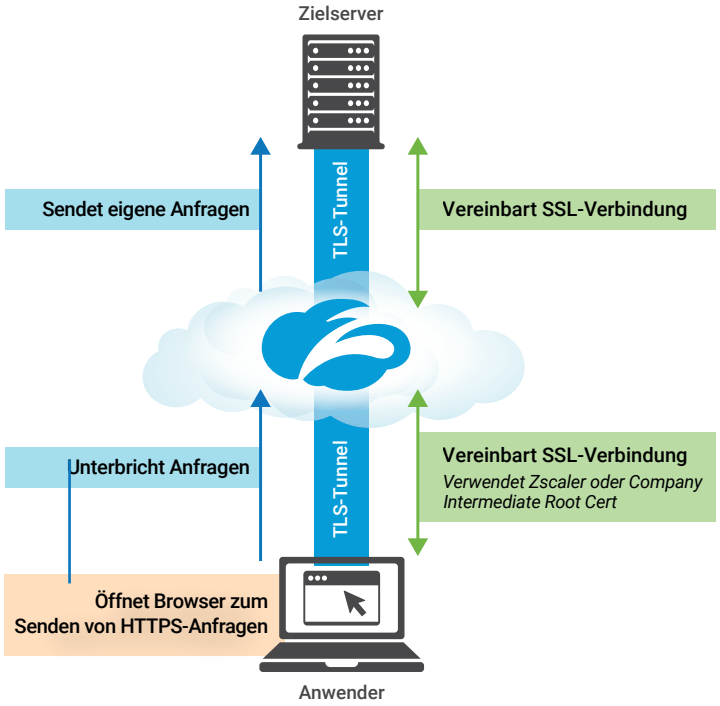
SSL/TLS-Überprüfung wird zur Durchsetzung von Richtlinien und zur Erkennung von Bedrohungen in verschlüsseltem Daten-Traffic eingesetzt. Zur Identifizierung von Bedrohungen entschlüsselt ein Überprüfungsgerät die Daten, vergleicht sie mit einer Reihe von „bekannt falschen" Signaturen und untersucht den Datenstrom, um Bedrohungsrisiken wie eindringende Malware oder unberechtigt ausgehende Unternehmensdaten zu erkennen. Wenn die Daten keine Bedrohung darstellen, werden sie neu verpackt und weitergeleitet. Eine auf diese Weise durchgeführte SSL/TLS-Überprüfung schränkt die Privatsphäre der Mitarbeiter nicht ein. Die Daten werden weder an Dritte weitergegeben noch in einer Weise verwendet, die die Rechte des betroffenen Datensubjekts verletzt. Der SSL/TLS-Überprüfungsprozess schützt die Unternehmenswerte vor bedrohlichen Angriffen, ohne gegen individuelle Datenschutzrechte zu verstoßen.

Zscaler bietet umfassende SSL/TLS-Überprüfungsfunktionen zum Schutz des Kundendaten-Traffic und zur Gewährleistung von „Perfect Forward Secrecy" (PFS).[15] Zscaler speichert Daten niemals auf der Festplatte: Nach Abschluss der Datenüberprüfung wird der Datenfluss ungehindert fortgesetzt, ohne dass Quelldaten über das Transaktions-Log hinaus aufbewahrt werden. Zscaler schützt nicht nur die Daten während der Übertragung sondern sichert bei der Überprüfung auch alle SSL/TLS-Schlüssel ab. (Abbildungen 3 und 4 verdeutlichen, wie Zscaler SSL/TLS verschlüsselte Daten überprüft. Weitere Informationen darüber, wie Zscaler sämtliche Daten und Kodierungsschlüssel absichert, finden Sie hier.[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

Wie Zscaler SSL/TLS verschlüsselte Daten überprüft – Workflow



Zscaler dient als Inline SSL-Proxy. Wir lösen die vom Client etablierte SSL-Verbindung auf und stellen eine neue SSL-Verbindung zum Server her. Aus Sicht des Client wird Zscaler zum Server, und aus Sicht des ursprünglichen SSL-Servers wird Zscaler zum Client.

Cloud-basierte SSL/TLS-Überprüfung durch Zscaler:

- Umfassende Untersuchung des gesamten Traffic
- Straffung der Zertifikatsverwaltung
- Vereinfachung der Netzwerkadministration
- Sicherer Traffic mit AES/GCM/ECDHE - Codes für PFS
- Durchsetzung effektiver Richtlinienkontrollen
- Schutz von Benutzer-Daten (da Daten nur vorübergehend und niemals in der Cloud gespeichert werden)

Abbildung 4. Inline-Proxy-Modell der Überprüfung von SSL/TLS-verschlüsselten Daten durch Zscaler.[17]

Es ist hilfreich, das Recht auf Privatsphäre als Ergebnis zu betrachten und zu prüfen, wie dieses Ergebnis erzielt werden kann, statt die einzelnen Schritte zu benennen, die dieses Ergebnis beeinträchtigen könnten. Überprüfung des Traffic und das binäre Resultat von Blockieren oder Nichtblockieren sind nicht dasselbe wie Zugriff, Überwachung und Speicherung der verschlüsselten Daten.

Umfassende SSL/TLS-Überprüfung stärkt die Compliance eines Unternehmens mit DSGVO und allgemeinen Datenschutzbestimmungen, weil dadurch die Daten der Organisation und seiner Mitarbeiter sowie die Vermögenswerte des Unternehmens geschützt werden. Ohne SSL/TLS-Überprüfung besteht ein höheres Risiko, interne personenbezogene Daten/PII offenzulegen und dadurch gegen Gesetze zu verstoßen.

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

Datenschutzvorschriften unterstützen Privatsphäre *und* Sicherheit

Datenschutzbestimmungen – insbesondere europäische Gesetze wie die DSGVO,[18] die britische Network and Information Systems Regulation 2018 (NIS)[19]und das TKG[20]– wurden verabschiedet, um sicherzustellen, dass Organisationen personenbezogene Daten schützen und gleichzeitig freien, fairen Zugang zum Internet gewähren. Diese Bestimmungen betreffen sowohl die Rechte des Einzelnen als auch die Sicherheitsmaßnahmen, die Unternehmen zum Schutz von Systemen und Daten ergreifen müssen. Laut Vorschriften des TKG sind Organisationen beispielsweise zur Einrichtung „technischer Schutzmaßnahmen[21]" verpflichtet, um Datenverlust zu verhindern und Angriffe von außen abzuwehren. Die NIS verlangt von Organisationen ausdrücklich die Implementierung geeigneter Sicherheitsmaßnahmen, um zu verhindern, dass Systeme (und die darin enthaltenen Daten) kompromittiert werden. Und laut Artikel 5 der DSGVO[22] müssen diese Organisationen Daten

> *...auf eine Art und Weise verarbeiten, die angemessene Sicherheit von personenbezogen Daten gewährleistet, einschließlich Schutz vor unbefugter und rechtswidriger Verarbeitung sowie vor versehentlichem Verlust, Zerstörung oder Beschädigung. Hierfür müssen geeignete technische oder organisatorische Maßnahmen ergriffen werden.*

Darüber hinaus haben Organisationen laut Artikel 32 (Sicherheit der Verarbeitung) der DSGVO eine affirmative Pflicht, Sicherheitsmaßnahmen für die Verarbeitung personenbezogener Daten zu ergreifen, die „ein dem Risiko angemessenes Sicherheitsniveau gewährleisten." SSL/TLS-Überprüfungen sind angesichts des Umfangs von Sicherheitsrisiken, die sie minimieren sollen, äußerst „angemessen".

Bedrohungen lauern in verschlüsseltem Traffic. Ohne Überprüfung kann ein Unternehmen unmöglich zwischen „guten" und „schlechten" SSL/TLS-verschlüsselten Daten unterscheiden. Kein Unternehmen kann ohne Überprüfung von verschlüsseltem Daten-Traffic sowohl die Datenschutz- als auch die Sicherheitsvorschriften von TKG, NIS und DSGVO einhalten – geschweige denn seine Mitarbeiter und die Unternehmensinteressen schützen.

---

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#87

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

Zum Mitnehmen: Wie Sie SSL/TLS-Überprüfung in Ihrem Unternehmen implementieren

Die Sicherheits- und Datenschutzgründe für SSL/TLS-Überprüfung im Unternehmen sind stichhaltig und unanfechtbar. IT-Verantwortliche müssen eine SSL/TLS-Überprüfung durchführen, um Daten, Mitarbeiter und Vermögenswerte ihres Unternehmens zu schützen–Andernfalls kann es zu irreparablen Schäden und zu Pflichtverletzungen kommen.

Wenn IT-Verantwortliche SSL/TLS-Überprüfung in ihrer Organisation einführen wollen, müssen sie mehrere wichtige Faktoren berücksichtigen:

1. Information der Mitarbeiter

- Stellen Sie sicher, dass eine gültige AUP vorhanden ist und dass die betreffenden Richtlinien am Proxy-/Inhaltsfilter durchgesetzt werden.
- Stellen Sie sicher, dass alle Mitarbeiter dieser AUP ausdrücklich zugestimmt haben, in der Regel in ihren Arbeitsverträgen.
- Stellen Sie sicher, dass die Mitarbeiter wissen, was personenbezogene Daten sind und wie lange diese von der Organisation gespeichert werden.
- Stellen Sie sicher, dass Mitarbeiter genau darüber informiert werden, was überprüft wird, damit sie fundierte Entscheidungen bei der Nutzung von Unternehmensressourcen treffen können.
- Holen Sie zur Bestätigung, dass SSL/TLS-Überprüfung tatsächlich auch den Mitarbeitern zugute kommt, die Zustimmung und Unterstützung von Betriebsräten und/oder Gewerkschaften ein.
- Erklären Sie, was unternommen wird und wie es durchgeführt wird.

2. Stützen Sie sich bei der Datenverarbeitung auf eine Rechtsgrundlage im Rahmen der DSGVO. Die Verordnung ist hier nicht der Feind – wenn ein Unternehmen der NIS oder ähnlichen Bestimmungen unterliegt, ist „Rechtspflicht" die gesetzliche Grundlage. Wie zuvor erwähnt, hat ein Unternehmen ein „legitimes Interesse" am Schutz der Organisation und ihrer Vermögenswerte.

3. Lassen Sie sich vom hausinternen Team oder von externen Fachleuten in Rechts- und Datenschutzfragen beraten, scheuen Sie jedoch keine Diskussionen über einzelne Punkte. Einige Anwälte oder Datenschutzexperten verstehen die angeboten Dienstleistungen vielleicht nicht vollständig oder können aus Mangel an technischen Kenntnissen nicht beurteilen, ob die Sicherheitsmaßnahmen dem Risiko entsprechen.

4. Stellen Sie sicher, dass Verfahren und Kontrollen effektiv und angemessen sind.

- Verschleiern Sie die Daten oder verbergen Sie diese auf andere Weise vor regulären Benutzern; stellen Sie sicher, dass die Daten nur auf Basis von „begründeter Notwendigkeit" verfügbar sind.
- Stellen Sie sicher, dass ein strenges und dokumentiertes Verfahren zur Prüfung personenbezogener Daten verwendet wird.
- Kontrollieren und implementieren Sie diesen Workflow regelmäßig.
- Speichern Sie die Daten während des festgelegten Zeitraums und löschen Sie diese anschließend.
- Bewahren Sie die Daten sicher auf, während sie sich im Besitz des Unternehmens befinden.

SSL/TLS-Überprüfung: Die korrekte Methode zur Einhaltung gesetzlicher Vorschriften

SSL/TLS-Überprüfung ist die „angemessene Sicherheitsmaßnahme" für den Schutz von Daten, Mitarbeitern und Vermögenswerten eines Unternehmens. SSL/TLS-Überprüfung schützt Organisationen vor Angriffen, wahrt aber gleichzeitig auch individuelle Persönlichkeitsrechte. Auf diese Weise wird die gesetzliche Compliance der Organisation gestärkt.

Verschlüsselte Bedrohungen sind spürbar, destruktiv, ansteckend und nehmen (exponentiell) an Umfang zu. Wenn IT-Verantwortliche den Traffic nicht entschlüsseln, gefährden sie sowohl die Privatsphäre ihrer Benutzer als auch die Vermögenswerte des Unternehmens und riskieren außerdem Verstöße gegen verschiedene Datenschutzbestimmungen. In der heutigen modernen Zeit müssen IT-Verantwortliche SSL/TLS-Überprüfung einführen, um Sicherheitsrisiken für das Unternehmen zu bekämpfen und die Privatsphäre von Mitarbeitern und Benutzern zu wahren.

Über Zscaler

Zscaler wurde im Jahr 2008 auf der Grundlage eines einfachen aber wirkungsvollen Konzepts gegründet: Da Anwendungen in die Cloud verlagert werden, muss sich auch die Sicherheit dorthin bewegen. Heute helfen wir Tausenden von globalen Organisationen bei der Transformation zu Cloud-fähigen Betriebsabläufen.