Qurbanov Fərhad İmran oğlu, müəllim,
Bakı Biznes Universiteti,
Email: f.qurbanov@yahoo.com

MALİYYƏ SİSTEMLƏRİNƏ KİBERHÜCUMLAR VƏ KİBERTƏHLÜKƏSİZLİYİN TƏMİN EDİLMƏSİ

Kibertəhlükəsizlik kiberməkanı təşkil edən informasiya texnologiyaları sistemlərini təhdidlərdən qorumaq, oradakı məlumatların məxfiliyini, bütövlüyünü və əlçatanlığını təmin etmək, hücumları və kiber vəziyyətləri müəyyən etmək, bu təsbitlər üçün tədbirlər görmək və sonra kibertəhlükəsizlik hücumundan əvvəl sistemlərdə rast gəlinən problemləri aradan qaldırmaq üçündür (2016-2019 Milli Kibertəhlükəsizlik Strategiyası, 2018).

Türkiyə Cümhuriyyətinin 2013-2014-cü illər üçün Milli Kibertəhlükəsizlik Strategiyası Fəaliyyət Planının 11-ci maddəsində, kibertəhlükəsizlik riskləri ilə bağlı institusional və şəxsi məlumatlılıq səviyyəsinin lazımi səviyyədə əldə edilmədiyi vurğulanmışdır. Milli kibertəhlükəsizliyin təmin edilməsi baxımından, prinsiplərin 4-cü maddəsində qeyd olunur ki, fərdlər, qurumlar, cəmiyyət və dövlət HS-nin təmin edilməsində hüquqi və sosial öhdəliklərini yerinə yetirməlidir (Yeniman Yıldırım və Adalı, 2017).

Türkiyə Cümhuriyyətinin 2016-2019 Milli Kibertəhlükəsizlik Strategiyası Fəaliyyət Planında ən mühüm risklər bunlardır:

a) sosial şəbəkələrdən asılılıq;

b) kiber məkanda qurumların mövqeləri;

c) kibercasusluq fəaliyyətləri və məqsədyönlü hücumlar;

ç) kibertəhlükəsizlik kadr, bilik, bacarıq və təcrübə;

d) qurumlar arasında koordinasiyanın olmaması;

e) kiberməkanda müxtəlif ölçülərdə fəaliyyət göstərən sektorların iqtisadi problemləri (2016-2019 Milli Kibertəhlükəsizlik Strategiyası, 2018).

Peşəkar hakerlər və ya haker qrupları tərəfindən maliyyə sistemlərinə korporativ və ya fərdi internet saytlarına, kompüterlər və internetlə zərər vermək məqsədi ilə edilən hücumlara “Kiber Hücumlar” deyilir .

Amerika Birləşmiş Ştatları Milli Tədqiqat Şurasının 2009-cu ildə apardığı araşdırmada kiberhücumlar "şəbəkələri, kompüter sistemlərini və ya məlumatları və onlara daxil edilmiş və ya onları daşıyan proqramları pozmaq, aldatmaq, alçaltmaq və ya məhv etmək üçün qəsdən hərəkətlər" kimi müəyyən edilir (Singer & Friedman, 2015).

Bu gün kiberhücumlar kibertəhlükəsizliyə təhlükə törətsə də, həm təşkilati, həm də fərdi olaraq bu təhdidləri başa düşmək və onlardan xəbərdar olmaq böyük əhəmiyyət kəsb edir. Əgər qurumlar və fərdlər gələcək real təhlükələri dərk etsələr və hədəflənmiş hücumların üsul və üsullarının daha geniş sahədə necə olduğunu görsələr, bu, təhlükələrə qarşı qoruyucu olacaq (Miller, 2016).

Bu sahədə ən geniş yayılmış olan aldadıcı proqram təminatının iki növü var, şifrələyicilər və bloklayıcılar.

1. Bu təhlükəli proqramla o, kompüterdəki məlumatları bloklayır və sənədləri

yenidən quraşdırmaq üçün hər dəfə insanlardan pul istəyir. Bu əsasən Windows və Android cihazlarını hədəf alır.

2. Bu gün ən çox yayılmış və ən təhlükəli Kiber Hücum proqramı «WannaCRY» bir çox böyük qurumların maliyyə sistemlərinə yayılıb. Bu proqram "qurd" adlı virus vasitəsilə kompüterlərə sızır. Bu zərərli proqram əsasən naməlum mənşəli proqramlar, forma saytları, e-poçt, saxta oyunlar, disklər vasitəsilə ötürülür. "WannaCry" təşkilatların sistemlərinə sızdığı anda zəif maşınları müəyyən edir və özünə yoluxur.

Qorunmaq üçün:

– daxil olan e-poçtun kimdən gəldiyinə və onun həqiqiliyinə tam əmin olmaq lazımdır;

– naməlum şəxslərdən və ya qurumlardan göndərilən e-poçtlardakı keçidlərə kliklənməməli və daxil olan fayllar kompüterə endirilməməlidir;

– elektron poçt və ya digər media vasitəsilə təqdim edilən veb səhifə keçidlərindən istifadə edilməməlidir;

– daxil olmaq istədiyiniz veb-səhifələrin ünvanları brauzerin ünvan sətrində yazılmalıdır.

Bu araşdırmanın əsas məqsədi qurumların kibertəhlükəsizlik üzrə səylərini müəyyən etmək, onların məlumatlılıq səviyyələrini ölçmək, kiberhücumların səbəb olduğu kibertəhlükəsizlik risklərinin qurumlara təsirini qiymətləndirmək və nə etməli olduğuna dair təkliflər verməkdir. Bu gün informasiya-kommunikasiya texnologiyalarının sürətli inkişafı və internetdən geniş istifadə ilə təhlükəsizlik kibertəhlükəsizliyin riskləri də artmışdır. Bu səbəblə qurumlarda kibertəhlükəsizliyin təmin edilməsi, maarifləndirmənin artırılması və lazımi tədbirlərin görülməsinin vacibliyi vurğulanmışdır.

Bu araşdırma çərçivəsində dünyanın bəzi ölkələrində müxtəlif təhlükəsizlik qurumları tərəfindən hazırlanan kibertəhlükəsizlik anketləri araşdırıldı. Kibertəhlükəsizlik və kiberhücumlarla bağlı qurumlara sorğu tətbiq edilib. Sorğu kibertəhlükəsizlik və ümumilikdə hücumlarla bağlı görüləcək tədbirləri aşkar etmək xarakteri daşıyır. Anketlərdən əldə edilən məlumatlar ədədi və faizlə qiymətləndirilmiş və şərh edilmişdir. Bu baxış nəticəsində kiber təhdidlər və bununla bağlı görülən işlər, təhlükəsizlik riskləri, təhlükəsizlik zəiflikləri təhlil edilmiş, görüləcək tədbirlər və maarifləndirmə ilə bağlı təkliflər verilmişdir.

2016-cı il Kibertəhlükəsizliyi Pozuntuları Sorğusuna görə:

1) müəssisələrin 69%-i kibertəhlükəsizliyin yüksək səviyyəli menecerlər üçün yüksək prioritet olduğunu deyir, lakin yalnız 51%-i kiber risklərə qarşı tədbir görür;

2) 29%-i rəsmi olaraq kibertəhlükəsizlik siyasətlərini qurub;

3) 10%-i isə deyə bilərik kiber hücumların idarə edilməsinin rəsmi planına sahibdir.

2015-ci ildə iri şirkətlərin 65%-i kibertəhlükəsizliyin pozulması və hücumlarına məruz qalıb. Bu şirkətlərin 25%-i ən azı ayda bir dəfə pozuntu ilə üzləşib.

2016-cı ildə şirkətlərin kibertəhlükəsizliyinə dair ən böyük pozuntuların və hücumların 68%-i viruslar, casus proqramlar və zərərli proqramlar, 32%-i isə müəssisələr və ya şirkətlər daxilindəki insanlar tərəfindən törədilib.

Şirkətlərin 51%-i hökumətin tətbiq etdiyi kibertəhlükəsizlik tədbirlərinin 10 ad-

dımının ancaq 5 maddəsini həyata keçirir. Şirkətlərin 48%-i hökumətin kibertəhlükəsizlik mövzusuna uyğun texniki tədbirlərdən istifadə etdiyi halda, 13%-i təchizatçıları üçün müəyyən etdikləri kibertəhlükəsizlik standartlarına malikdir. Şirkətlərin 25%-i orta ölçülü, 34%-i iri şirkətlərdir (Kibertəhlükəsizliyin pozulması sorğusu, 2016).

Dünyaca məşhur maliyyə şirkətlərindən olan PwC-nin "İnformasiya Təhlükəsizliyinin Qlobal Vəziyyəti Sorğu 2017" Qlobal İnformasiya Təhlükəsizliyi Sorğusu 10 000-dən çox iştirakçı ilə sənaye sektorlarının geniş spektrini əhatə edib. Sorğuda istirak edən təşkilatların 48%-nin gəliri 500 milyon dollardır. Bu sorğuya əsasən, şirkətlərin diqqət yetirdiyi əsas məsələ, Mobil və IoT daha çox nəzarət tələb edən yeni qaydalara uyğunlaşdıqca artan hücum səthi nəticəsində yaranan mürəkkəbliyin kəskin artmasıdır. Aydın olan odur ki, təhlükəsizlik proqramları, işçilərin təlimi, ən son siyasətlər və nəzarətlər kimi əsas məsələlər hazırlığa və dayanıqlığa dair təşkilati öhdəliyə yönəldilməlidir (The Global State of Information Security Survey, 2017).

Tətbiq edilən sorğuların ümumi nəticələrinə görə;

1. Qurumların təxminən 50%-nin ümumi informasiya təhlükəsizliyi strategiyasının olmadığı və böyük bir hücum zamanı hazırlanmış bir kommunikasiya strategiyası və ya planının olmadığı görünür.

2. Əksər təşkilatlar Kiber hücumlarla mübarizə üçün lazım olan potensial təsirli tədbirləri yaxşı başa düşsələr də, təşkilatların yarısının insidentlə üzləşdiyini nəzərə alsaq, qəbul edilmiş tədbirlərin kifayət qədər güclü olmadığını və ya bir problemin olduğunu güman etmək olar.

3. Təşkilatlarda ən çox artan kiber risk təhdidləri saxta, yalançı və ya virus kompaniyalı hücumlar, fişinq, İP və ya məlumatları oğurlamaq və maliyyə məlumatlarını ələ keçirmək üçün olan kiberhücumlardır.

İstifadə olunmuş ədəbiyyat:

1. Cyber Security Breaches Survey 2016, (2016), HM Government&Social Research Institute&University of Portsmouth.
https://assets.publishing.service.gov.uk/government/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf,

2. The Global State of Information Security Survey 2017, Uncovering the Potential of the Internet of Things, (2017), PwC.
https://www.pwc.com/gx/en/issues/assets/pwc-GSISS-2017-uncovering-the-potential-of-iot.pdf,

3. The Global State of Information Security Survey 2017, Bold Steps to Manage Geopolitical Cyber Threats, (2017), PwC.
https://www.pwc.com/gx/en/issues/assets/2017-gsisss-bold-steps-to-manage-geopolitical-threats-final.pdf,

4. Global Risks Report 2017 (2017), World Economic Forum.
http://www3.weforum.org/docs/GRR17_Report_web.pdf

5. Ulusal Siber Guvenlik Stratejisi 2016 - 2019, (2018).
http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf