UOT 004.056 DOI: 10.25045/jpit.v11.i2.01

Ələkbərov R.Q., Həşimov M.A.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
t.direktor_muavini@iit.science.az, mamedhashimov@gmail.com

BULUDƏSASLI SCADA SİSTEMLƏRİNDƏ TƏHLÜKƏSİZLİK MƏSƏLƏLƏRİ

Daxil olmuşdur: 05.06.2020 Düzəliş olunmuşdur: 17.06.2019 Qəbul olunmuşdur: 30.06.2020

Məqalədə neft-qaz sənayesinin monitorinqi və idarə edilməsində geniş istifadə olunan buludəsaslı SCADA (ing. Supervisory Control and Data Acquisition) sistemlərinin təhlükəsizlik məsələlərinə baxılmışdır. Ənənəvi SCADA sistemləri çox bahalı, qeyri-çevik, miqyaslanması çətin olduğundan məlumatların toplanması, ötürülməsi və emalında çoxsaylı problemlər yaranır. SCADA sisteminin tətbiqlərinin bulud mühitinə köçürülməsi xərclərin azaldılmasına, miqyaslanma imkanlarının yaxşılaşdırılmasına, sistemin səmərəli idarə olunmasına, etibarlılığın yüksəlməsinə və resurslarla bağlı problemlərin həllinə imkanlar yaradır. Məqalədə buludəsaslı SCADA sistemlərinin təhlükəsizliyinə mane ola biləcək mövcud boşluqlar göstərilmişdir. Buludəsaslı SCADA sistemlərində təhlükəsizlik tədbirlərinin görülməsi və risklərin qiymətləndirilməsi aktual məsələlərdəndir. Bu məqsədlə buludəsaslı SCADA sistemlərinin istifadəsində meydana çıxan təhlükəsizlik problemləri və risklər analiz edilmiş və bunların müəyyən qədər həllinə kömək edən təkliflər verilmişdir.

Açar sözlər: *neft-qaz sənayesi, buludəsaslı SCADA sistemləri, cloud computing, cloud xidmətləri, cloud modelləri, təhlükəsizlik.*

Giriş

Neft-qaz sənayesi enerji istehlakı üçün vacib olan və dünya iqtisadiyyatına çox böyük təsir göstərən bir sahədir. Neft-qaz sənayesi neft məhsullarının kəşfiyyatı, hasilatı, emalı, nəqli və satışı proseslərini əhatə edir. Neft-qaz sənayesinin innovasiyalı idarəetmə sistemində son dövrlərdə hesablama buludları *(ing. cloud computing)* texnologiyalarının tətbiqi ən aktual və vacib məsələlərdəndir. Məlum olduğu kimi, elmi-texniki tərəqqinin inkişaf səviyyəsi hal-hazırda neft-qaz sənayesində daha mükəmməl və müasir standartlara cavab verən yeni idarəetmə və nəzarət modellərinin istifadə edilməsinə şərait yaratmışdır. Ənənəvi SCADA sistemləri digər idarəetmə sistemləri kimi böyük həcmdə resurs, təhlükəsizlik, sürətli emal tələb edir. SCADA sistemlərinin buluda miqrasiyası vasitəsilə sənaye idarəetmə sistemləri mühitində sürətli emal və resursla bağlı problemlər həll edilə bilər. Neft-qaz sənayesi sektorunda sistemlərin avtomatlaşdırılması, səmərəliliyin və gəlir imkanlarının artırılması məqsədilə buludəsaslı SCADA sistemlərindən istifadə getdikcə artır. SCADA tətbiqləri üçün hazırlanmış buludəsaslı həllər səmərəlilik, miqyaslanma, emal və çəkilən xərclər baxımından bir sıra üstünlüklər təklif edir. Sənaye idarəetmə sistemləri mühitində yüksək emal sürəti tələb olunur ki, bu da bulud texnologiyaları vasitəsilə həll oluna bilər. Yuxarıda qeyd edilən üstünlüklərdən əlavə SCADA qurğuları üçün tətbiq edilən hesablama buludları İnternet bağlantısı olan istənilən məkandan girişin həyata keçirilməsinə və bununla da verilənlərin əlyetərliyinin təmin edilməsinə imkan verir. Miqyaslanma imkanları ilə yanaşı SCADA qurğuları vasitəsilə bir neçə saniyə ərzində yeni xidmət və serverlərin əlyetərliyi təmin olunur. Əsas qurğuların və ya xidmətlərin buluda miqrasiyası ilə resurs və sürət problemini həll etməklə xərclərin azaldılmasını təmin etmək mümkündür. Hal-hazırda bir çox təşkilatlar hesablama texnologiyalarının faydalarından yararlanır və öz SCADA tətbiqlərini bulud mühitinə miqrasiya etməklə xərclərini minimuma endirir, effektivliyini artırır və etibarlılığı yüksəldirlər. Nisbətən yeni texnologiya olduğundan, buludəsaslı SCADA sistemlərinə edilən hücumların sayı hələlik çoxdur və bu da təhlükəsizlik məsələlərində problemlərin yaranmasına səbəb olur. Beləliklə, buludəsaslı SCADA sistemlərində təhlükəsizlik tədbirlərinin görülməsi və risklərin qiymətləndirilməsi aktual məsələlərdəndir.

Əlaqəli tədqiqat işləri

[1]-də SCADA tətbiqlərin (proqram təminatları) ənənəvi kompüter sistemlərində deyil, tamamilə cloud computing mühitində quraşdırılması məsələlərinə baxılmışdır. Bu zaman hesablama resurslarının yenilənməsinə artıq ehtiyac qalmır, bunun əvəzinə isə ehtiyac olduqda, bulud infrastrukturundan istifadə edilməsi qeyd edilmişdir. Eyni zamanda məqalədə SCADA sisteminin buludda tətbiqinə mane ola biləcək etibarlılıq, təhlükəsizlik və hesablama kimi bir sıra problemlərin hələ də həll edilməməsi göstərilmişdir. [2]-də SCADA sistemlərinin cloud computing (Hibrid Bulud) mühitində tətbiqi üçün iki konseptual model irəli sürülmüşdür. Birinci mərhələdə SCADA tətbiqləri bütünlüklə hibrid buludda emal olunur. İkinci mərhələrdə isə SCADA tətbiqləri SCADA şəbəkəsində yerləşmiş qurğulara birbaşa qoşulmuş ayrı-ayrı proqram serverində işə salınmışdır. Məqalədə, həmçinin SCADA və cloud computing rabitəsinin təhlükəsizlik məsələləri də müzakirə olunmuşdur. [3]-də neft-qaz sahəsindəki ənənəvi SCADA sisteminin etibarlılığının, texniki təminatının təşkili, genişləndirilməsi imkanları və resurs istifadəsinin artırılması məqsədilə Cloud computing əsaslı SCADA sistemlərindən istifadənin üstünlükləri qeyd edilir. [4]-də SCADA sistemlərinin buluda inteqrasiya edilməsində meydana çıxan əsas problemlər kimi təhlükəsizlik məsələləri göstərilmişdir. Bu tip mühitdə məxfi məlumatların təşkilatın nəzarətindən kənarda saxlanılması kimi təhlükəsizlik risklərinin daha yüksək olması qeyd edilir. [5]-də bulud serverlərdə məlumatların saxlanması sahəsində təhlükəsizlik məsələlərini araşdırmaqla, bulud administratorlar tərəfindən istifadəçilərin (təşkilatların) məlumatlarına icazəsiz daxil olmanın qarşısının alınması üçün metod təklif edilmişdir. [6]-da neft və qaz sənayesinin tətbiq proqramlarının buludlara miqrasiyası araşdırılmışdır və məlumatların açıq buludlara köçürülərkən təhlükəsizlik məsələlərinin nəzərə alınması tədqiq edilmişdir. [7]-də SCADA sistemlərinin bulud mühitinə miqrasiyası zamanı əsas risk faktoru qismində kiber təhlükəsizliyə xüsusi diqqət yetirilməsi göstərilmişdir. Bu məqsədlə, əlavə araşdırmaların aparılması və miqrasiyanın tədricən həyata keçirilməsi tələb olunur. Bəzi sahələrdə bir sıra irəliləyişlərin olduğu, lakin bəzi açıq məsələlərin hələ də mövcud olduğu göstərilmişdir. [8]-də müasir SCADA arxitekuralarında edilən dəyişikliklərə baxmayaraq, aşağıda qeyd olunan problemlərin həll edilməsi üçün bəzi işlərin həyata keçirilməsinin zəruri olduğu qeyd olunmuşdur: a) çoxsaylı sensorlar vasitəsilə genişmiqyaslı nəzarətin təmin edilməsi; b) hər hansı hücum və ya hadisə aşkarlandıqda, onun qarşısının alınması üçün tələb olunan zamanın minimuma endirilməsi; c) insidentlərin qarşısının alınması məqsədilə SCADA sistemləri arasında qarşılıqlı fəaliyyətin təmin edilməsi. Bu baxımdan genişmiqyaslı və bir-birindən asılı olan kritik infrastrukturlara nəzarət etmək məqsədilə sensor buludlardan istifadə edilməsi təklif olunur. [9]-da ənənəvi və müasir SCADA sistemlərinin arxitekturası geniş şəkildə təhlil edilmişdir. SCADA sistemlərinə qarşı olunan hücumların təsnifatı aparılmışdır. SCADA sistemlərinin təhlükəsizliyi üçün bir sıra tövsiyələr və bu sahədə ən uğurlu təcrübələr haqqında məlumat verilmişdir. [10]-da SCADA sistemləri üçün Təhlükəsizlik Yönümlü Arxitektur (SOA) əsaslı bulud platforması təklif edilmişdir. Burada əsas məqsəd bulud platformalarının SOA-əsaslı SCADA sistemlərinə inteqrasiyası üçün innovativ həllin təmin edilməsidir. [11]-də IPv6 əsaslı simsiz sensor şəbəkəsi (6LoWPAN) üzərindən qurulan SCADA sistemlərində müxtəlif təhdidləri müəyyən etmək və aradan qaldırmaq üçün təhlükəsizlik idarəetmə üsulları təklif edilmişdir. [12]-də SCADA sistemlərinə qarşı edilən hücumların təhlili nəticəsində bulud mühitində sənaye SCADA sisteminin fəaliyyətinə mane ola biləcək mövcud təhlükəsizlik boşluqları araşdırılmışdır.

Ənənəvi SCADA sistemlərinin problemləri

Neft-qaz sənayesinin texnoloji prosesini şərti olaraq üç əsas sektora ayırmaq olar [13, 14]. Birinci sektor kəşfiyyat, qazma və istehsal (neft-qazın çıxarılması) proseslərini əhatə edir. Burada, ilk növbədə, potensial yeraltı və ya sualtı xam neft, təbii qaz yataqları ehtiyatları araşdırılır və tədqiq edilir, sonrakı mərhələdə isə kəşfiyyat quyuları qazılır, karbohidrogen yataqlardan neft və ya qaz çıxarılır. İkinci sektorda isə xam neftin və ya neft məhsullarının nəqli həyata keçirilir. Daha

sonra emal edilmiş müxtəlif məhsullar üçüncü sektora ötürülür. Bu sektor xam neftin emalını və təmizlənməsini əhatə edir. Beləliklə, neft-qaz sənayesinin aşağı səviyyəsi kəşfiyyat və hasilatla məşğul olduğu halda, sənayenin orta səviyyəsində saxlama və nəql, yuxarı səviyyəsində isə emal və kimya sənayesi, eləcə də satış həyata keçirilir. Beləliklə, yuxarıda qeyd edilən neft-qaz sənayesinin texnoloji prosesini üç əsas sektorda səmərəli idarə etmək üçün SCADA sistemindən istifadə edirlər. SCADA sistemləri coğrafi olaraq paylanmış texnoloji avadanlıqları mərkəzləşdirilmiş qaydada idarə edən və onlara nəzarət edən nəzarət və idarəetmə sistemidir [15]. SCADA sistemləri qazma qurğularından, vericilərdən və ya digər nəzarət sensorlarından alınan böyük həcmli məlumatlar əsasında real zaman rejimində texnoloji prosesləri idarə edir. Resurslardan maksimum istifadə etmək və istehsalın səmərəliliyini artırmaq, qazma metodlarının optimallaşdırılması, istismar işinin yaxşılaşdırılması və dəqiq geoloji təlimatların təmin edilməsi üçün quyu sahələrindən, quyunun özündən və yerin altında quraşdırılmış sensorlardan real zaman rejimində verilənlər toplanılır. Əlaqəli sahələr üzrə toplanmış verilənlərin analizi qazma və tamamlama işlərinin səmərəliliyini artıra bilər. SCADA sistemi, geniş ərazidə paylanmış avadanlıqlara davamlı nəzarəti həyata keçirə və idarəetmə mərkəzindən uzaqda yerləşən cihazları idarə edə bilər ki, bununla da, idarəetmənin səmərəliliyi artırıla, enerjiyə qənaət oluna və xərclər azala bilər [16].

SCADA sistemi neft və qaz sənayesində texnoloji proseslərin idarə edilməsində geniş istifadə edilir. Buna baxmayaraq, mövcud SCADA sistemlərində aşağıdakı problemlər mövcuddur [17]:

• SCADA sistemlərində etibarlılığı təmin etmək məqsədilə köməkçi serverlərdən istifadə olunur. Əsas server onlayn işləyərkən, köməkçi server əsas serverin iş vəziyyətinə nəzarət edir və əsas server ilə köməkçi server arasındakı məlumat ardıcıllığının saxlanılması məqsədilə əsas serverdən məlumatı qəbul edir. Əsas server sıradan çıxdıqda, köməkçi server dərhal əsas serverin işini öz üzərinə götürməklə əsas serverə çevrilir, təmir olunan əsas server isə köməkçi serverə çevrilir. Beləliklə, sistemin etibarlılığı yalnız bir ehtiyat server tərəfindən təmin edilə bilməz. Sistemin miqyası daim genişləndikcə, serverlərin sayı da artır və bu serverlərin sistemdə yerləşdirilib işə salınması böyük vaxt tələb edir. Ehtiyat serverlərin sayının çox olması sistemin bahalaşmasına səbəb olur və sistemin səmərəli idarə edilməsində problemlər yaradır.

• SCADA sisteminə qoşulan neft-qaz sənaye müəssisələri daim genişləndikcə, idarəetmə mərkəzində yerləşən serverlərin və idarəedici qurğuların da sayı artır. Serverlərdə sensorlardan və icra mexanizmlərindən çoxlu sayda əməliyyat və məlumatlar daxil olur və emal edilir. Serverlərin emal yükü onlara daxil olan məlumatların xarakterindən asılı olaraq fərqlənir. Belə ki, müxtəlif serverlər fərqli yüklənməyə malikdir, yəni, bəzi serverlər həddən artıq yüklənir, bəziləri isə boş qalır. Bu səbəbdən də, sistemin fəaliyyətini yaxşılaşdırmaq üçün yüklənmənin balanslaşdırılması üçün yeni strategiyaların araşdırılması tələb olunur.

• Sistemin texniki imkanlarının artırılması üçün yeni avadanlıqların alınması, quraşdırılması, sistemin yenidən konfiqurasiya edilməsi və sınaqdan keçirilməsi aylarla vaxt tələb edir və bu da sistemin səmərəli idarə edilməsində problemlər yaradır.

Son illərdə neft-qaz sənayesində sistemlərin səmərəli idarə edilməsində cloud computing texnologiyalarından geniş istifadə olunur. Bu texnologiyanın köməyi ilə yaradılan buludəsaslı SCADA sistemlərindən neft-qaz sənaye müəssisələrinin monitorinqində və idarə edilməsində geniş istifadə olunur.

SCADA sistemlərinin buludlara köçürülməsi

Cloud computing texnologiyalarından texnoloji proseslərin idarə edilməsində istifadə edilən sistemlərin infrastrukturunun və proqram təminatının bilavasitə şəbəkə və bulud mühitində yaradılmasında geniş istifadə olunur. Bu texnologiyanın köməyi ilə məlumatlar bulud sistemlərində saxlanılır, emal edilir, emal proqramlarının işə salınması və nəticələrə baxılması təmin edilir. Aparılan tədqiqatlar göstərir ki, müəssisələr bulud texnologiyalarından istifadə etsələr, idarəetmə və nəzarət sistemlərinin yaradılmasında böyük xərc tələb edən avadanlıqların (serverlərin, kompüterlərin, yaddaş sistemlərinin) və proqram təminatlarının alınıb

quraşdırılmasına ehtiyac qalmır. Son vaxtlar cloud computing texnologiyalarından neft-qaz sənayesinin müxtəlif sektorlarının idarə edilməsində geniş istifadə edirlər. Cloud computing texnologiyaları seysmik kəşfiyyat, qazma, hasilat və digər sektorların idarə edilməsi üçün məlumatların toplanması, saxlanması və emal edilməsini təmin edən bulud xidmətləri təklif edir.

Buludəsaslı SCADA sistemlərinin idarə edilməsində istifadə olunan xidmətlərə baxaq: hal-hazırda bulud sistemləri ümumiyyətlə üç cür xidmət təklif edir [18, 19]: Proqram təminatı xidmət kimi *(ing. Software as a service, SaaS),* Platforma xidmət kimi *(ing. Platform as a service, PaaS)* və İnfrastruktur xidmət kimi *(ing. Infrastructure as a service, IaaS).*

IaaS xidməti geniş yayılmış xidmət modeli hesab edilir. IaaS xidməti virtual serverlərin, yaddaş, şəbəkə və digər hesablama resurslarının təminatına imkan yaradır. İstifadəçilər isə yalnız istifadə etdikləri resursa görə ödəniş edir. Müştərilər istifadə edilən bulud infrastrukturuna nəzarət etmir, lakin əməliyyat sistemlərinə, virtual resurslarda yerləşdirilmiş tətbiqlərə nəzarət etmək və şəbəkə komponentlərini seçmək imkanına malik olurlar. PaaS xidməti provayderin infrastrukturunda yerləşən proqram təminatı və məhsul yaratma alətləri dəstidir. PaaS xidməti istifadəçilər tərəfindən virtual serverlərdə (fiziki serverlərdən təşkil olunan) yerləşən əməliyyat sistemlərindən və xüsusi proqram əlavələrindən istifadə edilməsinə imkan yaradan virtual platformadır. İstifadəçilər bu alətlərdən İnternet üzərindən tətbiqlərin yaradılmasında istifadə edirlər. SaaS xidmətində istifadəçi ona lazım olan proqram əlavələrinin rezident hissəsini öz kompüterinə yükləmədən şəbəkə kanallarının köməyi ilə bulud serverlərə müraciət edir. Proqram əlavələri SaaS xidməti verən təchizatçının bulud serverində işləyir və istifadəçiyə hesablamaların nəticəsini göndərir. Beləliklə, istifadəçi proqram təminatını almır və lazım gələndə ondan məsələnin həllində istifadə edir və istifadəyə görə uyğun pul ödəyir.

Konseptual səviyyədə bulud arxitekturasının əsas üç növü mövcuddur: ictimai (açıq) bulud, özəl bulud və hibrid bulud [20, 21]:

İctimai buludlar (*ing. Public cloud*) – geniş istifadəçilər üçün nəzərdə tutulmuş bulud infrastrukturudur. Təşkilatın korporativ şəbəkəsindən kənarda yaradılır. İstifadəçinin məlumatlarının idarə edilməsi və təhlükəsizlik məsələləri bulud provayderləri tərəfindən həyata keçirilir. Bu tip buludlarda istifadəçilər bulud provayderlərinin təklif etdiyi standart konfiqurasiyalardan istifadə edirlər.

Özəl buludlar (*ing. Private cloud*) – bir təşkilat daxilində hesablama buludları xidmətindən istifadə üçün yaradılmış infrastrukturdur. Təşkilat yaratdığı buludu özü idarə edə bilər və ya kənar təşkilata həvalə edə bilər. Özəl buludlarda təhlükəsizlik məsələləri digər buludlara nəzərən daha yüksəkdir.

Hibrid buludlar (*ing. Hybrid cloud*) – yuxarıda qeyd edilən buludların birləşməsindən yaradılır. İstifadəçilərin bir qrupu daxili buludlardan, digər bir qrupu isə ictimai buludlardan istifadə edir. Hibrid buludlar dövlət və özəl bulud infrastrukturlarının birləşdirilməsindən yaradılır.

Hər üç xidmət modeli ilə birlikdə həyata keçirilən sistemlərdə miqyaslanma işləri sürətli və ucuz başa gəlir, çünki buraya yeni server və proqram təminatlarının təşkilat (istifadəçi) tərəfindən alqı-satqısı, yerləşdirmə və konfiqurasiyası daxil deyil. Daha çox hesablama gücü və ya verilənlər üçün yaddaş tələb olunduqda, istifadəçi provayderdən sadəcə olaraq ona lazım olan qədər resurs tələb edir və bunun üçün ödəniş edir. Şirkətlər üçün artıq sayda texniki təminat və proqram təminatı lisenziyalarının alınmasına ehtiyac qalmır. İT infrastrukturunun yaradılması, adətən çox uzunmüddətli olur. Sistemlərin alınması, quraşdırılması, konfiqurasiya edilməsi və sınaqdan keçirilməsi aylarla vaxt tələb edə bilər. Buludəsaslı SCADA sistemlərinin yaradılması isə qısa vaxt ərzində cüzi və ya çox az maliyyə xərcləri ilə həyata keçirilə bilər.

Cloud computing texnologiyaları əsasında buludəsaslı SCADA sistemləri iki yolla yaradılır [22, 23]:

1. Qismən buludlarda yerləşmə. Sensorların və icra mexanizmlərində məsələlərin istifadəsində yerinə yetirilən tətbiqi proqramlar SCADA sisteminin yaradıldığı binalarda (şirkət, təşkilat və s.) yerləşən kompüter serverlərdə icra olunur. Serverlər İnternet vasitəsi ilə birbaşa

buludda yerləşən idarəetmə mərkəzi ilə əlaqələndirilir və məlumatların saxlanılması üçün bulud serverə ötürülür. Bu modeldən daha geniş istifadə olunur. SCADA tətbiqlərinin nəzarət funksiyaları kontroller (idarəetmə) şəbəkəsindən icra olunur, SCADA sisteminin bəzi tətbiqləri (prosesin vizuallaşdırılması, hesabatlar, arxivləşdirmə və s.) isə bulud serverlərdə yerinə yetirilir. Bu cür model adətən ictimai bulud infrastrukturundan istifadə etməklə yaradılır.

2. Tam buludəsaslı SCADA sistemləri. Bu modeldə istehsalat prosesinə nəzarət və idarəetmə səviyyəsində yerinə yetirilən tətbiqi proqramlar buludda yerləşən serverlər tərəfindən icra olunur və distant olaraq idarəetmə şəbəkəsinə bağlanır. Bu model paylanmış SCADA sistemləri üçün uyğundur. İcra mexanizmləri kontroller vasitəsilə İnternet şəbəkəsi üzərindən SCADA tətbiqi proqramlarının icrasını həyata keçirən bulud serverlərə qoşulur. Bu cür tətbiqlər adətən özəl və hibrid bulud infrastrukturu vasitəsi ilə yaradılır.

Buludəsaslı SCADA sistemi ənənəvi SCADA sistemlərinə nəzərən aşağıdakı üstünlüklərə malikdir:

- Ehtiyac olduqda və ya tələb olunduqda, yeni avadanlıqların sistemə əlavə edilməsi asanlıqla təmin edilir. Şirkətə proqram və aparat təminatının alınması, quraşdırılması və işə salınmasının daha ucuz qiymətə başa gəlməsi;
- Sistemdə meydana çıxan nasazlıqların daha sürətlə bərpa edilməsi;
- Sistemdə hesablama yükünün qəfil artması ilə tələb olunan hesablama resurslarının dərhal əldə edilməsi;
- Mövcud tətbiqlərin yenilənməsi və yeni tətbiqlərin sistemə daxil edilməsinin asanlıqla həyata keçirilməsi;
- Sistemin idarə edilməsində meydana çıxan böyük həcmli verilənlərin yadda saxlanması üçün yaddaş resurslarının asanlıqla əldə edilməsi;
- Nəzarət və idarəetmə serverlərinin buludlarda ehtiyat serverlərini yaratmaqla sistemin etibarlılığının və təhlükəsizliyinin təmin edilməsi;
- İstifadəçilər tərəfindən bulud serverlərdə yerləşən məlumatların real vaxt müddətində əldə edilməsi;
- Buludəsaslı SCADA sistemlərin ümumi xərclərin azaldılmasına imkan verməsi.

Buludəsaslı SCADA sistemlərində təhlükəsizlik məsələləri

Ənənəvi SCADA sistemlərinin tətbiqlərinin bulud mühitinə köçürülməsi xərclərin azaldılmasına, miqyaslanma imkanlarının artmasına və texniki təminatı baxımından istifadəçilər üçün onun daha cəlbedici olmasına imkan verir. Eyni zamanda monitorinq və idaərəetmə sistemləri üçün texniki və proqram təminatının alınması, quraşdırılmasına, saxlanılmasına və texniki işçilərin sayının azalması hesabına çəkilən xərclər azalır. Xərclərin azalması və effektivliyin artırılması əsas biznes şərtlərindən olsa da, təhlükəsizliyin təmin olunması da çox vacib məqamdır. Belə ki, məlumatların itməsi və ya oğurlanması, təşkilati idarəetmənin itirilməsi və xidmətlərin imtinası buludəsaslı SCADA sistemlərinin üstünlükləri ilə balanslaşdırılmalıdır. Təşkilatlar qeyd edilən risklərə nə dərəcədə davamlı olduqlarını təyin etməli və idarəetməni bulud infrastrukturuna verməyi nəzərə almalıdırlar. SCADA tətbiqlərini buluda köçürməzdən əvvəl təhlükəsizlik riskləri əvvəlcədən nəzərə alınmalıdır.

Buludəsaslı SCADA sistemlərinin idarəetmə boşluqları da mövcuddur. SCADA sistemlərinin fəaliyyətinə manea ola biləcək mövcud boşluqların bəziləri aşağıda qeyd olunmuşdur [24, 25]:

1. Buludəsaslı SCADA sistemləri daha açıq olduğundan sistem əmrləri və məlumatları rabitə zamanı dəyişdirilə, itirilə və ya kopyalana bilər;
2. SCADA sistemləri ilə bulud arasındakı şəbəkə bağlantısı İnternet əsasında həyata keçirildiyindən əlaqə kanallarında məlumatlar hücumlara məruz qala bilər;
3. Bulud texnologiyalarına inteqrasiya olunmuş SCADA sistemləri bulud infrastrukturunda olan bütün risklərə malik ola bilər;

4. SCADA sistemlərinin bulludda istifadə olunan tətbiqləri asanlıqla hücumçular tərəfindən tapıla və istifadə oluna bilər;
5. İdarəetmə və avtomatlaşdırma məqsədilə SCADA sistemləri Modbus/TCP, IEC 40 və DNP3 protokollarından istifadə etsə də, bu protokolların bəziləri qorunma baxımından bir sıra boşluqlara malikdir. Bu protokollar autentifikasiyanı dəstəkləmədiyindən şifrələməni də dəstəkləmir. Şifrələnmənin olmaması isə hücumlar zamanı hücum edən tərəfindən həmin verilənlərin oxunmasına, ona dəyişiklik edilməsinə və ya trafikin istiqamətinin dəyişdirilməsinə səbəb ola bilər;
6. Əksər SCADA protokolları kommunikasiya quran müəssisələr arasındakı inamı yaratmaq məqsədilə autentifikasiyanı dəstəkləmirlər. Beləliklə də verilənlər potensial olaraq üçüncü şəxs tərəfindən ələ keçirilə bilər;
7. Verilənlərin buluda miqrasiyası onlar üzərində birbaşa nəzarətin itirilməsinə də səbəb ola bilər;
8. Buludəsaslı SCADA sistemlərinə qoşulan avadanlıqların sayının artması nəticəsində onun perimetri genişləndirilir və nəticədə hücumçular daha geniş əhatə dairəsi ilə təmin oluna bilər. Bu zaman yaranan risklər də artır. Buna görə də, təşkilatlar daim təhlükəsizlik tədbirləri görməlidirlər.

Beləliklə, təşkilatlar SCADA tətbiqlərinin qorunması və məhsuldarlığın təmin olunması məqsədilə təhlükəsizlik sahəsindəki boşluqlara davamlı olaraq nəzarət etməlidirlər. Belə ki, idarə və nəzarətetmə sistemlərində qeyd edilən boşluqların aradan qaldırılmasına çox az vaxt müddəti qoyulur. Risklərin qiymətləndirilmə nəticələri SCADA tətbiqlərinin buluda köçürülməsi haqqında dəqiq qərarların qəbul edilməsinə təsir göstərməlidir. Məlumatların təhlükəsizlik riski xərclərin, səmərəlilik və etibarlılığın qiymətləndirilməsi kimi qəbul edilərsə, onda buluda miqrasiya da bir o qədər effektiv nəticə verəcəkdir. Bu sahədə əsas problemlərdən biri odur ki, təhdidlər artdıqca, hücumların həm sayı, həm də əhatə dairəsi genişlənmişdir. Bu hücumlar əsasən də təhlükəsizlik sistemlərinə edilir. Aydındır ki, hücum vektoruna nəzər salsaq, qırılmaların necə baş verdiyini və hakerlərin sistemə necə daxil olduqlarını görə bilərik. Bəzi hallarda bu, buludəsaslı SCADA mühitinin bağlantılarının təhlükəsizliyinin təmin olunmaması və çoxsaylı avadanlıq və sistemlərin girişi nəticəsində baş verir. Digər hallarda isə bu, xarici və ya biznes şəbəkəsinin təhlükəsizliyinin təmin olunmaması nəticəsində baş verir. Adətən belə hallar bu cür sistemdən istifadə edən işçilərin özlərinin notbukları və ya telefon qurğuları vasitəsilə hücumçuların tələsinə düşməsi ilə baş verir.

Təşkilat buluda miqrasiya qərarını verdikdən sonra xidmət provayderi təyin olunmalıdır. Hər bir bulud xidmət provayderi təhlükəsizliyə nəzarət tələblərini qarşılaya bilməlidir. SCADA tətbiqləri üçün də xidmət provayderinin təhlükəsizlik mexanizmi və proseslərini yüksək səviyyədə təmin edə biləcəyinə əmin olmaq vacibdir.

Tam buludəsaslı SCADA sistemlərində tətbiqi proqramlar tamamilə buludda yerləşdirilmiş olur. Bu tətbiq trafiki generasiya edir və onları müştərinin sahəsində yerləşən idarəedicilərə növbəti emaletmə səviyyəsinə göndərir. Bu növ arxitekturada iki əsas təhlükəsizlik riski mövcuddur [26]:

1. Real zamanda verilənləri və ya əmrləri SCADA sisteminin qurğularından buluda ötürülərkən hücumçunun bacarığından asılı olaraq ələ keçirilir, oxunur, saxtalaşdırılır, inkar edilir və ya müxtəlif formalara dəyişdirilir.

2. Buludəsaslı tətbiqdən daxili SCADA mühitinin yerlərdə yerləşən qurğularına əmrlərin göndərilməsi ilə şəbəkə şlüzu vasitəsi ilə daxili bağlantı yaranır. Tələb olunan bu bağlantı daxili şəbəkəyə yol açır ki, bu da yolverilməz hesab olunur, çünki, bununla hücumçu şəbəkəyə yol tapa bilər.

Təşkilatlar buludəsaslı SCADA sistemlərindən istifadə etdikdə istifadəçilər verilənlərin xüsusiyyətlərini, veb tətbiqlərə hücumları, idarəetmə, autentifikasiya və şifrələnmə ilə əlaqədar bəzi problemləri nəzərə almalıdırlar [24, 26, 27].

Verilənlərin xüsusiyyəti. Qeyd etmək lazımdır ki, təşkilatların verilənləri minlərlə digər müştərilərin istifadə etdiyi bulud xidməti provayderi virtual serverində yerləşir. Belə olduğu halda həmin verilənlər bilərəkdən və ya bilməyərəkdən digərləri ilə bölüşdürülmüş olur. Bu cür hallar SCADA qurğularının buluda miqrasiyası zamanı nəzərə alınmalıdır.

SCADA tətbiqlərinə hücumlar. SCADA tətbiqlərinə hücumlar bulud infrastrukturu baxımından ən geniş yayılan təhdidlərdən biridir. Bu təhdid SCADA qurğularından da yan keçməmişdir. Veb tətbiq hücumları buludda yerləşdirilmiş SCADA tətbiqlərinə qarşı yönəldilir. Təbii ki, bu təhdid təşkilatın lokal məlumat mərkəzlərindən istifadəsi zamanı da yarana bilər. Bu hücumlar təsadüfi hücumlar hesab oluna bilər. Bu o deməkdir ki, hücumçu bulud xidməti provayderinin İP ünvanını skanerdən keçirərək ixtiyari SCADA tətbiqini tapar və ona hücum edə bilər.

Nəzarətin olmaması. Verilənlərin buluda miqrasiya etdirilməsi ilə təşkilatın həmin məlumatlar üzərindəki sahibliyi onun əlindən çıxır və bulud xidməti provayderinə ötürülür. SCADA qurğusunun məlumatlarını saxlayan bulud xidməti provayderi SCADA tətbiqi serverinə bağlanmış infrastrukturu ilə yeni bağlantıları inteqrasiya etmək istəsə, bu bağlantılar haqda məlumatın sahibi xəbərsiz olacaqdır. Bu isə müştəri üçün də naməlum risklərin yaranmasına səbəb olacaqdır.

Autentifikasiyanın olmaması. İki ən geniş yayılmış SCADA protokolları olan Modbus və DNP3 protokolları autentifikasiyanın dəstəklənməsi baxımından bir sıra əsas boşluqlara malikdir. Bəzi SCADA protokolları autentifikasiyanı dəstəkləmir və ya həyata keçirmir. Buludəsaslı SCADA arxitekturunun bir hissəsində yuxarıda qeyd edilən protokollardan, xüsusilə də açıq buludda yerləşdirilmiş protokoldan istifadə edilərsə, hücumçu yalnız İP ünvanını deyil, həmçinin istifadəçi adını və trafiki ələ keçirməklə məlumatlara giriş əldə edə bilər.

Şifrələnmənin olmaması. SCADA protokollarında autentifikasiya dəstəklənmədiyi kimi, məlumatların qorunması üçün vacib olan şifrələnmənin də heç bir növü təmin olunmur. Modbus və DNP3 protokolları da heç bir şifrələnmə növünü dəstəkləmir və bununla da trafik daha çox MiTM (man-in-the-middle) hücumlarına məruz qalır. Bu hücumlar vasitəsilə hücumçular ötürülən verilənləri nəinki görə, həm də trafikə istənilən dəyişikliyi edərək hər hansı digər sahə qurğusuna yönəldə bilərlər.

SCADA buluda miqrasiya edilərkən təhlükəsizlik riskləri artır və beləliklə də istənilən təşkilat öz məlumatlarının təhlükəsizliyini təmin etmək məqsədilə bir sıra tədbirlər görməlidir. Qeyd etmək lazımdır ki, aşağıda təklif edilən həllər müəyyən qədər göstərilən problemlərin həllinə kömək edə bilər [26, 28, 29]:

- *İstifadədə olmayan verilənlərin şifrələnməsi.* SCADA mühitində istifadə olunmayan verilənlərin şifrələnməsi hər zaman mümkün olmasa da, bulud mühitində bu şifrələnmə bir sıra üstünlüyə malikdir. Məsələn, hücumçu bulud xidməti provayderinin serverində saxlanılan verilənləri ələ keçirdikdə, hücumçu üçün onun deşifrələnib oxunması çox mürəkkəb olacaqdır. Şifrələnmə mümkün olduqda həmişə, xüsusilə də verilənlər ərazidən uzaqda yerləşdikdə daha çox məsləhət görülür.
- *Təhlükəsiz internet protokolundan (İPsec) istifadə.* Mümkün olduqda, İPsec imkanlarından yararlanmaq lazımdır. İPsec həm autentifikasiya, həm də şifrələnməni dəstəkləyir, bu isə hücumçulara verilənləri oxumaqda, dəyişdirməkdə və buludəsaslı SCADA mühitində trafiki ələ keçirməkdə problemlər yaradır.
- *Hərtərəfli giriş imkanını təmin etmək.* Ümumiyyətlə, bütün giriş məlumatlarının mərkəzləşmiş giriş həllində saxlanması məsləhət görülür. Bundan əlavə, mümkün qədər çox giriş məlumatları SİEM-ə (Security Information and Event Management) göndərilməlidir. Sistem, təhlükəsizlik və şəbəkə avadanlıqlardan məlumatları toplayır, analiz edir, düzgün qərarlar verilməsini təmin edir.

- *Təhlükəsiz protokollardan istifadə.* Mümkün olduqda, təhlükəsiz protokollardan istifadə etməklə autentifikasiya və şifrələmə ilə bağlı problemlərin bəzilərini aradan qaldırmaq olar. Secure DNP3 kimi daha təhlükəsiz protokolların istifadəsi məsləhət görülür.
- *Etibarlı razılaşmaların bağlanması.* Hər hansı üçüncü tərəfin serverə müdaxiləsinin olmayacağına əmin olmaq məqsədilə bulud xidməti provayderi ilə istifadəçilər arasında etibarlı razılaşmaların imzalanması məsləhət görülür. Bu, bulud xidməti provayderinə etibarı artıracaq, təhlükəsizliyin təmin olunmasına yardım edəcəkdir.

Nəticə

Bulud xidmətləri daha geniş miqyasda istifadə olunduqca, şirkətlər bu texnologiyanın idarəetmə sisteminə tətbiqinə daha çox diqqət ayırmağa başlamışdır. SCADA sistemlərinin tətbiqlərinin bulud mühitinə köçürülməsi xərclərin azaldılması, miqyaslanma imkanlarının artması və texniki təminatı baxımından istifadəçilər üçün daha cəlbedicidir. Digər tərəfdən isə iqtisadi cəhətdən da səmərəli hesab olunur. Bu məqsədlə məqalədə neft və qaz sənayesində buludəsaslı SCADA sistemlərinin imkanları, üstünlükləri və problemləri təhlil edilmişdir. SCADA sistemlərinin cloud computing mühitlərinə köçürülməsi yolları göstərilmişdir. Buludlara miqrasiya strategiyasında istifadə olunan müxtəlif bulud modellərinin və xidmətlərinin üstünlükləri qeyd olunmuşdur. Buludəsaslı SCADA sistemlərinin fəaliyyətinə mane ola biləcək mövcud boşluqlar göstərilmişdir. Buludəsaslı SCADA sistemlərindən istifadə etdikdə təhlükəsizliklə əlaqədar yaranan problemlər və risklər analiz edilmişdir. Bu problemlərin həlli üçün müəyyən təkliflər verilmişdir.

Minnətdarlıq

Bu iş Azərbaycan Respublikası Dövlət Neft Şirkətinin Elm Fondunun maliyyə yardımı ilə yerinə yetirilmişdir – Qrant – № 03 LR.

Ədəbiyyat

1. Is Moving Your SCADA System to the Cloud Right For Your Company, Cloud-Based SCADA Systems: The Benefits & Risks, White Paper, 2011. https://www.controlglobal.com/
2. Shahzad A., Musa S., Aborujilah A., Ismail M.N., Irfan M. Conceptual Model of Real Time Infrastructure Within Cloud Computing Environment // International Journal of Computer Networks, 2013, vol.5, issue 1, pp.18–24.
3. Liu M., Yuan M., Wang F., Sun C. The Oil and Gas Pipeline Clouding SCADA System and Multiple Data Centers Storage System Design / International Conference on Manufacturing Construction and Energy Engineering, 2016, pp.293–297.
4. Honeywell Process Solutions**.** Securing SCADA in the cloud, 2019. https://www.processonline.com.au/content/software-it/article/securing-scada-in-the-cloud-417777075
5. Mrabet Z.E, Kaabouch N., Ghazi H.E., Ghazi H.E. Cyber-Security in Smart Grid: Survey and Challenges // Computers & Electrical Engineering, 2018, vol.67, pp.469–482.
6. Soufiane S., Halima B. SaaS Cloud Security: Attacks and Proposed Solutions // Transactions on Machine Learning and Artificial Intelligence, 2017, vol.5, no.4, pp.291–301.
7. Stojanović M.D., Boštjanĉiĉ Rakas S.V., Marković-PetroviC J.D. Scada systems ın the cloud and fog envıronments: mıgratıon scenarıos and securıty ıssues // Electronics and Energetics, 2019, vol.32, no.3, pp.345–358.
8. Yosra B.D., Yacine D., Slim R., Noureddine B. A Novel Sensor Cloud Based SCADA infrastructure for Monitoring and Attack prevention / MoMM '16: Proceedings of the 14th International Conference on Advances in Mobile Computing and Multi Media, November 2016, pp.45–49. https://doi.org/10.1145/3007120.3007169

9. Yadav G., Paul K. Archıtecture and Securıty of Scada Systems: a Revıew // 2020. https://arxiv.org/abs/2001.02925
10. Baker T., Mackay M., Shaheed A., Aldawsari B. Security-oriented cloud platform for SOA-based SCADA / 15th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing May 2015, pp.961–970.
11. HyungJun K. Security and Vulnerability of SCADA Systems over IP-Based Wireless Sensor Networks // International Journal of Distributed Sensor Networks, 2012, doi:10.1155/2012/268478
12. Zakuan F., Norziana J., Qais S.Q., Mohd E.R., Norhamadi J., Maslina D., HafizahChe H. A Study on Security Vulnerabilities Assessment and Quantification in SCADA // Journal of Engineering and Applied Sciences, 2018, vol.13, no.6, pp.1338–1346.
13. Fataliyev T.Kh., Mehdiyev Sh.A. Analysis and New Approaches to the Solution of Problems of Operation of Oil and Gas Complex as Cyber-Physical System // International Journal of Information Technology and Computer Science, vol.10, no.11, 2018, pp.67–76.
14. Zhifeng Y., Fei H., Xuehui F., Qi F., Zhen C., Yidan Z. Cloud Computing and Big Data for Oil and Gas Industry Application China // Journal of Computers, 2019, vol.14, no.4, pp.268–282.
15. Keith S., Joe F., Karen K. Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems // National Institute of Standards and Technology Special Publication 800-82, 164 p.
16. Slay J., Miller M. A Security Architecture for SCADA Networks / 17th Australasian Conference on Information Systems, 2006.
17. Liu M., Yuan M., Li G. Design Private Cloud of Oil and Gas SCADA System // EAI Endorsed Transactions on Scalable Information Systems, 2014, vol.1, issue 3, pp.1–5.
18. Alguliyev R., Alekperov R. Cloud Computing: Modern State, Problems and Prospects // Telecommunications and Radio Engineering, 2013, vol.73, no.3. pp.255-266.
19. Diaby T., Rad B.B. Cloud Computing: A review of the Concepts and Deployment Models // International Journal of Information Technology and Computer Science, 2017, vol.9, no.6, pp.50–58.
20. Zhang Q., Cheng L., Boutaba R. Cloud computing: state-of-the-art and research challenges // Journal of Internet Services and Applications, 2010, vol.1, pp.7–18.
21. Ələkbərov R.Q., Həşimov M.A. Bulud texnologiyaları: xidmətlər, problemlər və tətbiq sahələri // İnformasiya texnologiyaları problemləri, 2016, №1, s.3–10.
22. Combs L. Cloud Computing for SCADA, moving all or part of SCADA applications to the cloud can cut costs, significantly while dramatically increasing reliability and scalability. http://www.indusoft.com/Documentation/White-Papers/ArtMID/1198/ArticleID/430/Cloud-Computing-for-SCADA
23. Tomáš L., Iveta Z. Improvement of Human-Plant Interactivity via Industrial Cloud-Based Supervisory Control and Data Acquisition System. / International Conference on Advances in Production Management Systems (APMS), 2014, pp.83–90.
24. Sajid A., Abbas H., Saleem K. Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges // IEEE Access, 2016, vol.4, pp.1375–1385.
25. Piggin R.S.H. Securing scada in the cloud: managing the risks to avoid the perfect storm / IET & ISA 60th International Instrumentation Symposium, 2014.
26. Kyle W. SCADA in the Cloud A Security Conundrum? Trend Micro Incorporated Research Paper 2013, https://blog.trendmicro.com/trendlabs-security-intelligence/scada-in-the-cloud-a-security-conundrum/
27. Wang Y. sSCADA: Securing SCADA infrastructure communications // International Journal of Communication Networks and Distributed Systems, 2012, vol.6, no.1, pp.59–78.

28. Patrıck D.H. A security checklist for SCADA systems in the cloud, https://gcn.com/articles/2015/06/29/scada-cloud.aspx
29. John D. F., Andres E. F. SCADA systems: vulnerabilities and remediation // Journal of Computing Sciences in Colleges, 2005, vol.20, no.4, pp.160–168.

УДК 004.056

Алекперов Рашид Г., Гашимов Мамед А.
Институт Информационных Технологий НАНА, Баку, Азербайджан
rashid@iit.ab.az, mamedhashimov@gmail.com

Вопросы безопасности в облачных системах SCADA

В статье рассматриваются вопросы безопасности облачных систем SCADA (Supervisory Control and Data Acquisition), которые широко используются при мониторинге и управлении нефтегазовой отраслью. Поскольку традиционные системы SCADA очень дорогие, негибкие и трудно масштабируемые, возникают многочисленные проблемы, связанные со сбором, передачей и обработкой данных. Миграция системных приложений SCADA в облачную среду обеспечивает снижение затрат, повышение масштабируемости, эффективное управление системой, повышение надежности и решение проблем, связанных с ресурсами. В статье рассматриваются существующие уязвимости, которые могут препятствовать безопасности облачных систем SCADA. Реализация мер безопасности и оценки рисков в облачных системах SCADA является актуальной проблемой. В связи с этим анализируются проблемы безопасности и риски при использовании облачных систем SCADA и даются рекомендации по их решению в определенной степени.

Ключевые слова: *нефтегазовая отрасль, облачные системы SCADA, облачные вычисления, облачные сервисы, облачные модели, безопасность*.

Rashid G. Alakbarov, Mammad A. Hashimov
Institute of Information Technology of ANAS, Baku, Azerbaijan
rashid@iit.ab.az, mamedhashimov@gmail.com

Security issues in cloud-based SCADA system

The article discusses the security issues of cloud-based SCADA (Supervisory Control and Data Acquisition) systems, which are widely used in monitoring and management of the oil and gas industry. Since the traditional SCADA systems are very expensive, inflexible, and difficult to scale, numerous problems related to data collection, transmission and processing occur. The migration of SCADA system applications to the cloud environment allows for cost reduction, improved scalability, efficient system management, increased reliability, and solution of resource related problems. The article highlights the existing vulnerabilities that could hinder the security of cloud-based SCADA systems. Implementing security measures and risk assessment in cloud-based SCADA systems is a topical issue. In this regard, security problems and risks in the use of cloud-based SCADA systems are analyzed and recommendations are provided to solve them to some extent.

Keywords: *Oil and gas industry, cloud-based SCADA systems, cloud computing, cloud services, cloud models, security.*