İDARƏETMƏ ORQANLARINDA KOMPÜTER ŞƏBƏKƏLƏRİNİN TƏHLÜKƏSİZLİK PROBLEMLƏRİNİN ARAŞDIRILMASI

GÜLŞƏN NAZİM QIZI MƏMMƏDOVA

Azərbaycan Respublikasının Prezidenti Yanında Dövlət İdarəçilik Akademiyası
glsnmmmdv@gmail.com

Məlumatların sürətli artımı müxtəlif sənayelər üçün ciddi problemlər yaradır və həmçinin qiymətli imkanlar gətirir. Şəbəkə böyük verilənləri(Network big data) kiberməkanda “insanların, maşınların və obyektlərin” qarışması nəticəsində yaranan və İnternetdə mövcud olan böyük verilənlərə aiddir[1]. Şəbəkə böyük verilənləri, miqyasından və mürəkkəbliyindən asılı olmayaraq, mövcud kompüterlərin işlənməsini çətinləşdirir. Şəbəkə böyük verilənləri ilə bağlı araşdırmalar böyük əhəmiyyət kəsb edir. Hazırda əlaqəli tədqiqatlar əsasən üç aspektə, yəni şəbəkə böyük məlumatlarının təmizlənməsi, saxlanması və təhlilinə yönəlib. Şəbəkə böyük verilənləri tez-tez əlaqələrin monitorinqi, nümunə və açar söz axtarışı, məlumat mühəndisliyi və s. sahələrdə istifadə olunur. Yaxın gələcəkdə bu texnologiya müxtəlif sənayelərdə inqilab edəcək, insanların daha səmərəli emal və tətbiqi üçün dəyərli məlumat əldə etməsini asanlaşdıracaq[2].

İnformasiyalaşdırma prosesinin davamlı dərinləşməsi və sürətlə inkişaf edən şəbəkə texnologiyası ilə şəbəkə təhlükəsizliyi sahəsinin konnotasiyası getdikcə genişlənir və tədricən çoxqatlı üçölçülü şəbəkə arxitekturasının təhlükəsizliyinə dərinləşir. Kompüter şəbəkəsinin təhlükəsizliyinin əsas xüsusiyyətləri əlçatanlıq, tamlıq, məxfilik, idarə oluna bilənlik və etibarlılıqdır[3]. Təhlükəsizliyin qorunması nöqteyi-nəzərindən kompüter şəbəkəsinin təhlükəsizliyi konsepsiyası üç hissədən ibarətdir: şəbəkə platformasının əməliyyat təhlükəsizliyi, fiziki təhlükəsizlik və təhlükəsizliyin idarə edilməsi. Fiziki təhlükəsizlik təməldir və şəbəkə platformasının əməliyyat təhlükəsizliyinə və təhlükəsizliyin idarə olunmasına z əmanət verilir. Birlikdə onlar nisbətən tam şəbəkə təhlükəsizlik mühafizə sistemini təşkil edirlər. Şəbəkəyə müdaxilə mücərrəd bir anlayışdır. Şəbəkəyə müdaxilə şəbəkə resurslarına müəyyən ziyan vura bilər. Bu zərərlər əsasən üç aspektdə əks olunur: biri şəbəkə resurslarının bütövlüyünü pozmaq, digəri şəbəkə resurslarının əlçatanlığını pozmaq, üçüncüsü isə şəbəkəni resursların məxfiliyini məhv etmək və bu təxribatlar şəbəkə təhlükəsizliyi problemlərinə səbəb ola bilər. Şəbəkəyə müdaxilə nöqteyi-nəzərindən şəbəkə müdaxiləsi maskalanma hücumları, xidmətin rədd edilməsi hücumları, təhlükəsizlik səviyyəsinin yüksəldilməsi hücumları və müdaxiləyə cəhd edilən hücumlara bölünə bilər.

Aşkarlama şəbəkədə görünə bilən və ya artıq görünən şəbəkə müdaxiləsi davranışını aşkar etmək və beləliklə, müdaxilə davranışına cavab vermək üçün istifadə olunur. Şəbəkə müdafiə üsulları baxımından müdaxilənin aşkarlanması aktiv müdafiə texnologiyasıdır. Şəbəkədəki kommunikasiyaları, hostları, jurnalları və s.-nin təhlili və

aşkarlanması ilə şəbəkə məlumatları və davranışı müdaxilə davranışlarını aşkar etmək və müdaxilə davranışlarına cavab vermək üçün təhlil edilir, şəbəkə resursları məhv edilir, şəbəkə hücumlarının qarşısını effektiv şəkildə alır. Müdaxilənin aşkarlanması təkcə şəbəkədən kənar davranışları hədəfə almır, həm də şəbəkə daxilindəki şəbəkə davranışlarını aşkarlayır. Müdaxilənin aşkarlanmasının əsas prinsipi şəbəkə müdaxiləsi davranışının şəbəkə sistemindəki normal şəbəkə davranışından fərqli olduğunu güman etməkdir, beləliklə, müdaxilənin aşkarlanması sistemi, şəbəkə qeydlərini və audit qeydlərini təhlil etməklə həyata keçirilə bilər. Hücumun aşkarlanması sistemi aşağıdakı funksiyaları təmin etməlidir: Birincisi, müdaxilənin aşkarlanması sistemi sistem administratoruna şəbəkə sistemindəki müxtəlif aparat və proqram təminatı dəyişikliklərini, əməliyyat prosedurlarını, rabitə dəyişikliklərini və s. anlamaqda kömək edə bilər. Hücumun aşkarlanması sistemi, həmçinin, sistem intruziyasının aşkarlanması sistemini də inkişaf etdirməlidir. İkincisi, şəbəkə müdaxiləsinin aşkarlanması sistemi sadə və istifadəsi asan idarəetmə üsulu ilə şəbəkəni izləyir və idarə edir. Şəbəkə administratoru şəbəkə sisteminin təhlükəsizliyini artırmaq üçün müdaxilənin aşkarlanması sistemi vasitəsilə şəbəkə təhlükəsizliyinin müxtəlif konfiqurasiyalarını həyata keçirə bilər. Üçüncü müdaxilə aşkarlama sistemi sürətli cavab səviyyəsinə malik olmalıdır. Müdaxilə aşkar edildikdə, o, sistem jurnalında zərərli davranışı vaxtında qeyd edə və müvafiq şəbəkə bağlantısını silmək və administratora həyəcan siqnalı vermək kimi zərərli davranışa müsbət cavab verə bilər[4]. Şəbəkəyə müdaxilənin aşkarlanması hostlar arasında şəbəkə xəttində ötürülən məlumatları təhlil etməklə işləyir. Şəbəkə vasitəsilə real vaxt rejimində məlumat axınına nəzarət etmək və təhlil etmək üçün adətən "Promiscuous Mode" rejimində işləyən şəbəkə kartından istifadə edir. Onun təhlil modulu adətən hücum davranışlarını müəyyən etmək üçün nümunə uyğunluğu və statistik təhlil kimi üsullardan istifadə edir. Şəbəkə şirkətləri, hökumət və digər aidiyyatı idarələr üçün onlar kompüter şəbəkəsinin monitorinqi texnologiyasını davamlı olaraq təkmilləşdirməli və şəbəkə monitorinqinin bu intellektual texnologiyası vasitəsilə şəbəkəni hərtərəfli idarə etməlidirlər. Kompüter şəbəkələri üçün bəzi sahələr insan monitorinqi ilə tam əhatə oluna bilməz, bu zaman siz intellektual texnologiyanın dəqiq monitorinq xüsusiyyətlərindən istifadə edə bilərsiniz. Virus müdaxiləsi verilənlər bazası qurulması, monitorinq modelinin qurulması və anormal monitorinq texnologiyaları şəbəkə monitorinq texnologiyalarıdır. Mümkün qədər qeyri-qanuni müdaxilənin qarşısını almaq üçün sistem proqramlarının hazırlanması, istismarı və tətbiqi zamanı monitorinq texnologiyasından istifadə oluna bilər. Bundan əlavə, məlumat ötürülməzdən əvvəl məlumatı yenidən kodlayın ki, ələ keçirən məlumatın həqiqi məzmununu ala bilməsin. Məlumat şifrələmə texnologiyası məlumatların təhlükəsiz ötürülməsinə zəmanət verən kompüter şəbəkələrində əsas təhlükəsizlik texnologiyasıdır. Hal-hazırda, asimmetrik açar şifrələməsi ən çox istifadə edilən şifrələmə üsuludur və onun təhlükəsizliyi simmetrik şifrələmədən daha yüksəkdir. O, bir-biri ilə əlaqəli bir cüt açardan istifadə edir, onlardan biri ictimai, digəri isə özəldir. Hazırda nisbətən təhlükəsiz asimmetrik şifrələmə alqoritmlərinə əsasən RSA, DSA, PKCS və PGP daxildir [5]. Bəzi şəbəkə nümunəsi təhlilinin köməyi ilə istifadəçilər kompüter şəbəkələrinin təhlükəsizlik müdafiəsini həyata keçirməyə və onları qeyri-qanuni müdaxilələrin zərərliliyi və şəbəkə təhlükəsizliyi tədbirlərinin vacibliyi barədə xəbərdar olmağa təşviq edilir. İstifadəçi adları və təhlükəsizlik parollarını təyin edərkən istifadəçilərə daha yüksək təhlükəsizlik

səviyyələrinin birləşməsindən istifadə etməyə icazə verilir. Məsələn, krekinq çətinliyini artırmaq üçün simvollar, hərflər və rəqəmlər qarışdırıla bilər. Fərqli saytlar üçün eyni paroldan istifadə etməmək lazımdır. Eyni zamanda, onun təhlükəsizliyini artırmaq üçün müntəzəm parol dəyişikliyi etmək lazımdır. Digər tərəfdən, hər bir istifadəçi öz giriş hüquqlarına malik olmaq üçün onların şəbəkə marşrutlaşdırıcıları mümkün qədər öz giriş hüquqları ilə məhdudlaşdırılmalıdır. İstifadəçilər şəxsi məxfi məlumatları ehtiva edən bəzi proqram təminatı və vebsaytlara daxil olmaq üçün ictimai WİFİ tətbiq etməməlidirlər.

Ədəbiyyat

1. Yang, J.W. (2019) A brief analysis of computer network security precautions in the era of big data. Science and Technology Communication, no.2, pp.108-109.
2. Long, Z.H. (2019) Computer network information security and protection strategy in the era of big data. Management Informationization in China, no.3, pp.161-162.
3. Deng, Q.F. (2019) Computer network information security technology and its development trend. Electronic Technology and Software Engineering, no.24, pp.194-195.
4. Liu, W. (2018) Research on Optimizing Network Security Strategy Based on Big Data. Software, vol.39, no.9, pp.205-208.
5. Zhao, L. (2019) Research on computer network security protection strategy under the background of big data. Journal of Heihe University, vol.10, no.1, pp.217-218.
6. Wang, Q., Pan, C. (2017) Analysis of Network Complete Vulnerabilities and Preventive Measures in the Era of Big Data. Network Security Technology and Application, no.2, pp.77 - 79.
7. Bao, L.J. (2019) Application of Big Data-based Network Security Situation Awareness Platform in Private Network Field. Information Security Research, vol.5, no.2, pp.168-175.
8. Wang, B. (2019) Network security fuzzy risk assessment based on computer network technology. Foreign Electronic Measurement Technology, vol.38, no.5, pp.11-16.
9. Liu, Q., Cai, Z.P., Yin, J.P., et al. (2017) Research on the framework and methods of network security detection. Computer Engineering and Science, vol.39, no.12, pp.2224-2229