https://doi.org/10.36719/2706-6185/44/388-391

Tura Quliyeva
Azərbaycan Universiteti
https://orcid.org/0009-0009-4224-025X
tura.guliyeva@student.au.edu.az

Neft və qazçıxarma şirkətlərinin informasiya təhlükəsizliyinə təhdidlər

Xülasə

Hücumlar və daxili təhdidlər şirkətin həm maddi, həm də qeyri-maddi aktivlərini risk altında qoyur. Avadanlıqlarla bağlı problemlər istehsal prosesini dayandırmaq və ətraf mühiti çirkləndirmək təhlükəsi yaradır ki, bu da milyonlarla dollar itki ilə nəticələnir və ictimai etirazların artmasına səbəb olur. Qlobal və milli iqtisadiyyatlar üçün kritik əhəmiyyətinə görə kibertəhlükəsizlik neft və qaz sənayesi üçün əsas prioritetdir. Sənayenin rəqəmsal transformasiyası tam sürətlə davam edir. IoT cihazları, ötürülən məlumatların həcmi, yeni İT həllərinin inteqrasiyası və avtomatlaşdırılmış proseslərə nəzarət sistemləri kibertəhlükəsizlik təhdidlərinin artmasına səbəb olur. Sənaye müəssisələrinin aktivləri həm kibercinayətkarlar, həm də ayrı-ayrı dövlətlərin xüsusi xidmət orqanları tərəfindən həyata keçirilən getdikcə daha çox mürəkkəb hücumların hədəfinə çevrilir. Hücuma məruz qalan şirkət istehsalın dayanması, avadanlıqların zədələnməsi, daxili xidmətlərin pozulması və məlumat sızması ilə üzləşə bilər. Buna görə də, informasiya aktivlərinin mühafizəsi üzrə standart tədbirlərlə yanaşı, avtomatlaşdırılmış proseslərə nəzarət sisteminin təhlükəsizliyini təmin edən tədbirlər də nəzərdən keçirilməlidir.

Açar sözlər: *kibertəhlükəsizlik, sənaye müəssisələri, neft və qaz sənayesi, hücumlar*

Tura Guliyeva
Azerbaijan University
https://orcid.org/0009-0009-4224-025X
tura.guliyeva@student.au.edu.az

Threats to Information Security of Oil and Gas Companies

Abstract

Attacks and inside threats put both tangible and intangible assets of the company at risk. Problems with equipment threaten to stop the production process and pollute the environment, which results in millions of dollars in losses and leads to increase public protests. Due to its critical importance for global and national economies, cybersecurity is a top priority for the oil and gas industry. The digital transformation of the industry is in full swing. IT devices, the volume of transmitted data, the integration of new IT solutions and automated process control systems lead to an increase in cybersecurity threats. The assets of industrial enterprises are becoming the target of increasingly sophisticated attacks carried out by both cybercriminals and special services of individual states. A company that is attacked may face production shutdowns, equipment damage, disruption of internal services and data leakage. Therefore, in addition to standard measures for the protection of information assets, measures to ensure the security of the automated process control system should also be considered.

Keywords: *cybersecurity, Industrial enterprises, oil and gas industry, attacks*

Giriş

Neft və qaz sənayesi ehtiyatların tükənməsi və qiymətlərin düşməsindən tutmuş informasiya və məlumatların idarə edilməsi sistemlərinə qədər müxtəlif sahələrdə mürəkkəb problemlərlə üzləşir.

Sənaye rəqəmsallaşma və avtomatlaşdırma kimi yeni texnologiyalara tez zamanda qoşuldu, bu da xərcləri azaltmağa və qərar qəbul etməyə kömək edə bilər. Bununla belə, neft və qaz sənayesinin qarşısında informasiya təhlükəsizliyinin idarə edilməsi kimi çətin vəzifə durur.

Kiberhücumların potensial nəticələri əsasən kibercinayətkarlar və onların məqsədlərindən asılıdır. Məsələn, dövlət tərəfindən dəstəklənən bəzi xüsusi hallarda rəqiblər və ya hakerlər məxfi məlumatların açıqlanmasında maraqlıdırlar. Digər tərəfdən, təxribat daha çox haktivistlərdən qaynaqlanır (məsələn, 2013-cü ildə #OpPetrol Əməliyyatı) (Alastair Stevenson).

Hücum uğurlu alınarsa, şirkətin üzləşə biləcəyi bəzi risklər aşağıdakılardır:

- İstehsal müəssisənin bağlanması;
- Avadanlıqların zədələnməsi;
- Bir sıra məhsullara texnoloji müdaxilə;
- Uyğunsuz məhsul keyfiyyəti;
- Aşkar edilməmiş dağılmalar;
- Yaralanma və ya hətta ölümlə nəticələnən təhlükəsizlik qaydalarının pozulması.

Hakerlər məlumat toplamaq üçün casus proqramlardan istifadə edir, istehsala nəzarət sistemlərini zərərli proqramlarla yoluxdurur və ya nəzarət sistemləri vasitəsilə məlumat axınına mane olurlar və digər kiberhücumlar kibercinayətlər təşkil edir. Məsələn, 2014-cü ildə hakerlər yaxşı tədqiq edilmiş fişinq kampaniyaları və Trojan Atı hücumlarının təkmil versiyalarından istifadə edərək Avropadakı 50 neft və qaz şirkətinə hərtərəfli hücuma keçmişdilər (FireEye, 2023).

Kibercinayətkarların müəyyən edilməsinin kifayət qədər mürəkkəb olması təəccüblü deyil. ICS - CERT Sənaye Kiber Fövqəladə Hallara Müdaxilə Qrupununu (US Department of Homeland Security, 2015) məlumatlarına görə, 2015-ci il hücumlarının üçdə birindən çoxu naməlum "infeksiya vektoru"na malik idi. Müəyyən bir zamanda məlumatı silən virus 2012-ci ildə Yaxın Şərqin neft və qaz şirkətlərində 30.000 kompüteri yoluxdurmuş (Jim Finkle, 2016) – bu və ya digər formada hal-hazırda da görünməkdə davam edir.

Potensial kiberhücumların qarşısını almaq üçün neft hasilatı və təchizatının texnoloji zəncirində istehsalın hər bir addımında informasiya təhlükəsizliyinə ən çox ehtimal olunan təhdidləri başa düşmək lazımdır.

Tədqiqat

Bu əməliyyatda ən böyük risk şirkətin sahə məlumatlarına aiddir və birbaşa məlumat xərclərinin olmaması və ya görünən nəticələrin olmaması səbəbindən hücum uzun müddət aşkar edilmədən qala bilər. Məsələn, 2011-ci ildə Night Dragon kiberhücumunun (McAfee, 2011) arxasında duran hakerlər bir çox neft və qaz şirkətlərinin kəşfiyyat və ticarət məlumatlarını oğurlamaq üçün uzun illər ərzində proksi server parametrlərini deaktiv etmiş və uzaqdan idarəetmə alətlərindən istifadə etmişlər.

Mövcud kəşfiyyat işinin nisbətən əlverişli informasiya təhlükəsizliyi riski profilinə malik olmasına baxmayaraq, şirkətlər yeraltı təsvirin dəqiqliyini artırmaq və rəqəmsallaşdırmaq, saxlamaq və emal etmək yolu ilə getdikcə artan terabaytlıq seysmik məlumatların istifadəsinə yerləşdirmək üçün inkişaf etmiş cazibə dalğası sensorlarından getdikcə daha çox istifadə edirlər. Məsələn, CNOOC seysmik məlumatların emalı müddətini iki aydan bir neçə günə azaldıb və çox sayda saxlama klasterlərində miqyas alan açıq mənbəli, böyük məlumat tutumlu serverləri yerləşdirməklə yaddaş performansını 4,4 dəfə artırıb.

Bu cür proqram təminatının, yüksək performanslı hesablama və saxlama sistemlərinin genişləndirilməsi, şübhəsiz ki, məhsuldarlığın və gəlirin eksponensial artmasına imkan verəcəkdir. Lakin bu kəşfiyyat məlumatları real vaxt rejimində yaxınlıqdakı qazma planları, tamamlama layihələri və ehtiyat təxminləri kimi əməliyyatlara axmağa başlayanda kiberhücumun təsiri potensial gəlir itkisindən biznesin əhəmiyyətli dərəcədə pozulmasına qədər artacaq.

Quyunun işlənməsi

Neft və qaz dəyər zəncirində neft və qaz quyularının işlənməsi kiberhücumlara qarşı xüsusilə həssas bir əməliyyatdır. Birincisi, bütün maraqlı tərəflərin müxtəlif biznes məqsədləri operatorların vahid kibertəhlükəsizlik protokolundan istifadəsini çətinləşdirir, ikincisi, ekosistemə daxil olan

qazma qurğularının və alt sistemlərinin mikroprosessor avtomatlaşdırılması və idarəetmə sistemlərində sistem nasazlığı baş verə bilər.

Kiberhücumun şiddəti qazma əməliyyatları zamanı ən yüksək olur. İstər aktiv itkisi, biznes prosesinin pozulması, tənzimləyici cərimələr, nüfuzun zədələnməsi, istərsə də sağlamlıq, ətraf mühit və təhlükəsizlik hadisəsi olsun, bu mərhələ bütün risk kateqoriyaları üzrə ən yüksək gələcək fürsət xərclərinə malikdir. Açıq, neytral məlumat ötürmə protokollarından istifadə etməklə oflayn qazma əməliyyatlarının nisbi təhlükəsizliyinə baxmayaraq (məsələn, İşarələmə Dili üçün Wellsite Məlumat Ötürmə Standartı, WITSML), şirkət oxuna bilən quyu məlumatlarını mümkün qədər qorumalıdır.

Neft məhsullarının və qaz emalı məhsullarının istehsalı

Neft və qaz hasilatı əməliyyatı, ilk növbədə kibertəhlükəsizlik nəzərə alınmadığından köhnə aktiv bazasına görə kiber zəiflik baxımından ən yüksək yer tutur. Dünya üzrə dəniz aktivlərinin təqribən 42 faizinin 15 ildən çox yaşı var, neft və qaz şirkətlərinin yarısından azı öz şəbəkələrində monitorinq alətlərindən istifadə edir və bu şirkətlərin yalnız 14 faizinin təhlükəsizlik monitorinqi mərkəzləri tam fəaliyyət göstərir (Tim Heidar, 2016).

Yuxarıda təsvir edilən kibertəhlükəsizlik problemi əməliyyat mühitinin genişlənməsi və sistem provayderlərindən tutmuş sistem aqreqatorlarına qədər alət təminatçılarının dəyişən rolu ilə izah olunur və ya kəskinləşir. Böyük bir neft-qaz şirkətinin on minlərlə hasilat quyusu var və hər quyuda müxtəlif sənaye idarəetmə sistemləri var - quyulardakı sensorlardan, quyuda proqramlaşdırıla bilən məntiq nəzarətçilərinə, yerli idarəetmə mərkəzlərində SCADA sistemlərinə qədər (Yakovis, 2013).

Bundan əlavə, bu sərbəst birləşdirilən, lakin buna baxmayaraq, inteqrasiya olunmuş avtonom avtomatlaşdırma sistemləri getdikcə daha çox müəssisə resurslarının planlaşdırılması sistemləri ilə əlaqələndirilir. Qlobal neft və qaz hasilatının 75%-i resursların planlaşdırılması sistemləri tərəfindən idarə olunan dəyər zəncirinin bu hissəsi həm yuxarıdan (İT sistemləri), həm də aşağıdan (ənənəvi də əməliyyat texnologiyası sistemləri) kiber risklərlə üzləşir. Beləliklə, neft və qaz hasilatına kiberhücumun nəticələri həm yuxarı, həm də aşağı axın səviyyələrində sürətli təsirlərlə ciddi ola bilər. Daha mürəkkəb və ixtisaslaşdırılmış seysmik və qazma məlumatlarından fərqli olaraq, neft məhsullarının hasilatı, hazırlanması və daşınması istehsal proseslərinin parametrləri (adətən temperatur, axın, təzyiq, sıxlıq, sürət və s.) nisbətən asan başa düşülür və hakerlərə imkan yaradır (Yefremov, 2016).

Çox vaxt risklərin qarşısını almaq kiberhücumun nəticələri ilə mübarizə aparmaqdan daha asan və ucuz başa gəlir. Kiberdavamlı qalmaq üçün neft və qaz şirkətləri potensial hücumdan identifikasiya, qorunma, aşkarlama, riskə reaksiya və bərpa proseslərini əhatə edəcək şəkildə informasiya təhlükəsizliyini qurmalıdırlar (Bova, 2014).

Nəticə

Təhlükəsizlik tədbirlərinin həyata keçirilməsi, kritik və həssas sahələrin qorunması və təhdidləri aşkar etmək və onlara effektiv cavab vermək bacarığına sərmayə qoymaq şirkətlərə gələcək hücumların öhdəsindən gəlməyə kömək edəcək.

Bir şey aydındır ki, kibercinayətkarlar çox vaxt bir addım öndə olurlar və buna görə də şirkətlərin informasiya təhlükəsizliyi təhdidlərinin monitorinqində və onlara cavab məsələlərində sayıq və fəal olmaları çox vacibdir.

Ədəbiyyat

1. Alastair Stevenson. (2025). *Anonymous OpPetrol hacking campaign targets oil and gas sectors* https://www.v3.co.uk/v3-uk/news/2276288/oiland-gas-sector-warned-of-anonymous-oppetrol-hacking-campaign
2. FireEye. (2023). *Cyber threats to the Nordic region*. https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rptnordic-threat-landscape.pdf
3. US Department of Homeland Security. (2015). *NCCIC / ICS - CER – 2015 year in review.* https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf.

4. Jim Finkle. (2016). *Shamoon virus returns in new Saudi attacks after 4 - year hiatus*. www.reuters.com/article/cyber-saudi-shamoon-idUSL1N1DW05H
5. McAfee. (2011). *Global energy cyberattacks: Night Dragon*. www.mcafee.com/hk/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf
6. Tim Heidar. (2016). *Digital trenches: On the front lines of the cyber war*. www.fox-it.com/en/about-fox-it/corporate/news/65-oil-gas-companies-unprepared-major-cyberattack
7. Yakovis, L. M. (2013). *Ot yedinogo informatsionnogo prostranstva k yedinomu prostranstvu upravleniya proizvodstvom. Avtomatizatsiya v promyshlennosti*, 20-26. https://elibrary.ru/item.asp?id=18419873
8. Yefremov, A. A. (2016). *Yedinyye tsifrovyye prostranstva: v poiske balansa mezhdu integratsiyey i suverennost'yu*. Informatsionnoye pravo №3, 36-39. https://elibrary.ru/item.asp?id=27036305
9. Bova, V. V. (2014). *Kontseptual'naya model' predstavleniya znaniy pri postroyenii intellektual'nykh informatsionnykh system*. Izvestiya YUFU. Tekhnicheskiye nauki №7, 109-117. https://elibrary.ru/item.asp?id=21782588

Daxil oldu: 09.10.2024
Baxışa göndərildi: 03.12.2024
Təsdiq edildi: 22.01.2025
Çap olundu: 28.02.2025