DOİ: https://doi.org/10.30546/301678.02.02.2025.028

TLS/SSL PROTOKOLLARININ MÜƏSSİSƏ İNFRASTRUKTURLARINDA TƏHLÜKƏSİZLİK TƏMİNATINDA ROLU

Həsənli Mətləb Malik

Azərbaycan Dövlət İqtisad Universiteti (UNEC),
Beynəlxalq Magistratura və Doktorantura Mərkəzi
E-mail: metlebhesenli7@gmail.com

XÜLASƏ

Bu məqalədə TLS/SSL protokollarının müəssisə infrastrukturlarında informasiya təhlükəsizliyinin təmin edilməsində oynadığı əsas rol araşdırılır. Müasir rəqəmsal mühitdə internet üzərindən ötürülən məlumatların məxfiliyinin, bütövlüyünün və autentifikasiyasının qorunması müəssisələr üçün prioritet məsələlərdən biridir. TLS/SSL protokolları bu tələbləri qarşılayan əsas kriptoqrafik mexanizmlər kimi çıxış edir. Məqalədə əvvəlcə TLS/SSL-in texniki əsası, şifrələmə metodları, TLS handshake prosesi və sertifikat infrastrukturu (PKI) izah olunur. Daha sonra protokolun web serverlər, elektron poçt sistemləri, VPN həlləri, API-lər və cloud mühitlərində tətbiq istiqamətləri təhlil edilir. TLS/SSL-ə qarşı tətbiq olunan hücum vektorları və tarixi zəifliklər (MITM, downgrade, Heartbleed və s.) praktiki nümunələrlə araşdırılır. Sonda müəssisə miqyasında TLS/SSL-in düzgün tətbiqi, təhlükəsiz konfiqurasiyası, sertifikatların idarə olunması və monitorinqi üçün ən yaxşı təcrübələr təqdim olunur. Araşdırmanın nəticələri göstərir ki, TLS/SSL protokolları təşkilatların kibertəhlükəsizlik strategiyasının ayrılmaz hissəsidir və düzgün tətbiq edildiyi halda məlumatların təhlükəsizliyini əhəmiyyətli dərəcədə artırır.

Açar sözlər: *TLS/SSL, kriptoqrafiya, şifrələmə, MITM hücumları, təhlükəsizlik protokolları, müəssisədə informasiya təhlükəsizliyi*

JEL kodları : C88, L86, M15, O33

GİRİŞ

Rəqəmsal transformasiyanın sürətləndiyi müasir dövrdə müəssisələr məlumat mübadiləsini, biznes proseslərini və xidmətlərini geniş şəkildə internet üzərindən həyata keçirirlər. Bu isə onların təhlükəsizlik tələblərini daha da artırır və ötürülən məlumatların məxfiliyinin, bütövlüyünün və autentifikasiyasının təmin olunmasını zəruri edir. İnformasiya təhlükəsizliyinin bu əsas komponentlərini təmin edən ən etibarlı texnologiyalara Transport Layer Security (TLS) və Secure Sockets Layer (SSL) protokollarını aid etmək olar. Bu protokollar istənilən şəbəkə mühitində məlumatların şifrələnmiş şəkildə ötürülməsinə şərait yaradır və istifadəçi ilə server arasındakı kommunikasiya kanalını potensial hücumlardan qoruyur. Müəssisə infrastrukturlarında TLS/SSL-in tətbiqi təkcə veb servisləri deyil, həm də elektron poçt sistemlərini, VPN bağlantılarını, API inteqrasiyalarını, cloud mühitlərini və daxili biznes tətbiqlərini əhatə edir. İnfrastrukturun genişlənməsi və sistemlərin daha çox inteqrasiya olunması korporativ mühitdə şifrələnmiş trafikə olan tələbi daha da artırmışdır. Bu səbəbdən TLS/SSL protokollarının düzgün tətbiqi, təhlükəsiz konfiqurasiyası, sertifikatların effektiv idarə edilməsi və zəruri monitorinq mexanizmlərinin qurulması müəssisələrin təhlükəsizlik strategiyalarında xüsusi önəm kəsb edir. Eyni zamanda, TLS/SSL protokolları hər nə qədər güclü təhlükəsizlik təmin etsə də, zəif konfiqurasiya, köhnəlmiş versiyalardan istifadə, zəif şifrələmə suiteləri və yanlış sertifikat idarəçiliyi kimi problemlər onların effektivliyini azalda bilər. Tarixdə baş vermiş Heartbleed, POODLE, BEAST kimi ciddi zəifliklər bu protokolların davamlı olaraq təkmilləşdirilməsinin vacibliyini bir daha göstərmişdir.

TLS/SSL Protokollarının Texniki Əsasları

TLS və SSL protokolları müasir rəqəmsal kommunikasiya sistemlərinin təhlükəsizliyini təmin edən əsas texnoloji baza hesab olunur. Bu protokollar şifrələnmiş rabitə kanalı yaradaraq istifadəçilərin serverlərlə və tətbiqlərlə apardıqları informasiya mübadiləsinin məxfiliyini, bütövlüyünü və autentikasiyasını qoruyur. İnternet mühitində məlumatlar çoxsaylı şəbəkə nöqtələrindən, provayderlərdən, router və kommutatorlardan keçdiyi üçün onların müdaxiləyə və dəyişdirilməyə qarşı müdafiəsi həyati əhəmiyyət daşıyır. Buna görə də TLS və SSL protokolları şifrələmə, sertifikat doğrulama və təhlükəsiz sessiya idarəetməsi kimi mexanizmlərlə kommunikasiya prosesinin potensial təhlükələrdən qorunmasına şərait yaradır. TLS və SSL protokollarının texniki əsasını təşkil edən ilk prinsip kriptoqrafiyanın iki əsas modelindən ibarətdir. Bunların birincisi simmetrik şifrələmə modelidir ki, burada məlumatları şifrələmək və deşifrələmək üçün eyni açardan istifadə edilir. Bu yanaşma yüksək sürət və performans təmin edir və

səbəbindən məlumat ötürülməsi prosesi zamanı geniş şəkildə tətbiq olunur. Lakin simmetrik açarın qarşı tərəfə təhlükəsiz şəkildə çatdırılması problemi mövcuddur. Bu problemi həll etmək üçün ikinci model olan asimmetrik kriptoqrafiya tətbiq edilir. Asimmetrik şifrələmə açıq və gizli açar cütlüyü əsasında fəaliyyət göstərir. Açıq açar hər kəs üçün əlçatan ola bilər, gizli açar isə yalnız sahibində qalır. Bu model məlumatın mənbəyini doğrulamağa və simmetrik açarın təhlükəsiz ötürülməsinə şərait yaradır.

TLS protokolunun əsas elementlərindən biri handshake adlanan ilkin razılaşma prosesidir. Bu proses müştəri və server arasında şifrələmə parametrlərinin razılaşdırılması, sertifikatların təqdim edilməsi və sessiya üçün lazım olan açarların yaradılması kimi funksiyaları yerinə yetirir. Handshake prosesi müştərinin serverə ClientHello mesajı göndərməsi ilə başlayır. Bu mesajda müştərinin dəstəklədiyi TLS versiyaları, şifrələmə alqoritmləri və digər parametrlər öz əksini tapır. Server bu mesaja Server Hello ilə cavab verir və seçilmiş şifrələmə dəstini, istifadə ediləcək TLS versiyasını və sertifikat məlumatlarını təqdim edir. Sertifikat serverin kimliyini təsdiq edən əsas sənəd olduğundan müştəri bu sənədi doğrulamaq üçün sertifikatın imzasını yoxlayır, sertifikatın etibarlılıq müddətinə baxır və kök sertifikat mərkəzinin güvənilir olmasına diqqət yetirir. Sertifikat doğrulandıqdan sonra tərəflər sessiya açarları formalaşdırır və təhlükəsiz kanal yaradılır. TLS protokolunun digər vacib hissəsi rekord layıdır. Bu lay tətbiqlərdən gələn məlumatları bloklara bölür, sıxılma, autentifikasiya və şifrələmə əməliyyatlarını həyata keçirir və məlumatları şifrələnmiş formada ötürür. Rekord layı həmçinin məlumatın bütövlüyünü qoruyan MAC və ya AEAD mexanizmlərindən istifadə edir. Bu mexanizmlər ötürülən məlumatın dəyişdirilib dəyişdirilmədiyini müəyyən etməyə imkan verir və nəticədə şəbəkə boyunca məlumatın təhlükəsiz şəkildə ötürülməsi təmin olunur.

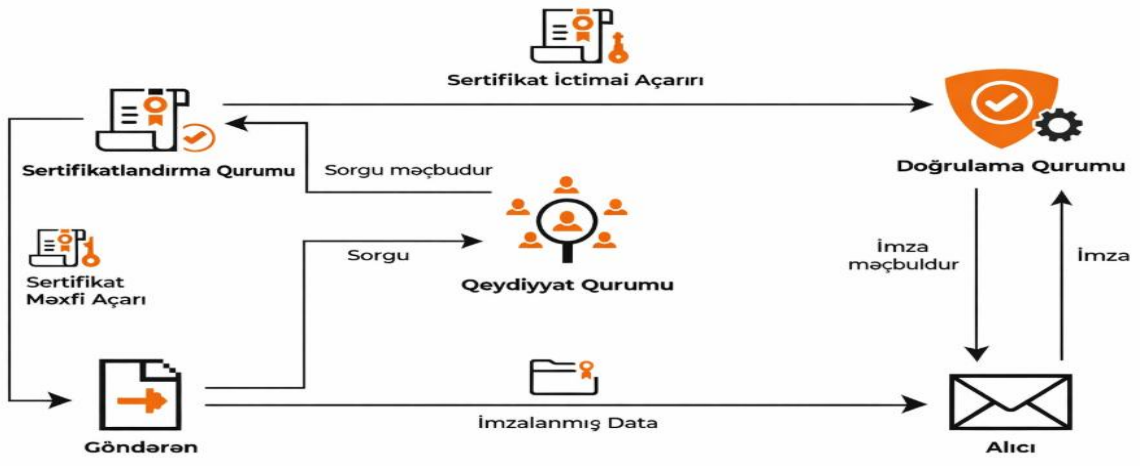
SSL protokolunun əvvəlki versiyaları bir sıra zəifliklərə görə istifadə üçün yararsız hesab olunur və onların yerini daha təhlükəsiz olan TLS protokolu almışdır. TLS 1.0 və TLS 1.1 versiyalarında müəyyən boşluqlar mövcud olduğundan bu versiyaların da istifadəsi məhdudlaşdırılır və müəssisələrə TLS 1.2 və TLS 1.3 protokollarına keçid tövsiyə edilir. Xüsusilə TLS 1.3 versiyası daha sürətli handshake prosesi, daha güclü şifrələmə suiteləri və daha az sayda mesaj mübadiləsi ilə təhlükəsiz rabitəni təmin edir. Bu isə həm performansı artırır, həm də protokolun hücum səthini əhəmiyyətli dərəcədə azaldır. TLS protokollarının fəaliyyət göstərməsi üçün Public Key Infrastructure adlanan açar və sertifikat idarəetmə sistemi mühüm rol oynayır. PKI sistemi sertifikat mərkəzləri, qeydiyyat orqanları və sertifikat siyasətlərindən ibarətdir. Sertifikat mərkəzləri serverlərin və istifadəçilərin kimliyini təsdiq edən rəqəmsal sertifikatlar hazırlayır və imzalayır.

Müştəri və server arasında etibarın yaranması məhz bu strukturun düzgün və ardıcıl işləməsindən asılıdır. Sertifikatların vaxtında yenilənməsi, CRL siyahılarında ləğv edilmiş sertifikatların izlənməsi, OCSP mexanizminin düzgün qurulması PKI-nin ayrılmaz tərkib hissələridir və TLS təhlükəsizliyinin davamlılığını təmin edir.

PKI İnfrastrukturunda TLS/SSL-in Rolu və Sertifikatların İdarə Edilməsi

TLS və SSL protokollarının təhlükəsiz şəkildə fəaliyyət göstərməsi birbaşa olaraq Public Key Infrastructure adlanan açar və sertifikat idarəetmə sistemindən asılıdır. PKI müəssisələrdə informasiya təhlükəsizliyinin əsas sütunlarından biri olub müxtəlif şəbəkə xidmətlərinin autentifikasiyasını, məlumatların bütövlüyünü və gizliliyini təmin edən kompleks mexanizmlər toplusudur. TLS protokolu məlumatın təhlükəsiz ötürülməsi üçün asimmetrik kriptoqrafiyaya əsaslandığından etibarlı açar cütlüklərinin yaradılması, saxlanması və doğrulanması funksiyalarını yerinə yetirən PKI quruluşu mütləq şəkildə tələb olunur. Bu səbəbdən PKI və TLS bir-biri ilə ayrılmaz şəkildə bağlıdır və bu əlaqə müasir müəssisə infrastrukturunun təhlükəsizlik arxitekturasının əsas komponentini təşkil edir. PKI sisteminin əsasını sertifikat mərkəzləri təşkil edir. Sertifikat mərkəzi serverlərə, tətbiqlərə və istifadəçilərə məxsus açıq açarların doğruluğunu təsdiq edən rəqəmsal sertifikatlar imzalayır. Hər bir sertifikat müəyyən bir subyektə məxsus olan açıq açarın kimlik və etibarlılıq xüsusiyyətlərini özündə əks etdirir. Sertifikat mərkəzinin imzası olmadığı halda müştəri serverin kimliyini təsdiqləyə bilmir və nəticədə TLS protokolunun əsas məqsədlərindən biri olan autentifikasiya təmin edilmir. Buna görə də sertifikat mərkəzlərinin etibarlılığı və onların verdiyi sertifikatların düzgün idarə edilməsi TLS təhlükəsizliyinin əsas şərtlərindən biri hesab olunur.

Şəkil 1. PKI-nın açıq açarlı infrastrukturu



Mənbə: Public Key Infrastructure (AppViewX, 2020)

Sertifikatlar müxtəlif növlərdə olur və onların seçimi müəssisənin ehtiyaclarından asılıdır. Domain doğrulamalı sertifikatlar əsasən kiçik təşkilatlar və standart veb xidmətlər üçün nəzərdə tutulur. Təşkilat doğrulamalı sertifikatlar müəssisənin hüquqi şəxs kimi mövcudluğunu təsdiqləyir və daha yüksək etibar səviyyəsi təqdim edir. Ən yüksək etibarlılığı isə genişləndirilmiş doğrulama sertifikatları təmin edir. Bu sertifikatların alınması üçün təşkilatın hüquqi, fiziki və operativ mövcudluğu hərtərəfli şəkildə yoxlanılır və nəticədə bu sertifikatlar təhlükəsizlik baxımından ən güclü üsullardan biri hesab olunur. Bundan əlavə vahid domeni qoruyan sertifikatlarla yanaşı wildcard və ya SAN sertifikatları da mövcuddur ki, bunlar bir neçə domen və subdomenin eyni vaxtda qorunmasına imkan verir. Sertifikatın etibarlılığının doğrulanması prosesində Certificate Revocation List və OCSP kimi mexanizmlər mühüm rol oynayır. CRL siyahısı etibarsız və ya ləğv olunmuş sertifikatların siyahısını təqdim edir və müştərilər bu siyahıya baxaraq sertifikatın aktiv və etibarlı olub olmadığını müəyyən edirlər. Daha operativ variant olan OCSP isə sorğu cavab mexanizmi ilə real vaxtda sertifikatın statusunu yoxlayır və nəticəni dərhal müştəriyə təqdim edir. Bu mexanizmlər olmadan TLS protokolunun autentifikasiya səviyyəsi ciddi şəkildə zəifləyər və saxta sertifikatlarla aparılan hücumlar qarşısında sistem müdafiəsiz qala bilər. Müəssisə infrastrukturunda PKI tətbiq edildikdə onun idarə edilməsi xüsusi diqqət tələb edir. Sertifikatların vaxtında yenilənməsi, açarların təhlükəsiz mühitdə yaradılması və saxlanması, daxili və xarici sertifikat mərkəzlərinin rolunun düzgün müəyyən edilməsi bu idarəetmənin əsas hissələridir. Böyük korporativ mühitlərdə daxili CA-ların yaradılması geniş yayılmış bir praktikadır. Bu yanaşma müəssisələrə öz sistemləri üçün xüsusi sertifikat siyasəti tətbiq etməyə, sərt təhlükəsizlik qaydaları müəyyən etməyə və bütün domeni əhatə edən mərkəzləşdirilmiş sertifikat idarəetmə mexanizmi qurmağa imkan verir. Lakin daxili CA-ların düzgün idarə olunmaması təhlükəsizlik baxımından ciddi risklər yarada bilər. Buna görə də daxili CA-lar üçün hardware security module kimi fiziki təhlükəsizlik həllərindən istifadə olunması tövsiyə olunur. TLS protokolu sertifikatların autentifikasiya prosesində mühüm rol oynayır. Müştəri ilə server arasında əlaqə yaradıldıqda server öz sertifikatını təqdim edir və müştəri bu sertifikatı etibarlı kök sertifikat mərkəzlərinin siyahısı ilə müqayisə edir. Sertifikat zəncirində boşluqlar və ya uyğunsuzluqlar aşkar edildikdə əlaqə dərhal dayandırılır və istifadəçiyə xəbərdarlıq edilir. Bu mexanizm MITM tipli hücumların qarşısının alınmasında son dərəcə vacib rol oynayır. Sertifikatlar həmçinin sessiya açarlarının təhlükəsiz paylaşılması üçün də istifadə olunur və TLS protokolunun şifrələmə mexanizmlərinin düzgün işləməsinə bilavasitə təsir göstərir. PKI və sertifikat idarəetməsinin digər mühüm aspekti sertifikatların avtomatlaşdırılmasıdır. Müəssisə miqyasında yüzlərlə və ya minlərlə sertifikat istifadə

olunduğundan onların əl ilə idarə olunması həm vaxt itgisinə, həm də potensial təhlükəsizlik risklərinə səbəb ola bilər. Bu səbəbdən ACME protokolu və ona uyğunlaşdırılmış avtomatlaşdırma vasitələri sertifikatların yenilənməsi və idarə olunmasını xeyli sadələşdirir. Avtomatlaşdırılmış sistemlər sertifikatın vaxtının bitməsini öncədən aşkar edir və lazımi yeniləmələri avtomatik olaraq həyata keçirir. Bu mexanizm sertifikat müddətinin bitməsi ilə əlaqəli sistem nasazlıqlarının və təhlükəsizlik problemlərinin qarşısını alır.

TLS/SSL-in müəssisə infrastrukturunda tətbiq sahələri

Müasir müəssisə infrastrukturları çoxsahəli, müxtəlif texnoloji komponentlərin qarşılıqlı inteqrasiya etdiyi mürəkkəb bir ekosistemdən ibarətdir. Bu ekosistemdə məlumatların fasiləsiz, düzgün və təhlükəsiz ötürülməsi ən kritik tələblərdən biridir. TLS və SSL protokolları bu tələbi təmin edən əsas texnologiyalardan biri kimi müəssisələrin müxtəlif xidmət və sistemlərində tətbiq edilir. Bu protokollar yalnız veb trafikin qorunması ilə məhdudlaşmır, həmçinin elektron poçt mühitindən tutmuş VPN şəbəkələrinə, API inteqrasiyalarından bulud xidmətlərinə qədər geniş spektrdə istifadə olunur. Bu fəsildə TLS/SSL protokollarının müxtəlif korporativ sistemlərdə tətbiqi geniş izah olunur və onların təhlükəsizlik baxımından təmin etdiyi üstünlüklər hərtərəfli şəkildə təhlil edilir. Müəssisə infrastrukturunda TLS-in ən geniş tətbiq sahəsi veb serverlərdir. HTTPS protokolunun əsası olan TLS veb brauzer və server arasında ötürülən hər bir məlumatın şifrələnməsini təmin edir. Bu mexanizm istifadəçi məlumatlarını, autentifikasiya proseslərini, ödəniş əməliyyatlarını və şəxsi məlumatları müdaxilədən qoruyur. Xüsusilə də e-ticarət, dövlət xidmətləri və daxili korporativ portallar kimi həssas tətbiqlərdə HTTPS-in məcburi tələb kimi qəbul olunması məlumatların təhlükəsizliyini artırır və istifadəçi etibarını gücləndirir. Müasir veb texnologiyalarında HSTS kimi mexanizmlər TLS-in rolunu daha da gücləndirərək brauzerlərin yalnız şifrələnmiş əlaqə ilə serverə qoşulmasını təmin edir. Elektron poçt sistemləri də TLS protokollarının geniş tətbiq olunduğu sahələrdən biridir. Məktublaşma infrastrukturunda SMTP, IMAP və POP3 kimi protokolların TLS ilə qorunan variantları istifadə olunur və bu yanaşma həm istifadəçi ilə mail server, həm də mail serverlər arasında məlumat ötürülməsində şifrələnmiş kanal yaradır. STARTTLS mexanizmi isə mövcud bağlantının şifrəsiz rejimdən şifrəli rejimə çevrilməsinə imkan verir. Elektron poçt sistemlərində TLS-in tətbiqi phishing, MITM və məlumatların sızması kimi təhlükələrin qarşısını almaqda mühüm rol oynayır. Xüsusilə korporativ mühitdə istifadəçi hesablarının, daxili yazışmaların və konfidensial sənədlərin təhlükəsiz ötürülməsi üçün TLS-in düzgün konfiqurasiyası vacibdir.

TLS protokolları müəssisələrdə geniş istifadə olunan virtual şəxsi şəbəkələrin də müdafiəsində əhəmiyyətli rol oynayır. OpenVPN, AnyConnect və SSL VPN kimi texnologiyalar kommunikasiya kanallarını TLS əsasında şifrələyir və uzaqdan qoşulan istifadəçilərin müəssisə resurslarına təhlükəsiz şəkildə daxil olmasını təmin edir. VPN bağlantılarında TLS-in tətbiqi ənənəvi IPSec tunelləri ilə müqayisədə daha elastik, platformaya uyğun və konfiqurasiya baxımından daha sadədir. Bu xüsusiyyətlər onu korporativ mühit üçün geniş tətbiq olunan həllə çevirir. TLS əsaslı VPN tunellərində həm server, həm də müştəri sertifikatla doğrulandığından əlaqənin saxtalaşdırılması ehtimalı xeyli azalır.

Müasir müəssisələrdə geniş yayılmış mikroservis arxitekturalarında və API inteqrasiyalarında TLS-in rolu xüsusi olaraq önəm kəsb edir. İnfrastruktur daxilində bir-biri ilə ünsiyyət quran xidmətlərin məlumat mübadiləsi açıq text şəklində ötürüldükdə ciddi risklərlə üzləşə bilər. Bu risklərə daxili trafikə müdaxilə, identifikasiya məlumatlarının sızması, daxili sistemlərin xəritələnməsi və tətbiqlərarası autentifikasiyanın pozulması kimi hallar daxildir. Buna görə də API-lərin də TLS üzərindən qorunması, həm daxili, həm də xarici mikroservislər arasında şifrələnmiş kanal yaradılması təhlükəsizliyin əsas komponentlərindən birinə çevrilmişdir. “Mutual TLS” kimi mexanizmlər isə həm serverin, həm də müştərinin sertifikatlar vasitəsilə qarşılıqlı təsdiqini təmin edir və xüsusilə yüksək təhlükəsizlik tələbinə malik infrastrukturlarda geniş tətbiq olunur. Cloud mühitlərində TLS-in tətbiqi müəssisələrin təhlükəsizlik strategiyasının ayrılmaz hissəsidir. Bulud texnologiyalarına keçid zamanı məlumatlar müxtəlif coğrafi bölgələrdə yerləşən serverlərdən və şəbəkələrdən keçir. Bu səbəbdən cloud xidmətləri ilə əlaqə zamanı TLS-in tətbiqi həm məlumat ötürülməsini qoruyur, həm də autentifikasiya mexanizmini gücləndirir. Azure, AWS və Google Cloud kimi platformalar bütün giriş nöqtələrində TLS 1.2 və TLS 1.3 versiyalarının tətbiqini məcburi edir və köhnə protokolların deaktiv edilməsini tələb edir. Bundan əlavə cloud mühitlərində daxili resurslar arasında şifrələnmiş trafik istifadəsi də getdikcə daha geniş yayılır və zero trust modelinin tətbiqi ilə birlikdə TLS-in rolu daha da artır. İnternet of Things və sənaye sistemlərində də TLS-in tətbiqi xüsusi önəm daşıyır. IoT cihazlarının əksəriyyəti internetə qoşulur və məlumat ötürür, lakin bu cihazların resurs məhdudiyyətləri səbəbindən onların təhlükəsizlik səviyyəsi çox zaman zəif olur. Bu isə sənaye nəzarət sistemləri, ağıllı ev qurğuları, sensorlar və telemetriya cihazlarında məlumat sızması və müdaxilə kimi ciddi risklər yaradır. TLS-in bu cihazlarda tətbiqi kommunikasiya kanalının şifrələnməsini təmin edir və cihazların identifikasiyasını asanlaşdırır. Lakin IoT cihazları üçün TLS-in yüngülləşdirilmiş versiyalarının hazırlanması mühüm məsələdir və bu cihazlarda minimal resursla maksimum təhlükəsizliyin təmin edilməsi əsas məsələdir.

Ümumilikdə, TLS və SSL protokolları müəssisə infrastrukturlarının bütün səviyyələrində kritik rol oynayır. Bu protokollar yalnız şifrələmə vasitəsi olaraq deyil, həm də autentifikasiya, məlumat bütövlüyü və etibarlı əlaqə səviyyəsinin təminatçısı kimi çıxış edir. İnfrastrukturun hansı hissəsində tətbiq olunmasından asılı olmayaraq TLS korporativ mühitin təhlükəsizlik arxitekturasının ayrılmaz hissəsidir və onun düzgün tətbiqi müəssisənin ümumi təhlükəsizlik mövqeyinin gücləndirilməsində həlledici əhəmiyyət kəsb edir.

TLS və SSL protokollarında təhlükəsizlik zəifliklər, hücum modelləri və müdafiə strategiyaları

TLS və SSL protokolları rəqəmsal mühitdə məlumatların gizliliyini, bütövlüyünü və identifikasiyasını təmin edən əsas kriptoqrafik təhlükəsizlik mexanizmləridir. İnformasiya axınlarının böyük hissəsi şifrələnmiş kanallar vasitəsilə ötürüldüyündən bu protokolların etibarlılığı şirkətlərin ümumi kibertəhlükəsizlik səviyyəsində həlledici rol oynayır. Lakin geniş tətbiqinə baxmayaraq TLS və SSL protokolları, həm dizayn xüsusiyyətlərinə, həm də implementasiya xətalarına bağlı olaraq, müəyyən zəifliklərə malik ola bilər. Bu zəifliklərin düzgün təhlili təşkilatların təhlükəsizlik strategiyalarının formalaşdırılması baxımından xüsusi əhəmiyyət kəsb edir.

TLS və SSL protokollarında rast gəlinən əsas problemlərdən biri köhnəlmiş versiyaların istifadəsi ilə bağlıdır. SSL 2.0 və SSL 3.0 təhlükəli hesab edilən dizayn qüsurlarına malikdir və artıq beynəlxalq təhlükəsizlik standartları tərəfindən istifadəsi qadağan olunmuşdur. Bu versiyalar zəif bütövlük təminatı, primitiv identifikasiya mexanizmləri və RC4 kimi gücdən düşmüş alqoritmlərdən istifadə etdiyinə görə müasir hücumlara qarşı dayanıqsızdır. Oxşar şəkildə TLS 1.0 və TLS 1.1 versiyaları da kriptoqrafik cəhətdən zəif hesab olunur, çünki bu protokollar BEAST, CRIME və digər hücum üsullarına qarşı həssasdır. Hazırda təhlükəsiz hesab edilən və müəssisələr tərəfindən istifadəsi tövsiyə olunan versiyalar yalnız TLS 1.2 və TLS 1.3-dür.

Protokollardakı zəifliklərin digər böyük kateqoriyası kriptoqrafik alqoritmlərin səhv seçilməsi ilə bağlıdır. Müasir tədqiqatlar göstərir ki SHA1 heş funksiyası artıq kolliziya hücumlarına qarşı dayanıqsızdır və böyük həcmdə hesablama resurslarından istifadə etməklə sındırıla bilər. RC4 axın şifrəsi statistiki zəifliklərə sahibdir və məlumat axınının təhlili ilə şifrə açarları müəyyən edilə bilər. Diffie–Hellman açar mübadiləsində istifadə olunan zəif parametrlər əlaqənin təhlükəsizliyini daha da zədələyə bilir. Buna görə müəssisələrdə AES-GCM, ECDHE, SHA256 və SHA3 kimi müasir alqoritmlərin tətbiqi xüsusi əhəmiyyət kəsb edir.

TLS və SSL protokollarına qarşı ən geniş yayılmış hücum metodlarından biri man-in-the-middle hücumlarıdır. Bu hücum növü zamanı kibercinayətkar istifadəçi ilə server arasında yerləşərək məlumat axınını ələ keçirir və dəyişdirə bilir. Sertifikat doğrulama prosesində hər hansı zəiflik mövcuddursa, hücum edən tərəf saxta sertifikatlar vasitəsilə əlaqəni öz üzərinə yönləndirə bilər. Digər ciddi təhlükələrə POODLE, BEAST, HEARTBLEED və CRIME kimi protokol əsaslı hücumlar daxildir. Bu hücumların bəziləri TLS-in dizayn qüsurlarından, bir qismi isə server və ya proqram təminatının düzgün implementasiya edilməməsindən qaynaqlanır. Sertifikatların idarə olunmasında baş verən səhvlər də təhlükəsizlik risklərini artıran mühüm faktorlardandır. Vaxtı keçmiş sertifikatların istifadəsi, sertifikat ləğv siyahılarının (CRL) və ya OCSP cavablarının yoxlanılmaması, etibarsız sertifikat mərkəzlərindən alınmış sertifikatların istifadəsi protokolun etibarlılığını ciddi şəkildə zəiflədir. Daxili PKI infrastrukturunun yanlış qurulması nəticəsində təşkilat daxilində xaotik sertifikat idarəetməsi yaranır ki, bu da həm serverlərin identifikasiyasını çətinləşdirir, həm də saxta sertifikatların istifadəsi üçün zəmin yaradır. TLS və SSL protokollarının təhlükəsizlik səviyyəsinin artırılması üçün müdafiə strategiyaları çoxsəviyyəli yanaşma tələb edir. İlk növbədə köhnə protokolların tamamilə deaktiv edilməsi və yalnız müasir versiyaların istifadəsi təmin olunmalıdır. Konfiqurasiya mərhələsində zəif şifr dəstlərinin deaktiv edilməsi, yalnız təhlükəsiz alqoritmlərin aktiv saxlanılması xüsusi əhəmiyyət daşıyır. Sertifikatların real vaxtda doğrulanması üçün OCSP stapling kimi mexanizmlərin tətbiqi əlaqənin təhlükəsizliyini daha da möhkəmləndirir. TLS parametrlərinin davamlı monitorinqi, mütəmadi audit prosesləri və zəriflik skanerlərinin istifadəsi protokollardakı zəifliklərin vaxtında aşkar edilməsinə imkan yaradır. Müəssisə səviyyəsində müdafiə strategiyalarının formalaşdırılması yalnız texniki tədbirlərlə məhdudlaşmamalıdır. Bu proses həmçinin təhlükəsizlik siyasətlərinin hazırlanmasını, əməkdaşların maarifləndirilməsini, kriptoqrafik açarların dövri dəyişdirilməsini, PKI infrastrukturunun mərkəzləşdirilmiş şəkildə idarə olunmasını və audit qeydlərinin saxlanılmasını tələb edir. Müasir təhlükəsizlik standartları göstərir ki TLS 1.3 protokoluna keçid, həm təhlükəsizlik, həm də performans baxımından müəssisələr üçün ən optimal həll hesab olunur. Nəticə olaraq qeyd etmək olar ki, TLS və SSL protokollarında mövcud olan zəifliklərin dərindən təhlili və onların aradan qaldırılması üçün müasir müdafiə mexanizmlərinin tətbiqi müəssisələrin kibertəhlükəsizlik səviyyəsini əhəmiyyətli dərəcədə artırır. Protokolların düzgün konfiqurasiyası, davamlı monitorinqi və müasir kriptoqrafik standartlara uyğun şəkildə idarə olunması məlumat axınının bütün mərhələlərdə etibarlı qorunmasını təmin edir və təşkilatın ümumi təhlükəsizlik arxitekturasını gücləndirir.

NƏTİCƏ

Müasir rəqəmsal ekosistemdə informasiya təhlükəsizliyinin təmin edilməsi təşkilatların strateji prioritetlərindən birinə çevrilmişdir. İnformasiya resurslarının genişlənməsi, bulud xidmətlərinin sürətlə yayılması, cihazların çoxalması və kiberhücum vektorlarının rəngarəngliyi təhlükəsizlik infrastrukturunun daha kompleks yanaşmalar tələb etməsinə səbəb olur. Bu kontekstdə TLS və SSL protokolları müəssisələrin daxili və xarici məlumat axınlarının əsas müdafiə mexanizmini təşkil edir və həm məlumatların məxfiliyini, həm də bütövlüyünü təmin edən fundamental texnologiya kimi çıxış edir. Aparılmış araşdırmalar göstərir ki TLS və SSL protokollarının effektiv və etibarlı tətbiqi yalnız texniki parametrlərlə məhdudlaşmır. Bu mexanizmlərin təhlükəsizliyi birbaşa olaraq düzgün konfiqurasiya, sertifikatların idarə olunması, təhlükəsizlik siyasətlərinin tətbiqi və PKI infrastrukturunun peşəkar şəkildə qurulmasından asılıdır. Köhnəlmiş protokol versiyalarının istifadəsi, zəif alqoritmlərin aktiv qalması, sertifikatların vaxtında yenilənməməsi və monitorinq prosesinin təşkil edilməməsi təşkilatın təhlükəsizlik səviyyəsini ciddi şəkildə zəiflədə bilər. Təhlil göstərir ki müasir müəssisələr yalnız TLS 1.2 və TLS 1.3 kimi etibarlı versiyaları tətbiq etməklə yanaşı, eyni zamanda kriptoqrafik açarların dövri dəyişdirilməsini, sertifikatların real vaxtda doğrulanmasını və şifrələmə mexanizmlərinin davamlı auditini təmin etməlidir. Bundan əlavə, protokollara qarşı mövcud hücum modellərinin təhlili və onların qarşısını almaq üçün hazırlanmış müdafiə strategiyaları təşkilatın kibertəhlükəsizlik arxitekturasını gücləndirən əsas komponentlərdən biridir. Nəticə olaraq demək olar ki, TLS və SSL protokollarının düzgün tətbiqi müəssisə infrastrukturunun informasiya təhlükəsizliyinin təmin edilməsində əvəzolunmaz rol oynayır. Bu protokolların bütün elementləri - kriptoqrafik alqoritmlər, sertifikatlar, protokol versiyaları və idarəetmə mexanizmləri - vahid təhlükəsizlik çərçivəsi daxilində koordinasiya olunmalıdır. Bu yanaşma yalnız məlumatların qorunmasını təmin etmir, həm də təşkilatın rəqəmsal etibarını, hüquqi uyğunluğunu və ümumi əməliyyat dayanıqlığını artırır.

ƏDƏBİYYAT

1. Abbasov, C. İnformasiya Təhlükəsizliyi və Kriptoqrafiya. Bakı: Qanun Nəşriyyatı, 2020.
2. Əliyev, R. Kibertəhlükəsizlik və Şəbəkə Təhlükəsizliyi. Bakı: Elm və Təhsil, 2021.
3. Rəsulov, M. Şifrələmə və Məlumatların Müdafiəsi. Bakı: Bakı Dövlət Universiteti Nəşriyyatı, 2019.
4. Stallings, W. Cryptography and Network Security: Principles and Practice. Pearson, 2023.
5. Pfleeger, C., Pfleeger, S., & Margulies, J. Security in Computing. Pearson, 2022.
6. NIST Special Publication 800-57. Recommendation for Key Management. National Institute of Standards and Technology, 2023.
7. NIST Special Publication 800-175B. Guideline for Using Cryptographic Standards in the Federal Government. NIST, 2022.
8. ISO/IEC 27001:2022. Information Security Management Systems Requirements.
9. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2020.
10. Microsoft. Windows Server Security Best Practices. Microsoft Docs, 2023.
11. Cisco. Cisco Network Security Technologies and Solutions. Cisco Press, 2022.
12. Cloud Security Alliance. Security Guidance for Cloud Computing. CSA, 2023.

SUMMARY

This article examines the key role played by TLS/SSL protocols in ensuring information security in enterprise infrastructures. In the modern digital environment, protecting the confidentiality, integrity and authentication of data transmitted over the Internet is one of the priority issues for enterprises. TLS/SSL protocols act as the main cryptographic mechanisms that meet these requirements. The article first explains the technical basis of TLS/SSL, encryption methods, TLS handshake process and certificate infrastructure (PKI). Then, the application directions of the protocol in web servers, email systems, VPN solutions, APIs and cloud environments are analyzed. Attack vectors and historical vulnerabilities (MITM, downgrade, Heartbleed, etc.) applied against TLS/SSL are examined with practical examples. Finally, best practices for the proper implementation, secure configuration, management, and monitoring of TLS/SSL across the enterprise are presented. The results of the study show that TLS/SSL protocols are an integral part of an organization's cybersecurity strategy and, when implemented correctly, significantly increase data security.

Keywords: *TLS/SSL, cryptography, encryption, MITM attacks, security protocols, enterprise information security*

JEL Classification Codes : C88, L86, M15, O33