[4] H. Coates, R. James, G. Baldwin, "A critical examination of the effects of learning management systems on university teaching and learning", Tertiary Education and Management, vol. 11, no. 1, 2005, 19–36 pp.
[5] A. A. Sejzi and B. Aris, "Learning management system (LMS) and learning content management system (LCMS) at virtual university", in 2nd International Seminar on Quality and Affordable Education, 2013, 216–220 pp.
[6] N. N. M. Kasim, F. Khalid, "Choosing the right learning management system (LMS) for the higher education institution context: a systematic review", International Journal of Emerging Technologies in Learning (IJET), vol. 11, no. 06, 2016, 55 p.
[7] R. Agaçi, "Learning management systems in higher education,", in in EDULEARN14 Conference, 2014: Proceedings of EDULEARN14 Conference-IATED Publications, 2017, 5360–5365 pp.
[8] D. Walker, J. Lindner, "Characteristics of a large-scale LMS: a case study of Texas A&M University", Journal of Technologies in Knowledge Sharing, vol. 11, no. 3, 2015, 1–8 pp.
[9] Z. Unal, A. Unal, "Investigating and comparing user experiences of course management systems: blackboard vs. moodle", Journal of Interactive Learning Research, vol. 25, no. 1, 2019, 101–123 pp.
[10] S. Roy, "Characterizing D2L usage at the U of C", Graduate Studies, 2017, 6–7 pp.
[11] **https://docs.moodle.org/en/About_Moodle**

ŞƏBƏKƏ TƏHLÜKƏSİZLİYİNDƏ TƏHLÜKƏLƏR

Ləman Səmədzadə
Azərbaycan Dövlət Neft Və Sənaye Universiteti

Xülasə
Məqalənin əsası informasiya təhlükəsizliyi sahəsində olan şəbəkə təhlükəsizloyini ön planda tutmaqdır.Şəbəkəyə olunan bir sıra təhdidləri və istifadə edilən təhlükəsizlik üsullarını əhatə edir.Burada əsas məqsədlərdən biri də şəbəkədə qorunub saxlanan məlumatlara hakerlərin hücumunun qarşısını almaqdır. Şəbəkə təhlükəsizliyində aparılacaq tədqiqatları üçün yeni inkişaf etdirici istiqamət təklif edir.Bu məqalədə məlumatların rabitəsinin təhlükəsizliyi üçün şəbəkə təklükəsizliyinin qorunmasını əhatə edir.
Açar sözlər: Şəbəkə təklükəsizliyi, təklükəsizlik təhdidləri, təhlükəsizlik tədbirləri, firewall, hücumların aşkarlanması, təhlükəsizlik səviyyəlləri
Dövrümüzdə informasiya təhlükəsizliyi günü-gündən dahada inkişaf etməkdədi. Əsasən müasir şirkətlər informasiya təhlükəsizliyi sahələrinə yönəldikləri üçün şəbəkə təklükəsizliyi vacib anspektlərdən biridir.Sistemli şəkildə təhlükəsizliyin qarşısı alınmazsa sistemə aradan qaldərəla bilməyən ziyanlar dəyə bilər.Bu cür təklükəsizlik hallarının qarşısını almaq üçün proqram təminatə, aparat təminatı və istifadəci ehtiyaclarını özündə cəmləşdirən təhlükəsizlik tədbirləri vacibdir.Bu tədbirlərin bir qisminə aid edə bilərik, firewall, antivirus proqramları vs.[1]
Şəbəkədə istifadə edilən resursların məxfiliyinin qorunması, əlçatanlığının təmin olunması həyata keçirilir.Şəbəəkədə baş verən təhdidlər özlüyündə müxtəlif səbəblərdən yarana bilər. Bura aid edə bilərik, zərərli proqramlar, xidmətdən imtina edilməsi, baş verən fişinq hücmları, MitM adlanan ortadan adam hücmları vs.
Şəbəkə təhlükəsizliyinin tədbirləridə, şəbəkədə baş verən təhdidlərin qarşısını almaq üçündür.Şəbəkə təhlükəsizliyinin yerinə yetirdiyi təhlükəsizlik tədbirlərini effektiv şəkildə yerinə yetirilməsi

məlumatlardan icazəsiz şəkildə digər şəxslərin sui-istifadəsinin qarşısına keçir.Rəqabətin irəliləməsi üçün hər bir şirkət öz məlumatlarının məxfiliyini qorumalıdır.Əks halda məxfilik qorunmazsa məlumat itkisinə, məxfiliyin pzoulmasına və şirkət dəyərlərinin xeyli enməsinə səbəb ola bilər.Bunun üçün də bu yazı işində şəbəkə təhlükəsizliyi və yerinə yetiriləcək təhlükəsizlik tədqiqatları mövzularına toxunulacaq və analız ediləcək.[2].

Bu məqalədə məqsəd şəbəkə təhlükəsizliyinə yönələn təhlükəli vəziyyətləri araşdırmaq və onlara müəyyən həll yoları tapmaqdır.Günümüzdə informasiya təhlükəsizliyi sahəsi aktual şəkildə inkişaf etməkdədir.Ancaq inkişaf etdikcə şəbəkədəki məlumatlara qaşı qeyri-qanuni təhlükəsizlik halları baş verir.Şəbəkəyə hücumlar edilərsə hansı tədbirləri görməliyik və bu hücumların qarşısını maksimim dərəcədə hansı yollarla ala bilərik.Əsas məqsəd bu tip təhlükələri müəyyən etmək və qarşısını almaq üçün atıla biləcək addımları müəyyənləşdirməkdən ibarətdir.

Bu günə kimi təhlükəsizlik halları üçün xeyli tədqiqatlar, araşdırma işləri aparılmışdır.Bunun başlıca səbəbi informasiya təhlükəsizliyi sahəsində təməl hesab edilən tələblərdən birinin olmasıdır.Şəbəkədə baş verən təhlükəsizlik təhdidlərinə daha dərindən nəzər yetirək.Təhlükəsizlik təhdidləri dedik də, məlumatların ələ keçirilməsi üçün yerinə yetirilən hücmlar anlaşılır.Bu hücmlar bir neçə kateqoriyaya bölünür.

I. Şəbəkədə olan resurslara qeyri-qanuni giriş
II. İcazəsiz şəkildə informasiyanın manipulyasiyası
III. Əməliyyatın başa çatmasına mane olan hücmlar

Şəbəkədə olan məlumatlara qeyri-qanuni giriş dedikdə, şəbəkəyə qoyulan parola, informasiya sistemlərinə icaəsiz daxil olmaq nəzərdə tutulur. Hücum dedikdə təkcə məlumatların qeyri-qanuni yolla ələ keçirilməsi deyil dı, həmdə onların məhv edilməsi başa düşülür.Bu halın baş verməsi şəbəkəyə çox ciddi fəsadlar yetirə bilər.[3]Şəbəkədə baş verən təhlükəsizlik təhdidlərini biz iki aspekt şəklində birləşdirə bilərik.Bunlar məntiq hücmları və ya resurs hücmlarıdır.Məntiq hücumunun əasa funksiyası proqramın zəifliyini təyin etmək və icazəsiz şəkildə proqrama girişi təmin etməkdir.Resurs hücmları isə şəbəkə resurslarının bitməsinə yönəlmişdir.Təhlükəsizlik təhdidləri və hücmlar şəbəkədə yerləşən məlumatların daha əlverişli təhlükəsizliyini təmin etməyə yönəlmişdır.

1. Hücumun baş verməsi hallarına nəzər salaq bura aid edilə bilər:
2. Konfiqurasiyanın zəif olmasından və zəif şifrələrdən yararlanmaq
3. Proqram təminatında baş verən mümkün səhvlər
4. Troyya atları
5. IP ünvanlarda bir sıra saxtalaşdırma işlərinin görülməsi
6. Paylanmış hücumlar

Şəbəkəyə edilən hücumların yaratdığı fəsadlara nəzər salsaq:

1. Müəyyən bank sistemlərindən külli miqdarda pulların köçürülməsi
2. Əməliyyat problemlərini həll etmək məqsədi ilə əldə edilmiş ödənişlər
3. Əqli mülkiyyət formalarının itirilməsi
4. Tibbi verilən analiz nəticələrinin dəyişdirilməsi vs.

Hücumlar funksiyalarına görə bir necə siniflərə bölünürlər.Omlardan birincisi kəşfiyyat, ikincisi giriş, üçüncüsü xidmətin rədd edilməsidir.

- Kəşfiyyat- Sistemlərin, bir sıra xidmətlərin, yaranan zəifliklərin qeyri-qanuni şəkildə aşkarlanması.
- Giriş- Məlumatların icazəsiz şəkildə manipulyasiya edilməsi, sistemlərə girişlərin yüksəldilməsi.
- Xidmətin rədd edilməsi – sistemləri, xidmətləri icazəsiz şəkildə sıradan çıxardır.Söndürür və korlayır.

Kəşfiyyat üsullarına ümumi əmrlər və inzibatı yardım proqramları nslookup, ping, telnet, dumpacl, netcat vs aid edilir.Bunlardan əlavə icma alətləri aid edilir ki, bura sniffers, SATAN, SAİNT, NMAP vs aitdir.

Giriş üsullarına aitdir:Tətbiqi sübutlardan istifadə etmək, protokolların gücsüz tərəfləri və trojan atları. Xidmətdən istifadə üsullarına görə isə, resurslarım normadan artıq şəkildə yüklənməsi, proqram təminatında yaranan səhvlər, paylanmış hücumlar vs aitdir.

Təhlükəsizlik tədbirləri

Təhlükəsizlik tədbirləri dedikdə, şəbəkədə yerləşən məlumatların mütövlüyünü təmin etməkdən ibarətdir.Şəbəkədə yerləşən hər bir məlumatın təhlükəsizliyini təmin etmək üçün müəyyən layihələndirmə metodlarından istifadə edilir.Şəbəkələrin qorunmasını təmin etmək üçün təhlükəsizliyin bütövlüyünü təmin edən bir sıra əsas addımlar mövcutdur.Bu addımlara aşağıdakılar aid edilir.Təklükəsizliyi təmin edən divarlar, müdaxilənin müəyyən edilməsi sisteməri və qarşısının alınması prinsipləri, antivirus proqramları, bunlardan əlavə anti-spam kimi bir sıra addımlar həyata keçirilir.

Təhlükəsizlik tədbirlərini həyata keçirən zaman əlbətdəki müəyyənn risklər yaranır.Amma bu riskləri çalışdığımız qədər ən aşağı yəni minimuma endirmək məqsədə uyğundur.Bunun üçün müəyyən edilməli bir sıra əməllər var.[4].

1. Şəbəkə komponentlərinin hamısında autentikikasiya və güclü mühafizə əməliyatları olmalıdır.
2. Şəbəkədə baş verən dəyişiklikləri ardıcıllıqlar müşahidə etmək
3. Baş verən dəyişikliklərə vaxtında müdaxilə etmək.

Şəbəkə təhlükəsizliyin müntəzəm həyata keçirilməsi üçün dayanmadan ona monitorinq və baxım həyata keçirmək lazımdır.Bundan əlavə təhlükələri aradan qaldırmaq üçün davamlı olaraq mümkun risklərin qiymətləndirilməsi vacibdir.İnformasiya təhlükəsizliyinin təmin edilməsi təhlükəsizlik üçün əsas olan üç səviyyəni əhatə edir.Bu səviyyələri nəzərdən keçirək.[5].

1. İnfrastruktur təhlükəsizliyi bloku - bura ad edilir, şəbəkə xidmətləri və yerinə yetirilən tətbiqlərin vacib tikinti bloku.

Məsələn:

- Açarlar, serverlər
- Ethernet bağlantıları
- WAN əlaqələr vs.

2. Xidmətlərin təhlükəsizliyinin layeri- bura aid edilir, ən son istifadəcilərə təklif edilın xidmətlər.

Məsələn:

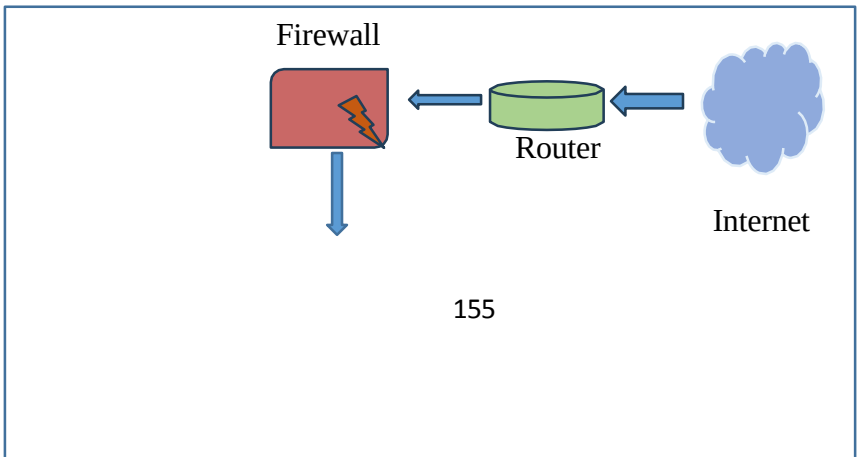
- WI-FI
- Pulsuz zəng xidmətləri
- ATM, İP vs.

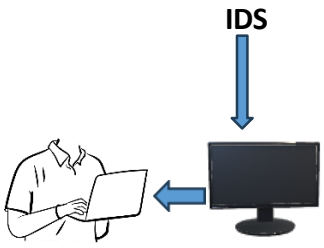
3. Tətbiqlərin təhlükəsizlik layeri- bura aid edilir, axırıncı istifadəçilərin əldə etdikləri proqramlar.

Məsələn:

- E-poçt
- Elektron ticarət

Bundan əlavə firewallın da əsas funksiyalarından biri şəbəkə istifadəçilərini ətrafdan gələn təhlükələrdən qorumaqdır.Çox hallarda şəbəkə interfeysində yaradılır.Firewallın əsas göstəricilərindən biridə hansı məlumatların sistemə giriş edə biləcəyini, hansılarının isə giriş edə bilməyəcəyini aşkar edə bilir.[6].Daha həssas olan məlumatları kibertəhlükələrdən qorumaq üçün xüsusi IDS adlanan Intrusion Detection Systemdən istifadə edilir.[7]





Şəkil 1.Hücumun aşkarlanması sistemi

Bu məlumatlar əsas üstünlüyü şəbəkəyə qeyri-qanunu girişin qarşısını almaqdır.Hücumlar viruslar,troyanlar şəbəkə vasitəsi ilə yayılırlar və bunun əlehinə çıxmaq üçün xususi tədbirlər görmək lazımdır.

Bu tədbirləri 3 mərhələdə apara bilərik:

1. Qoruma:Konfiqyrasiyanın düzgün şəkildə aparılması
2. Aşkarlama:Baş verən dəyişikliyi aşkat etmək üçün diqqətlə izləməliyik.[8]
3. Reaksiya:Hər hansı promlem aşkar edilərsə dərhal müdaxilə etmək.

Bu cür baş verən hücumların qarşısını almaq üçün bir üsuldan istifadə etmək təhlükəli hal yarada bilər.Bunun üçün şəbəkədəki təhlükələrə qarşı gəlmək məqsədi ilə şəbəkə təhlükəsizliyi üsullarından istifadə edilir.[9,10]

Bu üsullardan bir necəsi aşağıdakılardır.

1. Baş verə biləcək risklərin və gücsüzlərin müəyyənləşdirilməsi və düzgün nəzarətin yaradılması
2. İstifadəçilərin, şirkətlərin şəbəkə mühitlərini düzgün təkminləşdirmək
3. İnternet protokolları ünvanları vs hallar üçün şəbəkələrin optimallaşdırılması
4. Təhlükəsizlik hallarının müvafiq olaraq qeydə alınması üçün təkliflər.
5. Fərqli səviyyələrdə yerində və ya əksinə dövri təlim
6. Güclülük dərəcəsini müəyyən etmək üçün təhlükəsizlik sistemlərini məğlub etmək

Şəbəkə təhlükəsizliyi əməliyyat sistemlərinin təhlükəsizliklərini təmin etmək və istifadəçilərin yönəldilən xidmətlərin təhlükəsizliyini yaratmaqdan ibarətdir.Təhlükəsizliyi qorumaq və təmin etmək üçün ilkin systemin yaradılması aşağıdakılardan ibarətdir.

- Yaratdığımız hesablar üçün güclü şifrələrin təyin edilməsi
- Şəbəkə xidmətlərinin və sistemləri maksimum dərəcədə minumuma endirmək.
- Mövcud olan lazımsız proqramların çıxarılması
- Fayl icazələrinin düzəldilməsi vs.
- Giriş mexanizimlərinin konfiqurasiyasının təmin edilməsi
- Gücsuz olan giriş mexanizimlərinin daha təhlükəsiz olanları ilə əvəzlənməsi.
- Yedəklənmənin aparılması

Şəbəkəyə hər hansı giriş halı baş vermişsə diqqət yetirməliyik:Girişin əldə edilməsi üçün hansı mümkün sistemlərdən istifadə edilmişdir.Daha sonra hücum hansı sistemlərə olunub, Daxil olduğu system üçün hansı aktiv məlumatlar var idi, hücum edən hazırda nə edir.Bu zaman biz daxil olunan sistemə nəzarəti ələ keçirmyə çalışmalı, digər müdaxilələrin qarşının almaq üçün tədbirlər görməliyik.Baş verən hücumun qarşısını almaq üçün, giriş edilən sistemlərdə mövcut paroları dəyişməliyik.

Nəticə

Şəbəkə təhlükəsizliklərini həm daxili həm də xarici hücumlardan qorumaq əsasdır.Təhlükəsizlik şəbəkənin daxilində yerləşən məlumatların məxfiliyini, tamlığını və onların əlçatan olmasına şərait yaradır.Həmən bu məqsədlərə nail olmaq üçün bir neçə fikirlər təklif edilmişdir və təsdiqini

tapmışdır.Doğru şəkildə aşkarlanmış şəbəkə təhlüksizliyi bir necə hissədən ibarətdir.Bunlara aid edə bilərik, firewallar,müdaxilənin üzə çıxma sistemlərindən vs xidmətlərdən istifadə edilir.Əvvəlcədən təhlükəsizlik halları üçün sistemlərin əldə edilməsi təhlükəsizlik halarını artırır.Təşkilatların əldə etdikləri məlumatların təhlükəsizliklərini minimum etmək üçün əlverişki protokollar və bir sıra təlimatlar lazımdır.Bundan əlavə şəbəkə təhlükəsizliyi zamanı istifadə edilən avadanlıqlarda şəbəkədə baş verə biləcək təhlükələri artıra bilir.Şəbəkəyə edilən hücumların qarşısını ən effektiv şəkildə necə azalda və hansı yollarla qarşısını ala bilərik.Şəbəkə yaradan yazaman ilk öncə güclü parollrdan istifadə etmək, müxtəlif simvollardan istifadə edərək şəbəkənin təhlükəsizliyini təmin edə bilərik.Effektiv şəbəkə təhlükəsizliyi sistemə qeyri-qanuni şəkildə daxil olan girişlərin qarşısını alır və şəbəkədə mövcut olan məlumatları qoruyur.

Ədəbiyyat

[1] S. Tayal, N. Gupta, P. Gupta, D. Goyal, and M. Goyal, "A Review paperon Network Security and Cryptography." Advances in Computational Sciences and Technology, vol. 10 (5), pp. 763-770, 2017.

[2] R. Khan, and M. Hasan, "Network threats, attacks and security measures: A review." International Journal of Advanced Research in Computer Science, vol. 8 (8), pp. 116-120, 2017.

[3]]A. Tayal, N. Mishra, and S. Sharma, "Active monitoring & postmortem forensic analysis of network threats: A survey." International Journal of Electronics and Information Engineering, vol. 6 (1), pp. 49-59, 2017.

[4] S. Rathore, P. K. Sharma, V. Loia, Y.-S. Jeong, and J. H. Park, "Social network security: Issues, challenges, threats, and solutions." Informationsciences, vol. 421pp. 43-69, 2017.

[5] H. I. Kobo, A. M. Abu-Mahfouz, and G. P. Hancke, "A survey on software-defined wireless sensor networks: Challenges and design requirements." IEEE access, vol. 5pp. 1872-1899, 2017.

[6] D. Barrera, I. Molloy, and H. Huang "Standardizing IoT network security policy enforcement," In: Workshop on Decentralized IoT Security and Standards (DISS). p 6, 2018.

[7] T. Hayajneh, S. Ullah, B. J. Mohd, and K. S. Balagani, "An enhanced WLAN security system with FPGA implementation for multimediaapplications." IEEE Systems Journal, vol. 11 (4), pp. 2536-2545, 2015.

[8] P. Sinha, V. Jha, A. K. Rai, and B. Bhushan "Security vulnerabilities attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey," In: 2017 International Conference on Signal Processing and Communication (ICSPC). IEEE, pp. 288-293, 2017.

[9] S. Zheng, Z. Li, and B. Li "Implementation and application of ACL in campus network," In: AIP Conference Proceedings. vol 1. AIP Publishing LLC, p 090014, 2017.

[10] V. Pruthi, K. Mittal, N. Sharma, and I. Kaushik "Network Layers Threats & its Countermeasures in WSNs," In: 2019 International Conference on Computing, Communication, and Intelligent Systems(ICCCIS). IEEE, pp. 156-163, 2019.

ZƏRƏRLİ PROQRAM VASİTƏLƏRİ

Seyidsoylu Sevil

Azərbaycan Dövlər Neft Və Sənaye Universiteti

Xülasə

Məqalənin əsası zərərli proqramlar və onların təhlili təşkil edir.Təhlil üsullarından istifadə etməklə proqramı baş verəcək təhlükələrdən qorunma məsələlərinini əhatə edir.Burada əsas məqsədlərdən biri odur ki, kompüterin və yaxud faylın hakerlər tərəfindən hücumuna məruz qalmağının qarşısını almaqdır.Həmçinin məqalədə zərərli proqramları təhlil olunaraq,ən əlverişli üsullarla qorunmaqdan da bəhs olunur.

Açar sözlər-Zərərli proqram, zərərli proqramların aşkarlanması, təhlili, yoluxmanın qarşısının alınması, spyware,təhlil alətləri.

Giriş