Elektron imza və kibertəhlükəsizlik

Toğrul Qafarbəyli

Azərbaycan Respublikası Rabitə və Yüksək Texnologiyalar Nazirliyi

international-tg2@mincom.gov.az

***Xülasə*— Məqalədə Azərbaycan Respublikasının informasiya təhlükəsizliyi ilə bağlı vəziyyəti təhlil edilmiş və bu istiqamətdə həyata keçirilən tədbirlər haqqında məlumat verilmişdir. Həmçinin e-imza və asan imzanın informasiya təhlükəsizliyində rolu müəyyənləşdirilmişdir.**

Açar sözlər*— *informasiya təhlükəsizliyi; elektron imza; Elektron Azərbaycan; asan imza

I. GİRİŞ

Elmi-texniki inqilab informasiya cəmiyyətinin yaranmasına səbəb olmuşdur. Bu cəmiyyətdə informasiya və biliklər ən mühüm resurs və başlıca əmtəədir. Vətəndaşların, cəmiyyətin və dövlətin həyatında informasiyanın, informasiya resurslarının və texnologiyalarının rolunun artması informasiya təhlükəsizliyi məsələlərini ön plana çıxarır. Müasir cəmiyyət tədricən öz informasiya infrastrukturunun vəziyyətindən asılı olur [1].

İnformasiya təhlükəsizliyi informasiya və ona xidmət edən infrastrukturun sahibi və ya istifadəçilərinə ziyan vurmağa səbəb olan təbii və ya süni xarakterli, təsadüfi və ya qəsdli təsirlərdən informasiya və ona xidmət edən infrastrukturun mühafizəli olmasıdır [2].

İnformasiyanın mühafizəsi informasiya təhlükəsizliyinin təmin olunmasına yönəlmiş tədbirlər kompleksidir.

Təhdid dedikdə kiminsə maraqlarına ziyan vurmağa səbəb ola bilən potensial mümkün hadisə, şərait, hərəkət, proses və s. nəzərdə tutulur.

II. AZƏRBAYCANDA İNFORMASİYA TƏHLÜKƏSİZLİYİ ÜZRƏ HƏYATA KEÇİRİİLƏN TƏDBİRLƏR

Rabitə və Yüksək Texnologiyalar Nazirliyi yanında Elektron Təhlükəsizlik Mərkəzi ölkədə kibertəhlükəsizlik vəziyyətinin izlənilməsi və təhlili məqsədilə öz fəaliyyətini təşkil etmişdir. Mərkəzdə buna daha geniş imkanlar yaradan və müasir tələblərə müvafiq olan infrastrukturun qurulması istiqamətində tədbirlər görülməkdədir. Bunun üçün Təhlükəsizlik Əməliyyat Mərkəzinin (SOC) yaradılması və quraşdırılması, monitorinq sisteminin modelinin düzgün seçilməsi əsas vəzifələrdən biri kimi müəyyənləşdirilmişdir. Bu məqsədlə sahə üzrə ixtisaslaşmış bir sıra aparıcı şirkətlərlə ("HP", "IBM" və "Symantec" şirkətləri) danışıqlar aparılmışdır. Hazırda Azərbaycanın İKT bazarında fəaliyyət göstərən şirkətlərlə də (Bestcomp, RİSK, Sinam, Softline, JetInfosystems) görüşlər keçirilmiş və onların kibertəhlükəsizlik sahəsində imkanları araşdırılmışdır. Həmçinin, Elektron Təhlükəsizlik Mərkəzinin işində maraq göstərən və kibertəhlükəsizlik sahəsində fəaliyyət göstərən bir sıra xarici şirkətlərlə də (Koç-System (Türkiyə), NİCE (İsrail), DPA (Latviya)) görüşlər keçirilmişdir [3].

Ölkədə ümumi kibertəhlükəsizlik vəziyyətinin təhlilini təmin etmək məqsədilə Azərbaycan Respublikasının Rabitə və Yüksək Texnologiyalar Nazirliyi tərəfindən Azərbaycan Respublikası Xüsusi Dövlət Mühafizə Xidməti, Milli Elmlər Akademiyası, milli internet operatorları və bu sahədə fəaliyyət göstərən informasiya infrastrukturu subyektləri ilə əməkdaşlıq şəbəkəsi qurulmuşdur. Bu əməkdaşlıq çərçivəsində 2012-ci ilin sentyabr ayından etibarən cari dövrə qədər ölkə ərazisində aparılan monitorinq və daxil olan müraciətlər əsasında bir sıra dövlət və qeyri-dövlət qurumlarına qarşı yönəlmiş kiber hücumlar qeydiyyata alınmış və onların xarakteri müəyyən edilmişdir.

Ümumilikdə, 2013-cü ilin yanvar-noyabr ayları ərzində Azərbaycanda fəaliyyət göstərən 400-dən artıq internet informasiya ehtiyatları müxtəlif qruplar tərəfindən hücumlara məruz qalmışdır. Əsas hədəfi ən çox dövlət qurumlarının, müxtəlif bankların, strateji obyektlərin, təhsil müəssisələrinin internet informasiya ehtiyatları olan belə kiberhücumlar əsasən şəbəkələrin baza qovşaqlarının və iri server resurslarının iş qabiliyyətinin pozulması, sistem informasiyasının dağılması və ya nüfuzdan salınması, inzibatçı imtiyazlarının əldə edilməsi, dövlət orqanlarının informasiya resurslarına və ayrı-ayrı hostlara DoS (Denial of Service) və DDoS (Distributed Denial of Service) hücumlar, kompüter viruslarının məqsədyönlü şəkildə göndərilməsi, parolların və başqa autentifikasiya informasiyasının ələ keçirilməsi, informasiya resurslarından icazəsiz istifadə edilməsi və s. xarakterli olmuşdur.

Azərbaycan Respublikasında cari ilin noyabr ayında keçirilən prezident seçkiləri ilə əlaqədar yaradılmış seçkiləri izləmə sisteminə, o cümlədən informasiya kommunikasiya resurslarını saxlayan sistemlərə çoxsaylı kiberhücumlar olmuşdur. Sistemin təhlükəsizliyi yüksək səviyyədə təmin olunduğundan seçki prosesində sistemə heç bir ziyan dəyməmişdir [1].

Ümumiyyətlə, ölkə ərazisində qeydə alınmış kiberhücumların təhlili göstərir ki, hücumların 90%-i xaricdən həyata keçirilməkdədir. Statistika göstərir ki, ölkənin informasiya resurslarına edilən hücumların intensivliyi və sayı hər il 30% artmaqdadır [3].

Digər bir mənfi məqam isə kibertəhdidlərin sayının və mürəkkəbliyinin sürətlə artması, həmçinin avtomatlaşdırılmış hücum vasitələrinin açıq istifadə üçün geniş yayılmasıdır.

Təhlillər göstərir ki, baş verən bəzi haker hücumlarının arxasında siyasi-iqtisadi məqsədli bəd məramlar dayanır. Özlərini "Anonimlər" ("Anonymous") adlandıran haker qrupu tərəfindən müxtəlif siyasi hadisələrdə, adətən dövlət təşkilatlarına aid internet informasiya ehtiyatlarına edilmiş hücumların analizi də bunu deməyə əsas verir [3].

Mümkün kiberhücumlara qarşı mütəşəkkil fəaliyyət göstərmək üçün hazırda Azərbaycanda Rabitə və Yüksək Texnologiyalar Nazirliyi yanında Elektron Təhlükəsizlik Mərkəzində, Xüsusi Dövlət Mühafizə Xidmətinin Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Agentliyində, Milli Elmlər Akademiyasında, Azərbaycan Respublikasının Təhsil Nazirliyində kompüter və internet-təhlükəsizlik sahələrində yaranmış insidentləri araşdırmaqla məşğul olan və bu sahədə ən yaxşı mütəxəssislərdən ibarət olan xüsusi qruplar - kompüter insidentlərinə qarşı cavab qrupları (Computer Emergency Response Team, CERT) fəaliyyət göstərir ki, onların Azərbaycanda fəaliyyət göstərən digər informasiya infrastrukturu subyektlərinin fəaliyyətinin koordinasiyasını Azərbaycan Respublikasının Rabitə və Yüksək Texnologiyalar Nazirliyi yanında Elektron Təhlükəsizlik Mərkəzi həyata keçirir [3].

Ölkədə ümumi kibertəhlükəsizlik vəziyyətinin təhlili zamanı bir daha müəyyən edilmişdir ki, Azərbaycanda informasiya təhlükəsizliyinin təmin olunması üzrə yetərli qanunvericilik bazası formalaşdırılmışdır və qanunvericilik bazasının təkmilləşdirilməsi istiqamətində fəaliyyət davam etdirilməkdədir. Belə ki, ölkədə "Dövlət sirri haqqında" (7 sentyabr 2004), "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" (3 aprel, 1998), "İnformasiya əldə etmək haqqında" (30 sentyabr, 2005), "Milli Təhlükəsizlik haqqında" (29 iyun, 2004), "Məlumat toplularının hüquqi qorunması haqqında" (14 sentyabr, 2004), "Fərdi məlumatlar haqqında" (11 may, 2010) Qanunlar qəbul edilmiş, dövlət orqanlarında informasiya təhlükəsizliyinin təmin edilməsi üzrə tədbirlər haqqında Azərbaycan Respublikası Prezidentinin Fərmanı imzalanmışdır [7]. Bununla yanaşı Azərbaycan Respublikası "Fərdi məlumatların avtomatlaşdırılmış qaydada işlənməsi ilə əlaqədar şəxslərin qorunması haqqında" (30 sentyabr, 2009-cu ildə) [8] və "Kibercinayətkarlıq haqqında" (2009-cu ildə) [9] Konvensiyalara da qoşulmuşdur. Eyni zamanda, informasiya təhlükəsizliyi sahəsində cinayət hallarının qarşısının alınması və cinayətkarların cəzalandırılması məqsədilə kompüter texnologiyalarından istifadə edilməklə törədilən cinayətlərlə bağlı Azərbaycan Respublikasının İnzibati Xətalar və Cinayət Məcəllələrinə müddəalar daxil edilmişdir. Kibertəhlükəsizlik üzrə beynəlxalq standartlar əsasında hazırlanmış 14 identik milli standart təsdiq edilmişdir.

Dövlət orqanları ilə müxtəlif əməliyyatlar həyata keçirərkən vətəndaşların şəxsi məlumatlarının üçüncü tərəfin ələ keçirməməsi üçün təhlükəsiz şəbəkələr getdikcə daha çox yayılır. Bundan başqa elektron əməliyyatların həyata keçirilməsi zamanı vətəndaşın kimliyinin müəyyən edilə bilməsi də təhlükəsizlik qədər vacib məsələdir. Bütün qeyd olunanlar isə elektron imzanın zəruriliyini ortaya çıxarır [2].

III. ELEKTRON İMZA

Elektron imza (e-imza) elektron dünyada şəxsiyyəti müəyyənləşdirmə vasitəsidir. E-imza anlayışı ümumi xarakter daşıyır. İnsanların əl imzalarının rəqəmsal çeviricilərdən keçirilmiş təsviri, barmaq izləri, səs kimi bioloji əlamətlərinin və s. elektron halda kimliklərinin doğrulanmasını təmin edən vasitədir.

E-imza elektron sistemdə imzanın malik olduğu bütün işləri yerinə yetirən, elektron sertifikat vasitəsilə bir elektron məlumata əlavə edilən və məlumatı göndərəni təyin edən bir ədədi koddur [5].

E-imza kartından bütün vətəndaşlar, fiziki şəxslər, hüquqi şəxslər və dövlət orqanları istifadə edə bilər.

E-imzanın üstünlüklərinə vaxta qənaət, məxfilik, rahatlıq, bütünlük, tanınma, inkaredilməzlik (məsuliyyətdən yayınmanın mümkünsüzlüyü), işgüzar münasibətlərin və əlaqələrin tamamilə elektron formata keçirilməsi daxildir. E-imza ilə imzalanmış sənədlər bir neçə saniyə ərzində lazım olan yerə çatdırıla bilər. Elektron sənəd mübadiləsinin bütün iştirakçıları bir-birindən uzaqda olmalarına baxmayaraq, eyni imkanlar əldə edirlər.

Azərbaycan Respublikasının Qanunlarına əsasən elektron imza ilə imzalanmış elektron sənədlər əl imzası ilə imzalanmış və möhürlənmiş sənədlərə bərabər tutulur.

E-imza kartından xaricdə də istifadə etmək olar. E-imza kartı konkret şəxsə aid olduğu üçün bu elektron imzanı yalnız həmin adam qoya bilər. Kartın başqa şəxsə verilməsi və identifikasiya kodunun (PIN kodun) digər şəxsə bildirilməsi ciddi pozuntu halı hesab edilir [6].

IV. ASAN VƏ YA MOBİL İMZA

Elektron hökumət (e-hökumət) hər hansı bir ölkənin dövlət strukturlarının hamısı haqqında məlumatların hər bir vətəndaş üçün açıq olan şəbəkədə yerləşdirilməsi deməkdir. Yəni hər bir vətəndaş hər hansı bir nazirlik və komitədən tutmuş, mənzil-təsərrüfat idarəsi ilə məktəbə qədər olan idarənin mövcud durumu, bu qurumlara müraciət etmənin qaydalarını istənilən vaxt əldə edə və bu təşkilatlara elə elektron rabitə vasitəsilə müraciət edə bilər.

E-hökumət sistemi tərəfindən vətəndaşa verilmiş kod ilə – fiziki və hüquqi şəxslər, o cümlədən dövlət qulluqçuları "elektron hökumət" sistemi tərəfindən onlara təqdim edilən kod vasitəsilə autentifikasiyadan keçərək, e-xidmətlərdən istifadə edə bilərlər.

Mobil autentifikasiya sertifikatı ilə – yalnız mobil imza sertifikatlarının sahibləri autentifikasiyadan keçərək, elektron xidmətlərdən istifadə edə bilərlər (smartfon və planşetlər üçün).

Smartfon ilə daxil olmaq – bu bölmədə yalnız mobil imza sertifikatlarının sahibləri smartfon vasitəsilə QR-kodu skan edib autentifikasiyadan keçərək xidmətlərdən istifadə edə bilərlər. Burada mobil imzası olan smartfon autentifikasiya vasitəsi kimi istifadə olunur.

ASAN imza vasitəsi ilə – fiziki və hüquqi şəxslər tərəfindən onlara təqdim edilən ASAN imza sertifikatları vasitəsilə autentifikasiyadan keçərək, elektron xidmətlərdən istifadə edə bilərlər.

ASAN İmza (Mobil imza) e-xidmətlərə daxil olan və rəqəmsal imzalar edən zaman kimliyinizi təsdiqləmək üçün sizin mobil identifikasiyanızdır və bütün mövcud e-xidmətlərdən istifadəni mümkün edir.

Asan İmza (Mobil imza) əslində elektron mühitdə fiziki İD-karta bərabər sənəd kimi sertifikatlara bağlı olan mobil telefon SİM-kartınızdır. Asan İmza (Mobil imza) ilə siz şəxsiyyətinizi təsdiq edə və sənədlərə rəqəmsal imza ata bilərsiniz [10].

NƏTİCƏ

Yuxarıda qeyd olunanlarla yanaşı, ölkəyə daxil olan ümumi internet trafikində qlobal kiberhücumların qarşısını almaq məqsədi ilə milli internet operatoru (Delta Telecom) ilə birlikdə əlavə qabaqlayıcı tədbirlərin də görülməsi zəruridir:

1. E-imza və asan imza (mobil imza) sistemlərinin kiberhücumlardan qorunması məqsədilə Rabitə və Yüksək Texnologiyalar Nazirliyi yanında Elektron Təhlükəsizlik Mərkəzi tərəfindən nəzarət olunan yeni vahid sistemin yaradılması;
2. Daxili İşlər Nazirliyi tərəfindən vətəndaşlara verilməsi nəzərdə tutulan yeni nəsil şəxsiyyət vəsiqələrində hər bir şəxs üçün individual elektron imza yerləşdirilərək təhlükəsizliyinin sözügedən qurum tərəfindən təmin olunması.

ƏDƏBİYYAT

[1] http://sia.az/az/news/politics/450260-nazir-secki-menteqelerinde-qurasdirilan-veb-kameralarin-kiber-tehlukesizlik-teminati-yaradilib
[2] http://az.wikibooks.org/wiki/%C4%B0nformasiya_t%C9%99hl%C3%BCk%C9%99sizliyi._Elektron_imza
[3] http://www.cert.az/xidmetler.html
[4] http://www.e-imza.az/index.php?lang=az
[5] http://az.wikibooks.org/wiki/Elektron_imza
[6] http://mincom.gov.az/fealiyyet/elektron-hokumet/
[7] http://e-qanun.az/
[8] http://azertag.az/xeber/
[9]]http://az.trend.az/business/economy/2120736.html
[10] http://www.asanimza.az/category/introduction-az/