Müasir kompüter şəbəkələrinin təhlükəsizlik trendləri haqqında

Ramiz Şıxəliyev

AMEA İnformasiya Texnologiyaları İnstitutu

ramiz@science.az

***Xülasə*— Məqalə kompüter şəbəkələrinin (KŞ) təhlükəsizliyi sahəsində mövcud trendlərinin analizinə həsr olunmudur. Bunun üçün əvvəlcə KŞ-də (İnternetdə) baş verən infrastruktur, tətbiqi və istifadə trendləri analiz edilmiş və onların KŞ-nin təhlükəsizliyinə təsiri analiz edilmişdir. KŞ-nin təhlükəsizlik trendlərinin müəyyən edilməsi yeni təhdidlərin aşkar edilməsinə və onlara qarşı effektiv mübarizə aparmağa imkan verər.**

Açar sözlər — kompüter təhlükəsizliyi; kompüter şəbəkələri; təhlükəsizlik trendləri; təhdidlər.

I. GİRİŞ

İlk kompüter şəbəkələri (KŞ) yarananda onların miqyası və müəkkəbliyi böyük deyildir. Lakin, informasiya və kommunikasiya texnologiyaları (İKT) sürətlə inkişaf etdikcə KŞ-lərin populyarlığı artmış və cəmiyyətin müxtəlif fəaliyyət sahələrində geniş tətbiq olunmağa başlanmışdır. Demək olar ki, cəmiyyət getdikcə KŞ-lərdən asılı vəziyyətə düşmüşdür. Bununla yanaşı KŞ-lərin mürəkkəbliyi artmış və miqyası çox geniçlənmişdir. Bu gün İKT əsasında yaradılmış xidmətlərin və tətbiqlərin istifadəsi genişlənir, intellektuallığı artır və mobilləşir. Digər tərəfdən xidmətlərin inkişafı və konvergensiyası baş verir, yəni mövcud KŞ-lər verilənlər şəbəkəsindən çoxxidmətli-multimedia şəbəkəsinə çevrilir, həmçinin yeni şəbəkə arxitekturaları yaranır və şəbəkələrə giriş texnologiyaları inkişaf edir. Göstərilən texnologiyalar, xidmətlər və tətbiqlər müasir cəmiyyətin müxtəlif fəaliyyət sahələrinə (isanlararası əlaqələrə, iqtisadiyyat, təhsil, səhiyyə, maliyyə və s.) geniş nüfuz edir və onların inkişafına birbaşa təsir göstərir. Bu səbəbdən, mövcud KŞ-lərin və kommunikasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi çox mühüm məsələyə çevrilir. Çünki, yeni təhdidlər meydana çıxır və demək olar ki, cəmmiyətin təhlükəzisliyi müəyyən dərəcədə mövcud İKT-nin təhlükəsizliyindən asılı vəziyyətə düşür. Bu şəraitdə cəmiyyətin təhlükəsizliyinin təmin edilməsi üçün KŞ-lərdə meydana gələn yeni təhdidlərin aşkar edilməsi və aradan qaldırılması çox vacibdir. Bunun üçün, təbii ki, müasir təhlükəsizlik trendləri müəyyən edilməlidir və əminliklə demək olar ki, bu trendlər KŞ-lərin (İnternetin) inkişaf trendləri ilə sıx bağlıdır. KŞ-lərin təhlükəsizlik trendləri dedikdə, zaman keçdikcə KŞ-lərdə baş verən infrastruktur, tətbiqi və istifadə sahəsində baş verən inkişafın nəticəsində təhlükəsizlik sahəsində baş verən dəyişikliklərdir (yeni boşluqların, təhdidlərin, hücum növlərinin yaranması). Göründüyü kimi, trend zamandan asılı olan dəyişiklikdir və buna görə də trendə qısa müddətdə, cari zamanda və uzaq perspektivdə baxıla bilər.

Təqdim edilən məqalənin əsas məqsədi müasir KŞ-lərdə baş verən trendlərin analiz edilməsi və bunun əsasında onlarda baş verən təhlükəsizlik trendlərinin müəyyən edilməsi və analizidir. Çünki, bu trendləri müəyyən etmədən təhdidlərin aradan qaldırılması, hücumlara qarşı mübarizənin təşkil edilməsi və digər təhlükəsizlik məsələlərinin həlli çox çətin olar.

II. KOMPÜTER ŞƏBƏKƏLƏRİNİN İNKİŞAF TRENDLƏRİ

İstənilən sahənin təhlükəsizlik trendlərinin müəyyən edilməsi üçün əvvəlcə həmin sahədə baş verən inkişaf trendlərinin müəyyən edilməsi və analizi çox vacib məsələdir. Ona görə də bu bölmədə KŞ-lərin inkişaf trendlərinin analizinə baxılır.

KŞ-lərin inkişaf trendlərini bir-neçə istiqamətə ayırmaq olar. Bu istiqamətlərə infrastruktur trendlərini, tətbiqlərin trendlərini və istifadə trendlərini aid etmək olar. Məsələn, İnternet yarandan bu günə kimi həm infrastruktur, həm tətbiqlər və həm də istifadə sahəsində əsaslı trendlər baş vermişdir.

İnternetin inkişafını şərti olaraq üç mərhələyə bölmək olar. Birinci mərhələ 1969-1992-ci illəri əhatə edir. Bu mərhələdə tədqiqat şəbəkələri yaradıldı və əsasən Telnet, Email, File Transfer kimi xidmətlər istifadə edilirdi. Bu mərhələdə şəbəkələrin və xidmətlərin istifadəçilərinin sayı az və şəbəkə trafikinin həcmi kiçik idı. Bununla yanaşı, kompüterdə işləməyi bacaran insanlar əsasən qapalı mühitdə işləyirdilər. Məsələn, 1969-cu ildə Amerika birləşmiş ştatlarında ARPAnet ilk qapalı şəbəkə yaradıldı və bu şəbəkədəki hər hansı hostla birləşmək üçün müəyyən ARPAnet IMP (Interface Message Processor) qovşağına qoşulmaq lazım idi. Daha sonra, keçən əsrin 70-ci illərində ALOHAnet, Havay adalarındakı universiteteləri birləşdirən peyk şəbəkəsi kimi yeni paket kommutasiyalı şəbəkələr yaradıldı [1]. İkinci mərhələ keçən əsrin 90-cı illərini əhadə edir. Bu mərhələdə kommersiya xidmətləri, ISP-lər (internet service provider) yarandı, Web və P2P xidmətləri istifadə edilməyə başlandı. Bunun nəticəsində şəbəkələrin sayı, istifadəçilərin sayı və şəbəkə trafikin həcmi sürətlə artdı. Bu zaman əsas problem şəbəkənin buraxma qabiliyyəti və ünvanlama ilə bağlı idi. Üçüncü mərhələ isə indiki zamanı əhatə edir. Bu gün xidmətlər inkişaf və konvergensiya edir (Internet/Telecom/Media). Şəbəkələrin və xidmətlərin istifadəsi genişlənir, intellektuallığı artır və mobilləşir, kompüterlərin hesablama gücünün artması ilə yeni şəbəkə xidmətləri (Cloud Computing, Payment Card Industry, Internet Banking və s.) meydana gəldi. İnternetdə böyük

həcmdə kontent və multimedia xidmətləri yarandı. Yeni şəbəkə texnologiyaları (məsələn, mobil texnologiyalar) meydana çıxdı və nəticədə yeni şəbəkə arxitekturaları və şəbəkə idarəetmə texnologiyaları (məsələn, veb-əsaslı idarəetmə texnologiyası) yaranmağa başlandı. Bütün bunların nəticəsində İnternet istifadəçilərinin sayı artdı və İnternet trafikinin həcmi həddindən artıq böyüdü. Bu şəraitdə ənənəvi IPv4 protokolu miqyas və marşrutlama problemləri yaratmağa başladı. Buna görə də, İnternet protokolunun (IP protokolunun) effektiv marşrutlamanı, xidmətlər üçün yüksək QoS (quality of service) və mobilliyi, təhlükəsizliyi və olduqca geniş ünvan fəzasını təmin edən IPv6 [2] versiyası tətbiq edilməyə başlanmışdır. IPv6-nın geniş ünvan fəzası təmin etmək imkanı "əşyaların interneti" [3] anlayışının meydana gəlməsinə səbəb oldu. Hal-hazırda marşrutlayıcılarda, şəbəkələrarası ekranlarda və digər kritik qurğularda IPv6 təhlükəsilik funksuyalarının və IPv6 üzrə sınaqların və təcrübənin olmadığı üçün əksər provayderlər IPv4-dən IPv6-ya keçidi yavaş həyata keçirirlər və yaud onları paralel işlədirlər.

Həmçinin, geniş zolaqlı şəbəkələr yaradıldı və onlara əsaslanan xidmətlərə və onların çatdırılma sürətinə tələbin artması yeni giriş infrastrukturun yaradılmasına gətirib çıxardı. Digər tərəfdən, verilənlərin yüksək sürətlə ötürülməsinin təmin edilməsi üçün geniş zolaqlı mobil GSM (Global System for Mobile) şəbəkələri meydana gəldi. Həmçinin, naqilsiz lokal şəbəkə texnologiyası (WI-FI) [4, 5] və WiMAX (Worldwide Interoperability for Microware Access) [6] və NFC (Near Field Communications) [7] kimi naqilsiz şəbəkələr yarandı

Bu gün ədəbiyyatda artıq koqnitiv şəbəkə anlayışına rast gəlinir [8, 9]. Bu cür şəbəkələrin arxitekturası koqnitiv proseslərdən ibarətdir və cari reallığı qiymətləndirə, gələcəyi proqnozlaşdıra və planlaşdıra bilər və onlara uyğun fəaliyyət göstərə bilər. Şübhəsiz qəbul olunmuşdur ki, koqnitiv şəbəkələr fikirləşmək, öyrənmək və yadda saxlamaq qabiliyyətinə malikdir.

KŞ infrastukturunun genişlənməsi (geniş zolaqlı naqilli və naqilsiz şəbəkələrin geniş yayılması), kompüterlərin hesablama gücünün artması və yaddaş texnologiyasının inkişaf etməsi real zaman rejimində virtual hesablama və yaddaş infrastrukturunun yaradılmasına və veb-əsaslı hesablamaların həyata keçirilməsinə, yəni bulud hesablamanın həyata keçirilməsinə imkan verir. İnternetə qoşulmuş istifadəçilər dünyanın istənilən nöqtəsində yerləşmiş hesablama və yaddaş resursalarına giriş əldə edə bilərlər. Verilənlərin emalı mərkəzlərinin virtuallaşması yeni konsepsiya deyil və bu gün verilənlərin emalı mərkəzlərində serverlərlə yanaşı digər resursların (məsələn, kommutatorların, marşrutlayıcıların və saxlancların) virtuallaşması nəzərdə tutulur. Virtual resurslar müəyyən fiziki resursları birləşdirir və bu resurslara şəbəkənin və dünyanın istənilən yerindən giriş əldə etmək olar və nəticədə vahid lokal resurs təəssüratı yaradır [10].

İnternetin bir-neçə onilliklər ərzində müvəffəqiyyətlə inkişaf etdirilməsi demək olar ki, bu gün İnterneti daha çevik, irimiqyaslı, etibarlı və təhlükəsiz etmişdir. İlk ənənəvi İnternet xidmətləri – faylların ötürülməsi və email xidmətlərindən sonra həm ənənəvi, həm də mobil İnternet xidmətləri və tətbiqlərinin yaradılması və inkişafı sahəsində böyük trendlər baş vermişdir. Həmçinin veb saytların yaradılmasında böyük trendlər baş vermişdir, məsələn bu gün veb saytların sayı bir milyarda yaxınlaşır [11] və onların yaradılmasında yeni texnologiyalar istifadə edilir. Bununla yanaşı, son illər sosial şəbəkələr, bulud hesablaması, P2P və sair kimi yeni xidmətlər yaradıldı və inkişaf etdirildi.

KŞ-lərdə yeni şəbəkə xidmətlərinin yaranması istifadəçilərə böyük seçim imkanı verdi və sosial-iqtisadi qarşılıqlı əlaqə üçün geniş imkanlar yaratdı. Bu da KŞ-lərin (İnternetin) sosial-iqdisadi sferada geniş istifadəsinə gətirib çıxarmışdır. Bu gün dünya üzrə İnternet istifadəçilərin sayı üç milyardı keçmişdir, İnternetin gündəlik trafikinin (ənənəvi və mobil trafiklər birlikdə) həcmi eksabaytla ölçülür, gündəlik emaillərin sayı 100 milyarada yaxın olur, Google və Facebook-un aktiv istifadəçilərinin sayı bir milyadı keçmişdir. İnternetin istifadəsi ilə bağlı digər tredlər haqqında məlumatları [11]-də almaq olar.

Təbii ki, KŞ-lərdə (İntranetdə) yuxarıda göstərilən istiqamətlər üzrə baş verən trendlər kompüter təhlükəsizliyinə bu və ya digər şəkildə təsir göstərir, yeni təhdidlər yaradır və təhlükəsizliyin təmin edilməsini çətinləşdirir.

III. KOMPÜTER ŞƏBƏKƏLƏRİNİN TƏHLÜKƏSİZLİK TRENDLƏRİ

Qeyd etmək lazımdır ki, KŞ-nin təhlükəsizliyi öz növbəsində İKT-nin, həmçinin İnternet xidmətlərinin inkişafında çox vacib rola malikdir. KŞ-nin təhlükəsizliyinin təmin edilməsi və vacib informasiya infrastrukturunun mühafizəsi hər bir təşkilatın, ölkənin təhlükəsizliyi üçün çox vacibdir. Təhlükəsiz İnternet yeni xidmətlərin yaranmasına və inkişafına şərait yaradır. KŞ-nin təhlükəsizliyinin yüksək səviyyədə təmin edilməsi üçün ən vacib addımlardan biri təhlükəsizlik trendlərinin müəyyən edilməsidir.

Analiz göstərir ki, bu gün KŞ təhlükəsizliyi sahəsində baş verən başlıca trend ondan ibarətdir ki, hücumlar əsasən şəbəkə infrastrukturunun və ya qovşaqlarının sıradan çıxarılmasına deyil, informasiyanın (verilənlərin, məsələn, korporativ, fərdi və s verilənlərin.) əldə edilməsinə yönəlmişdir. Şəxsi həyatın toxunulmazlığına və verilənlərin oğurlanmasına yönəlmiş hücumlar əsas təhlükəsizlik trendlərinə aid edilir. Bu gün fərdlər və təşkilatlar öz vacib informasiyalarını İnternetdə saxlamağa başlayıblar və buna görə də təhlükəsizlik tələbləri dəyişir. Təhlükəsizliyin təmin edilməsində əsas yanaşma sistemin təhlükəsizliyi ilə bərabər informasiyanın (verilənlərin) təhlükəsizliyinin təmin edilməsindən ibarətdir.

Təhlükəsizlik trendlərindən biri də hücum vasitələrinin avtomatikləşmə səviyyəsinin getdikcə artması ilə bağlıdır. Avtomatik hücumlar adətən dörd fazadan ibarət olur və bu fazalardan hər biri dəyişə bilər. Bu fazalara potensial qurbanın tapılması, zəif sistemin sıradan çıxarılması, hücumun yayılması və hücum vasitələrinin əlaqələndirilmiş idarə edilməsi daxildir. Bununla yanaşı hücum vasitələri təkmilləşir və hücum vasitələrinin yaradıcıları daha yeni inkişaf etdirilmiş üsullardan istifadə edirlər. Bu hücum vasitələrinin izini mövcud antivirusların və hücumların aşkar edilməsi sistemlərinin köməyi ilə aşkar etmək çətinləşir.

Digər bir təhlükəsizlik trendi mobil qurguların geniş istifadəsi ilə bağlıdır. Belə ki, mobil qurğuların sayının artması təhlükəsizlik risklərinin eksponensial şəkildə artmasına gətirib çıxarmışdı. Məsələn, 2017-ci ilə 8,6 milyard portativ və ya personal mobil qurğu olacağı gözlənilir [12]. Hər bir yeni smartfon, planşet və ya digər mobil qurğu kiber-hücumlar üçün yeni imkan yaradır, çünki hər bir belə mobil qurğu şəbəkəyə yeni zəif giriş nöqtəsi yaradır. Bununla yanaşı mobil tətbiqləri istifadə edən çoxlu ziyankar proqram təminatları yaradılmışdır. Məsələn, IPhones və Android qurğuları üçün nəzərdə tutulmuş ziyankar proqramların və onların yoluxdurduğu qurğuların sayı həndəsi silsilə üzrə artır.

Daha bir təhlükəsizlik trendi sosial medianın geniş istifadəsi ilə bağlıdır. Sosial medianın istifadəsi şəxsi təhlükəsizlik üçün kiber təhdid yaradır. Təşkilatlarda sosial medianın geniş istifadəsi hücumların kəskin artması təhlükəsi yaradır və sosial mühəndisliyin həyata keçirilməsi üçün əlavə kanal yaradır. Bu sahədə risklərin minimallaşdırılması üçün təşkilatlar informasiya sızmasının qarşısının alınması, şəbəkənin monitorinqi və loq faylların analizi üçün qabaqcıl texnologiyalardan istifadə etməlidir.

Bu gün əsas təhlükəsizlik trendlərindən biri bulud hesablaması mühitinin təhlükəsizliyinin təmin edilməsi ilə bağlıdır [13, 14]. Təşkilatlar xərcləri azaltmaq və effektivliyi artırmaq üçün işlərini bulud hesablaması mühitinə keçirirlər. Yaxşı yaradılmış arxitektura və yaxşı planlaşdırılmış əməliyyat təhlükəsizliyi təşkilatlara bulud hesablamalarda riskləri effektiv idarə etməyə imkan verər. Bütün bu məsələləri bulud hesablaması xidməti göstərən provayder öz üzərinə götürür. Lakin təşkilatlar bulud mühitinə keçən kimi bədəməllər də həmin mühitə keçir. Buna səbəb odur ki, çox zaman təşkilatlar öz korporativ verilənlərini də buluda köçürürlər. Bulud hesablama mühitinə hücumların əsas məqsədlərindən biri bu mühitə daxil olmaq və korporativ, həmçinin fərdi verilənlərin ələ keçirilməsidir.

NƏTİCƏ

Bu gün KŞ-lər demək olar ki, cəmiyyətin fəaliyyətinin bütün sahələrində, məsələn, sənyenin müxtəlif sahələrində, müəssisələrdə, dövlət idaretmə və özəl təşkilatlarda istifsdə edilir. Bununla yanaşı, KŞ-lər çox böyük süətlə inkişaf edir və müxtəlif infrastruktur, tətbiqi və istifadə trenləri ilə müşayət olunur. Bu da öz növbəsində kompüter təhlükəsizliyinə bilavasitə təsir edir, yəni yeni təhlükəsizlik trendlərinin meydana gəlməsinə səbəb olur. Demək olar ki, kompüter təhlükəsizliyi sahəsindəki trendlərin yaranma süəti. İKT sahəsindəki trendlərlərin yaranma sürəti ilə düz mütənasibdir. Bu da kompüter təhlükəsizliyinin pozulması (xüsusi ilə də, kritik infrastrukturların) risklərini həddindən çox artırır və nəticədə ölkələrin milli və sosial-iqtisadi təhlükəsizliyinə ciddi təhdidlər yaradır. Bu şəraitdə kompüter təhlükəsiliyi sahəsindəki trendlərin müəyyən edilməsi və analizi çox vacib məsələdir. Bu trendlərin vaxtında müəyyən edilməsi yeni yaranan təhdidlərə qarşı effektiv mexanizmlərin yaradılmasına imkan verərr.

MİNNƏTDARLIQ

Bu iş Azərbaycan Respublikasının Prezidenti yanında Elmin İnkişaf Fondunun maliyyə yardımı ilə yerinə yetirilmişdir – Qrant № EİF-RİTN-MQM-2/İKT-2-2013-7(13)-29/27/1.

ƏDƏBİYYAT

[1] N. Abramson, “The Aloha system - Another alternative for computer communications,” Proceedings of Fall Joint Computer Conference, AFIPS Conference, 1970, p.37.

[2] https://tools.ietf.org/html/rfc2460

[3] S. Agrawal, D. Vieira, “A survey on Internet of Things,” Abakys, Belo Horizonte, 2013, v. 1, n. 2, pp. 78-95.

[4] http://www.tra.gov.eg/uploads/technical%20material/Wi-Fi%20report.pdf

[5] S. K. Mohapatra, R. R. Choudhury, P. Das, “The future directions in evolving wi-fi: technologies, applications and services,” International Journal of Next-Generation Networks, vol.6, no.3, pp.13-22, 2014.

[6] http://media.johnwiley.com.au/product_data/excerpt/0X/04706968/047069680X.pdf

[7] http://www4.kfupm.edu.sa/ssc/4845_MohammedUmair_Yaqub.pdf

[8] R.W. Thomas, “Cognitive networks,” Ph.D. Dissertation, Virginia Polytechnic and State University, 2007.

[9] Q. Mahmoud, “Cognitive networks – Towards self-aware networks.” John Wiley and Sons, 2007.

[10] http://newsroom.cisco.com/dlls/2008/ts_012808.html

[11] http://www.internetlivestats.com/

[12] http://newsroom.cisco.com/documents/10157/1142732/Cisco_VNI_Mobile_Data_Traffic_Forecast_2012_2017_white_paper.pdf

[13] A. Behl, K. Behl, “An analysis of cloud computing security issues,” Information and Communication Technologies (WICT), World Congress, pp. 109-114, 2012.

[14] D. H. Parekh, R. Sridaran “An analysis of security challenges in cloud computing,” International Journal of Advanced Computer Science and Applications, vol. 4, no.1, pp. 38-46, 2013.