AzScienceNet elm kompüter şəbəkəsinin İnternet xidmətlərinin təhlükəsizliyi məsələləri

Rəşid Ələkbərov[1], Məmməd Həşimov[2], Tural Mustafayev[3], Məmmədrəsul Yaqubov[4]

AMEA İnformasiya Texnologiyaları İnstitutu

[1]rashid@iit.ab.az, [2]mhashimov@iit.ab.az, [3]tural.mustafayev@iit.ab.az, [4]mrasul.yagub@iit.ab.az

***Xülasə*— Məqalədə AzScienceNet elm kompüter şəbəkəsinin İnternet xidmətlərinin (hostinq, elektron poçt, eduroam, cloud computing) təhlili aparılmışdır. Qeyd olunan xidmətlərin istifadəsi zamanı meydana çıxan təhlükəsizlik məsələləri və onların həlli öz əksini tapmışdır.**

Açar sözlər*— *hostinq, eduroam, cloud computing, təhlükəsizlik, firewall, protokol.

I. GİRİŞ

AzScienceNet elm kompüter şəbəkəsi Azərbaycan Milli Elmlər Akademiyasının institut və təşkilatlarını elmi-tədqiqat, elmi-praktiki və tədris məsələlərinin həyata keçirilməsi zəruri olan müasir şəbəkə xidmətləri ilə təmin edir. AzScienceNet şəbəkəsinin yaradılması Azərbaycan elmi-tədqiqat və təhsil mühitini Avropa elmi-tədqiqat və təhsil fəzasına inteqrasiya edərək ölkəmizdə dünya standartlarına uyğun texnologiya və xidmətlərin istifadə edilməsinə, tədqiqatçılarımızın bu mühitdə daha səmərəli fəaliyyət göstərməsinə imkan verir. AzScienceNet şəbəkəsinin əsas vəzifəsi istifadəçilərinə günün 24 saatı ərzində qlobal İnternet şəbəkəsinə yüksək sürətli, təhlükəsiz çıxışı təmin etməkdir. AzScienceNet şəbəkəsi istifadəçilərə çoxsaylı İnternet xidmətləri (hosting, elektron poçt, elektron kitabxana, distant təhsil, AzScienceCERT, eduroam və s.) göstərir.

Hostinq xidməti - Sayta aid səhifələri, şəkilləri, sənədləri İnternet istifadəçilərinə təqdim edən serverlərə veb serverlər, bu serverin yaddaşında sənədləri yerləşdirmək üçün ayrılmış yerə isə hostinq deyilir [1]. Veb hostinq saytın İnternetdə yerləşdirilməsi, saxlanılması, istifadəçilərin sayta əlçatanlığını təmin edir. Veb-sayt yaradanlar saytı İnternetdə yerləşdirmək və istifadəçilərə tanıtmaq istəyirlər. Bunun üçün saytı xüsusi olaraq hazırlanmış, İnternet şəbəkəsinə çox surətli çıxışı olan, minlərlə istifadəçiyə eyni vaxda xidmət verə bilən bir serverdə yerləşdirmək lazımdır.

AzScienceNet şəbəkəsinə qoşulan bütün elmi-tədqiqat təşkilatları üçün bizim serverlərimizdə ödənişsiz hostinq xidməti göstərilir. Hostinq xidməti veb səhifələrin serverlərimizdə yerləşdirilməsinə cavab verir. 24x7 rejimində işləyən çoxnüvəli serverlərə, intellektual kommunikasiya avadanlığına və yüksək İnternet sürətinə malik AzScienceNet şəbəkəsinin Data Mərkəzi, yüksək səviyyədə hostinq xidmətinin göstərilməsinə imkan verir.

Elektron poçt xidməti – (Electronic Mail və ya E-Mail) indiki dövrdə insanlar arasında ən çox yayılmış ünsiyyət növüdür. Bu xidmət bir neçə saniyə ərzində İnternet şəbəkəsinin yerləşdiyi istənilən yerə mətn, şəkil, video və s. faylı göndərməyə imkan verir [2]. AzScienceNet şəbəkəsində e-poçt xidməti üçün Mail-server quraşdırılmışdır. Bu Mail-server AzScienceNet istifadəçilərinə xidmət edir. Mail-serverdə istifadəçilərə poçt qutuları yaratmaq, dəyişikliklər etmək üçün CommuniGate Pro proqram təminatı yazılaraq işə salınmışdır. Hazırda AzScienceNet şəbəkəsi AMEA-nın institut və təşkilatlarının 1500-dən çox əməkdaşına e-poçt xidməti göstərir. Onların hər birinə 1 Gbayt yaddaş həcmdə poçt qutusu yeri ayrılmışdır.

Eduroam xidməti – Eduroam "Education" və "Roaming" sözlərinin qısaldılmış formasıdır. Məqsədi bir sıra təhlükəsizlik standartlarından istifadə edərək, eduroam üzvü olan təşkilat nümayəndələrinin, digər eduroam üzvü olan təşkilatlarda olarkən rahat İnternet istifadəsini təmin etməkdir [3]. Eduroam xidməti AMEA-nın institut və təşkilatları əməkdaşlarının xarici ölkələrə ezamiyyəti zamanı bu ölkələrin eduroam xidmətinə qoşulan elm və təhsil müəssisələrinin daxili infrastukturundan istifadə edərək qlobal İnternet şəbəkəsinə qoşulmaq imkanı verir. Eyni zamanda eduroam xidməti xarici ölkələrdən AMEA-nın institut və təşkilatlarına ezamiyyətə gələn elmi əməkdaşların AMEA-da eduroam xidmətini dəstəkləyən bütün qoşulma nöqtələrindən istifadə edərək qlobal İnternet şəbəkəsinə heç bir əlavə konfiqurasiya edilmədən qoşulmasına imkan verir.

Cloud Computing xidməti – Cloud Computing – kommunikasiya texnologiyalarının köməyi ilə böyük təşkilatlarda yerləşən çox saylı kompüterlərin (server, kompüter, Data Mərkəz və s,) hesablama və yaddaş resurslarının klasterləşməsi və virtuallaşdırılmasını həyata keçirməklə, istifadəçilərin verilənlərinin emalı və yadda saxlanmasına xidmət edən hesablama sistemidir [4]. AzScienceNet şəbəkəsinin Data Mərkəzində OpenStack və OwnCloud proqram təminatları vasitəsilə müvafiq olaraq AzCloud və AzStorage xidmətləri qurulmuşdur.

AzCloud - xidməti qısa bir müddət ərzində böyük hesablama və yaddaş resursları tələb edən mürəkkəb məsələlərin həlli üçün virtual hesablama maşınları təqdim edir.

AzStorage - vacib məlumatların saxlanılması üçün yaddaş resursları təqdim edən xidmətdir. Kompüterin yaddaşı kifayət etmədikdə və ya xüsusi əhəmiyyətli faylları daha təhlükəsiz yerdə saxlamaq üçün istifadə olunur.

Yuxarıda qeyd olunan İnternet xidmətlərinin istifadəsi zamanı təhlükəsizlik məsələləri ön plana çıxır.

II. AZSCİENCE ŞƏBƏKƏSİNDƏ HOSTİNQ XİDMƏTİNİN TƏHLÜKƏSİZLİYİ MƏSƏLƏLƏRİ

AzScienceNet şəbəkəsi hal-hazırda 10-dan çox veb sayta hostinq xidməti göstərir. Həmin saytlara etibarlı xidmət göstərmək üçün AzScienceNet şəbəkəsində bir sıra təhlükəsizlik üsullarından istifadə olunur .

Qeydiyyat siyasəti və prosedur qaydaları – hər bir institut və təşkilatın səhifəsini aktivləşdirməzdən əvvəl tam araşdırılır. Serverlərdə yerləşdirilən bütün səhifələr monitorinq olunur ki, onların içərisində şəbəkəyə zərər verəcək hər hansı bir səbəb aşkarlanmasın.

Firewall – Firewall hostinq xidməti üçün çox vacibdir. AzScienceNet Data Mərkəzinin Firewall veb serverləri şəbəkə xaricindən gələn bütün təhlükələrdən qoruyur. Firewall qeyri–qanuni müdaxilənin qarşısını almaq üçün şəbəkələr arasında girişləri məhdudlaşdırır.

Müdaxilələri aşkarlayan monitorinq proqram təminatı – AzScienceNet şəbəkəsində işləyən bu proqram təminatı şəbəkəni monitorinq edərək sistem administratorlarını potensial risklər zamanı xəbərdar edir. Firewall və belə proqramların oxşar cəhətləri olsa da onların fərqləri var. Firewall kənardan gələn təhlükənin qabağını alır, bu proqramlar isə kənardan və daxildən gələn təhlükəni müəyyən edir və administratoru xəbərdar edir [5].

DDoS hücumundan müdafiə – DDoS hücumlarının qarşısının alınması üçündür. Belə hücumlar səhifənin normal işləməsinə mane olur və digər istifadəçilərə səhifədən istifadə etməyə imkan vermir. Belə hücumlar zamanı xakerlər şəbəkə üzərində bir neçə yerə virus yoluxdurur. Sonra bütün virus saldığı maşınlar hər birindən eyni anda səhifəyə müraciət göndərməyə başlayır. Belə olan təqdirdə AzScienceNet şəbəkəsinin monitorinq proqramı DDoS hücumunun mənbəyini aşkarlayıb, həmin İP-lərdən gələn bütün müraciətləri bloklayır.

SSH (Secure Shell) **və sFTP** (Secure File Transfer Protocol) – Faylların təhlükəsiz transferi üçün istifadə edilir. SSH iki kompüterə təhlükəsiz kanal vasitəsilə ünsiyyət imkanı verən şəbəkə protokoludur. AzScienceNet şəbəkəsində FTP əvəzinə, sFTP protokolu istifadə olunur. Çünki bu protokol Secure Shell bazasına əsaslanır və FTP üçün təhlükəsiz əvəzedicidir.

cPanel və ya Plesk – Hazırda məlum olan iki ən təhlükəsiz idarəetmə panelləridir. Gələcəkdə AzSciencenet hostinq xidmətində bu iki paneldən birindən istifadə nəzərdə tutulur.

III. AZSCİENCE ŞƏBƏKƏSİNDƏ ELEKTRON POÇT XİDMƏTİNİN TƏHLÜKƏSİZLİYİ MƏSƏLƏLƏRİ

E-poçt hazırda biznes və şəxsi məqsədlər üçün ən çox istifadə olunan əlaqə vasitəsidir. Buna baxmayaraq hələ də tam təhlükəsiz deyil. Virusa yoluxmuş e-poçtlar və şəbəkədəki dinləmələr e-poçtun etibarlılığına ən çox mənfi təsir edən amillərdir. E-poçt xidmətinin təhlükəsizliyini təmin etmək üçün aşağıdakı üsullar vardır :

Şifrələmə – AzScienceNet-in elektron poçt xidməti elektron məktubların digər şəxslərin əlinə keçməsinin qarşısını almaq üçün göndərilən informasiyanı şifrələməyi nəzərdə tutur. Məktubların şifrələnməsi üçün, xüsusi şifrələmə alqoritmindən istifadə olunacaqdır. Bu halda serverlə klient arasında informasiya mübadiləsi şirfərələnmiş formada aparılacaq.

Yeniləmə – Ən vacib məsələlərdən biri də yeniləmədir. AzScienceNet şəbəkəsində ən son yeniləmələr e-poçt proqram təminatında daim tətbiq olunur.

Viruslardan qorunma – Viruslar adətən məktubların içində əlavə fayl (attachment) kimi yerləşdirilir. AzSciencenet şəbəkəsində məktublar servere daxil olarkən xüsusi antivirus və antispam tətbiqləri vasitəsilə yoxlanıldıqdan sonra istifadəçinin poçtuna daxil olur. Beləliklə, əgər məktubda zərərverici əlavə aşkarlanarsa dərhal bu məktub silinir və istifadəçiyə məlumat göndərilir.

Protokollardan istifadə – AzScienceNet şəbəkəsində elektron–poçt xidmətindən istifadə edərkən ənənəvi POP (Post Office Protocol) və İMAP (Internet Message Access Protocol) əvəzinə secure (təhlükəsiz) POP və İMAP protokollarından istifadə etmək nəzərdə tutulmuşdur [6].

IV. AZSCİENCE ŞƏBƏKƏSİNDƏ EDUROAM XİDMƏTİNİN TƏHLÜKƏSİZLİYİ MƏSƏLƏLƏRİ

Şəbəkəyə qoşulmuş hər bir istifadəçi şəbəkənin infrastrukturuna təhlükə mənbəyi ola bilər. Eduroam xidməti ilə şəbəkəyə qoşulmuş istifadəçi müəyyən proqram vasitələri ilə şəbəkəni analiz edə, intensiv paket ötürülməsi ilə şəbəkənin xidmət intensivliyini aşağı sala bilər. Aşağıda qeyd olunan hücumlar şəbəkəyə daha çox təhlükə mənbəyi ola bilər [7]:

Passiv hücumlar – Şifrələnməmiş trafikə nəzarət edir, digər növ hücumlarda istifadə oluna biləcək mətn, parol və həssas məlumatları axtarır. Passiv hücumlara şəbəkədə trafikin təhlili, müdafiəsiz rabitə monitorinqi, zəif şifrələnmiş trafiki oxumaq, loqin və parol kimi identifikasiya informasiyalarını əldə etmək daxildir. Şəbəkə əməliyyatlarının nəzarətinin və trafikin ələ keçirilməsi növbəti informasiyaların da ələ keçirilməsi deməkdir.

Aktiv hücumlar – Aktiv hücumlarda xakerlər təhlükəsizlik sistemindən yan keçmək və ya bu sistemə daxil olmaq istəyirlər. Bu hücumları yerinə yetirilməsində proqram təminatı, virus və ya troyanlar istifadə olunur. Aktiv hücumlar müdafiə sistemindən sızaraq və ya onu tam ələ keçirərək təhlükəli kodları sistemə daxil etməkdən və hər hansı bir informasiyanı oğurlamaqdan və ya dəyişdirməkdən ibarətdir.

Yaxın hücumlar – Yaxın hücumlar hər hansı bir şəxsin şəbəkə haqqında daha çox informasiya əldə etməsi üçün şəbəkənin komponentlərinə, verilənlər bazasına və xidmət göstərən hər hansı bir sisteminə fiziki yaxın olması ilə həyata keçirilir. Bu tip hücumlardan müdafiə olunmaq üçün AzScienceNet şəbəkəsində eduroam xidməti ilə İnternetə çıxan istifadəçi yerli şəbəkədən ayrılaraq başqa bir virtual şəbəkə vasitəsi ilə İnternetə çıxır.

Virtual şəbəkələrin (VLAN) tətbiqi şəbəkənin qurulmasını sadələşdirib və məhsuldarlığını artırmasına baxmayaraq, müxtəlif növ hücumlar üçün açıq tərəfləri çoxdur. Virtual şəbəkələrin tətbiqi bir çox hücumların qarşısını almasına baxmayaraq, onların da şəbəkədə bir çox problemlərə səbəb olması mümkündür. Eduroam vasitəsilə şəbəkəyə qoşulmuş hər hansı bir istifadəçi eyni zamanda həm də AzScienceNet şəbəkəsi üçün də təhlükə mənbəyi ola bilər. Bu tip təhlükələr VLAN Hopping vasitəsi ilə həyata keçirilir. VLAN hopping bir virtual şəbəkədəki istifadəçinin, giriş icazəsi olmayan başqa bir virtual şəbəkəyə sızmasını təmin edən hücum metodudur.

Double-tagging VLAN hopping-in əsas metodlarından biridir. Burada xakerlər kommutatorların iş prinsiplərindən istifadə edir. Double-tagging-in ən vacib özəlliyi ondadır ki, kommutatorun portu magistral port olmasa belə, freymlər ötürülür. Çünki xaker magistral olmayan portla şəbəkəyə daxil olur. AzScienceNet şəbəkəsində bu növ hücumların qarşısını

almaq üçün AzScienceNet şəbəkəsinin təbii virtual şəbəkəsi (VLAN) eduroam istifadəçilərinə verilən virtual şəbəkədən fərqli ID ilə sazlanmışdır [8].

Eduroam xidməti iyerarxik şəkildə birləşmiş RADİUS (Remote Authentication Dial In User Service) serverlər tərəfindən istifadəçilərin tanınmasını təmin edən şəbəkə infrastrukturuna malikdir. Eduroam üzvü olan təşkilatların istifadəçiləri, öz təşkilatlarında şəbəkəyə bağlanmaq üçün istifadə etdikləri istifadəçi adı və şifrə ilə eduroam üzvü olan başqa bir təşkilatda şəbəkəyə qoşula və İnternet xidmətindən istifadə edə bilər. Istifadəçi qonaq təşkilatda olarkən aldığı eduroam SSİD-sinə (Service Set İDentifier) əlaqə tələbi göndərdiyində, qonaq təşkilatın avtorizasiya serveri o tələbi istifadəçidən onun öz təşkilatının avtorizasiya serverinə istiqamətləndirərək, səlahiyyətli olub-olmadığını müəyyən edir. AzScienceNet şəbəkəsində bu informasiyalar istifadəçidən access point-ə və oradan öz avtorizasiya serverinə ötürülən zaman təhlükəsizliyi təmin olunur. Bütün bu sorğuların serverlər arasında şifrələnmiş şəkildə ötürülür. Bu da istidəçi adı və şifrəsinin öz təşkilatı xaricində görülməsinə imkan vermir. Bunun üçün IEEE 802.1x və "Wi-Fi Alliance"-ın WPA (Wi-Fi Protected Access) və WPA2 (Wi-Fi Protected Access 2) standartları iki şifrələmə protokolundan istifadə edir [9]:

Temporal Key Integrity Protocol (TKIP) – TKIP WPA tərəfindən istifadə olunan şifrələmə metodudur. O 802.11 WPA şifrələmə metoduna əsaslanaraq ənənəvi simsiz şəbəkə qurğularının öz trafiklərini şıfrələməsini təmin edir. Şifrələnmiş paketlərdə mesajın tamlığının yoxlanması (Message Integrity Check-MIC) istifadə edərək ötürülmədə mesajın toxunulmamış olduğuna əminlik yaradır.

Advanced Encryption Standard (AES) – AES WPA2 tərəfindən istifadə olunan şifrələmə metodudur. AES TKIP kimi eyni funksiyanı yerinə yetirir, amma TKİP-dən, daha güclü şifrələmə metoduna sahibdir. AES informasiyanın dəyişilib-dəyişilməməsini xüsusi protokol (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP)) vasitəsilə yoxlayır.

AzScienceNet şəbəkəsinin eduroam serveri hər bir kliyent və istifadəçi üçün sertifikatlar müəyyən edir və bu sertifikatlar AzScienceNet şəbəkəsinin Data Mərkəzində yaradılır. Azərbaycan Milli Elmlər Akademiyasının institut və təşkilatlarında və eduroam xidmətindən istifadə edən digər universitet və elm təşkilatlarının eduroam xidməti göstərən serverləri bu sertifikatlar vasitəsi ilə istifadəçi informasiyalarını şifrələyirlər.

V. AZSCİENCE ŞƏBƏKƏSİNDƏ CLOUD VƏ VİRTUAL RESURSLARIN TƏHLÜKƏSİZLİYİ MƏSƏLƏLƏRİ

Cloud Computing xidmətindən istifadə zamanı cloud provayder və istifadəçi arasında olan münasibətlər bir ikili razılaşma əsasında tənzimlənir. AzScienceNet şəbəkəsində istifadəçiləri narahat edən bu məsələlər aşağıdakı formada həyata keçirilir :

Qarşılıqlı etimad – Bulud texnologiyalarında etimad məsələsinin vacib amili bulud provayderinin istifadəçi verilənlərindən sui-istifadə etmək cəhdlərinin qarşısını almaqdır. Bu problemin həlli üçün verilənlərin anonimləşdirilməsi yanaşması təklif edilmişdir [10]. İstifadəçi öz şəxsi məlumatlarını cloud xidmətinin serverinə yerləşdirərkən əmin olmalıdır ki, onun məlumatlarına provayder tərəfindən heç bir müdaxilə olmayacaq. AzScienceNet şəbəkəsində elə bir insident baş verməyəcəyinə təminat verilir.

Təhlükəsizlik, gizlilik və anonimlik – İstifadəçilər bulud xidməti təqdim edən provayderdən şəxsi məlumatlara icazəsiz girişlərin qarşısının alınmasını və məlumatların gizli qalmasını tələb edirlər. Onlar həm də öz şəxsi məlumatlarının 3-cü şəxs tərəfindən monitorinq edilməsinin əleyhinədirlər. Yalnız bir şərtlə bu məlumatları monitorinq etmək olar ki, həmin şəxs bu işi istifadəçinin razılığı ilə və göstərilən xidmətin keyfiyyətinin yoxlanılması və yaxşılaşdırılması məqsədi ilə etsin.

İcazəsiz girişlərin və kənar müdaxilələrin qarşısını almaq üçün AzScienceNet şəbəkəsi SSL-dən (Secure Sockets Layer) və HTTPS protokollarından istifadə edir. İstifadəçilər əlavə təhlükəsizlik üçün şifrələmə texnologiyalarından da istifadə edə bilərlər.

Giriş və istifadə qadağası – İstifadəçilər öz məlumatlarına heç bir məhdudiyyət olmadan istədikləri yerdən və istədikləri zaman çatmaq istəyirlər. Patentləşdirilmiş şəxsi məlumatların və lisenziyadan kənar istifadənin də qarşısının alınması provayderin öhdəliyidir.

AzScienceNet şəbəkəsinin cloud xidmətindən İnternet olan hər yerdən istifadə etmək mümkündür. Amma ola bilər ki, hansısa ölkədə məhdud İnternet istifadə olunur və ya sırf hansısa provayderin xidmətinə qadağa var. Bu hallarda provayder əvvəlcədən məlumat verir. Şəxsi proqram lisenziyası bulud tətbiqləri üçün də istifadə edilə bilər. Patent məsələsində isə mövzu daha çətindir. Müəllif hüququ konkret bir fiziki və ya hüquqi şəxsə aid olan proqramın, məqalənin, şəklin, filmin və sair məlumatların bulud resurslarında yerləşdiyi zaman ondan icazəsiz istifadə, yayılma, surətinin çıxarılması hallarının qarşısının alınması üçün bir sıra tədbirlər görülür. İstifadəçi qaydalarında da bu məsələnin məsuliyyəti ilə bağlı məlumat verilir. AzScienceNet şəbəkəsində belə hal aşkarlanarsa qarşısı dərhal alınır və həmin istifadəçinin xidmətə girişi bloklanır.

Məsuliyyət – İstifadəçilər bulud xidməti təqdim edən provayderdən fasiləsiz xidmət gözləyirlər. Çünki xidmətdə fasilənin baş verməsi istifadəçiyə ziyan verə bilər. Fasilə baş verərsə məsuliyyətin və insidentə görə öhdəliyin kimin üzərində olacağı əvvəlcədən dəqiq məlum olmalıdır.

AzScienceNet şəbəkəsi məsuliyyət məsələlərini əvvəlcədən təyin etdiyi qaydalar və hüquqi normalarla tənzimləyir.

AzScienceNet şəbəkəsində cloud və virtual resurslardan istifadə zamanı istifadəçilərin məlumatlarının etibarlılığını təmin etmək üçün bir neçə təhlükəsizlik üsulundan istifadə edilir.

1) DDoS və buna bənzər hücumlar

Xüsusi quraşdırılmış təhlükəsizlik monitorinq sistemi Data Mərkəzin trafikini tam olaraq analiz edir və hücumların qarşısını alır. Bu hücumlar bir neçə hissəyə bölünür:

• **Proqram təminatına edilən ənənəvi hücumlar** – Bu tip təhlükələr şəbəkə protokollarında, əməliyyat sistemlərində boşluqlar olduğu zaman meydana gəlir. Bu təhdidlərdən qorunmaq üçün AzScienceNet şəbəkəsində antivirus,

şəbəkəarası ekran, müdaxilələri aşkarlama sistemindən istifadə olunur.

• **Cloudun elementlərinə edilən funksional hücumlar** – Bu tip hücumlar cloudun çoxlaylı olması, təhlükəsizlik prinsiplərinin ümumi olması ilə əlaqədardır. Bunun qarşısının alınması üçün clouddan əvvəl əks proksi quraşdırılmışdır. DDoS − hücumun uğur qazanması bütün clouda olan girişi bloklayır, lakin cloudun daxilində bütün əlaqələr və funksiyalar işlək vəziyyətdə qalır.

• **Klientə edilən hücumlar** – Bu tip hücum veb mühit üçün səciyyəvidir, lakin cloud üçün də aktual hesab olunur. Çünki klientlər clouda brauzerlər vasitəsilə qoşulurlar. Bu sinif hücumlara Cross Side Scripting, veb-sessiyaların tutulması, parolların oğurlanması və s. aid edilir. Bu hücumlardan qorunmaq üçün ənənəvi olaraq ciddi autentifikasiya üsulundan və qarşılıqlı autentifikasiya zamanı şifrələnmiş əlaqədən istifadə edilir [11].

2) Parolun yığım metodları ilə ələ keçirilməsi riski Xüsusi proqram vasitəsi ilə digər şəxsə aid olan parolun müxtəlif variantlarda yığılaraq tapılması.

• Hər hansı bir kənar şəxs tərəfindən parolun yığım metodları ilə ələ keçirilməsi riskinin qarşısının alınması üçün istifadəçilərə parol dəyişikliyi zamanı məhdudiyyətlər qoyulur. Bu məhdudiyyətlərə paroldakı simvolların sayı və müxtəlifliyi (böyük və kiçik hərflər, rəqəmlər və simvollar) aiddir. Lakin etibarlılığın yüksək səviyyəsini təmin etmək üçün sertifikatlardan istifadə edilir. LDAP (Lightweight Directory Access Protocol) və SAML (Security Assertion Markup Language) kimi standartlardan istifadə edilməsi məqsədəuyğundur.

3) Fiziki serverlərin oğurlanması və ya sındırılması halları

Məlumatlar cloudda saxlanılan kimi dərhal onların bir nüsxəsi avtomatik olaraq bir neçə serverə paylanır. Bu serverlər struktura görə eyni Data Mərkəzdə və ya müxtəlif Data Mərkəzlərdə yerləşə bilər. Belə ki, sınma və ya oğurlanma halları baş verdikdə istifadəçinin məlumatları itmir.

4) Məlumatların itməsi təhlükəsi və qəza hallarından sonra bərpa

Qəza halları və məlumat itkisi. Data mərkəzdə belə halların qarşısının alınması üçün bütün virtual əməliyyat sistemlərinin və məlumatların ehtiyat nüsxələri çıxarılır. Bir qəza olduğu zaman qısa zamanda itmiş və ya məhv olmuş məlumatlar geri qaytarılır. Bu məsələnin bir neçə üsulla həlli mövcuddur [11] :

• Ümumi "backup" sistemi vasitəsilə bütün məlumatların ehtiyat nüsxələrinin çıxarılması. Xüsusi proqramlar vasitəsilə virtual maşınların və yaddaş qurğularında yerləşən istifadəçi fayllarının ehtiyat nüsxələri çıxarılaraq yaddaş kasetlərinə (tape drive) yazılır.

• Virtual maşınların yerləşdiyi fiziki serverlərin proqram təminatlarında nasazlıq baş verdiyi zaman həmin serverin üzərində yerləşən virtual maşınlar avtomatik olaraq digər serverin üzərinə keçirilir. Bu proses zamanı heç bir fasilə baş vermir.

• Məlumatları virtual resursdan şəxsin öz kompüterinə köçürülməsi. Yəni hər iş gününün sonunda virtual maşında həll olunan məsələnin nəticələri və ya orada olan lazımlı fayllar istifadəçinin şəxsi kompüterinə yazılır. Data Mərkəzin təhlükəsizlik standartlarına görə onun yerləşdiyi məkandan kənarda ehtiyat Data Mərkəz (Disaster Recovery and Backup Center) olmalıdır ki, hər hansı bir fövqəladə hal zamanı fəaliyyət oradan davam etsin və məlumat itkisi olmasın. Hal-hazırda AzScienceNet-də vahid Data Mərkəzi olduğundan təhlükəsizlik üçün bu metoddan istifadə olunur.

NƏTİCƏ

Məqalədə AzScienceNet şəbəkəsində İnternet xidmətlərinin istifadəsi analiz olunmuş və servis xidmətlərinin təhlili aparılmışdır. Eyni zamanda, eduroam, elektron poçt, hostinq və cloud xidmətlərindən istifadə zamanı meydana çıxan təhlükəsizlik problemləri və onların həlli yolları analiz olunmuşdur. Təhlükəsizlik məsələlərinin həll olunması AzScienceNet şəbəkəsinə qoşulan istifadəçilərin təqdim olunan xidmətlərdən daha səmərəli və etibarlı istifadə etməsinə imkan yaradır.

ƏDƏBİYYAT

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

[2] http://www.computerhope.com/jargon/e/email.htm

[3] https://www.eduroam.org/

[4] R.Q. Ələkbərov, M.A. Həşimov, "Azsciencenet Şəbəkəsində Cloud Computing texnologiyalarinin tətbiqi perspektivləri haqqinda," İnformasiya texnologiyaları problemləri, №2 (6), s 30-36, 2012.

[5] http://www.findbestwebhosting.com/web-hosting-blog/

[6] J. Berkman, "Security issues in running an email server," 2003 GIAC Security Essentials Certification 4.1b, Option 1.

[7] http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/types-of-attack.html

[8] http://www.ciscopress.com/articles/article.asp?p=2181837&seqNum=10

[9] http://www.juniper.net/documentation/en_US/network-director1.5/topics/concept/wireless-encryption-and-ciphers.html

[10] R.M. Əliquliyev, F.C Abdullayeva, "Bulud texnologiyalarının təhlükəsizlik problemlərinin tədqiqi və analizi," İnformasiya texnologiyaları problemləri, №1, s.3–14, 2013.

[11] R.Q. Ələkbərov, M.A. Həşimov "Cloud Computing xidmətinin təhlükəsizlik məsələləri və onlarin həlli yollari," İnformasiya texnologiyaları problemləri, №2, s 33-39, 2014.